8 IP Multicast Commands

8.1 IGMP Configuration Commands
8.2 MLD Configuration Commands
8.3 IPv4 PIM Configuration Commands
8.4 IPv6 PIM Configuration Commands
8.5 MSDP Configuration Commands
8.6 Multicast VPN Configuration Commands
8.7 IPv4 Multicast Route Management Commands
8.8 IPv6 Multicast Route Management Commands
8.9 VLAN-based IGMP Snooping Configuration Commands
8.10 VSI-based IGMP Snooping Configuration Commands
8.11 BD-based IGMP Snooping Configuration Commands
8.12 MLD Snooping Configuration Commands
8.13 Static Multicast MAC Address Configuration Commands
8.14 Multicast VLAN Configuration Commands
8.15 Controllable Multicast Configuration Commands
8.16 Multicast Network Management Commands

8.1 IGMP Configuration Commands

8.1.1 Command Support

Product	Support
S1700	Not supported.

Product	Support
S300	Supported.
S500	Supported.
S2700	Supported.
S5700	Supported except S5731-L and S5731S-L.
S6700	Supported.

NOTE

Only S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support the IGMP multi-instance feature.

8.1.2 display default-parameter igmp

Function

The **display default-parameter igmp** command displays default IGMP configurations.

Format

display default-parameter igmp

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

This command displays default IGMP parameter settings even if IGMP parameters have been modified. Therefore, you can use this command to check which parameters have been modified.

Example

Display default IGMP configurations.

```
<HUAWEI> display default-parameter igmp
  IGMP View Default Configurations:
```



```
---------------------------------
Lastmember-queryinterval: 1 s
Max-response-time: 10 s
Require-router-alert: disabled
Robust-count: 2
Send-router-alert: enabled
Ssm-mapping: disabled
Timer other-querier-present: 125 s
Timer query: 60 s

Interface View Default Configurations:
--------------------------------------
Group-policy: disabled
Lastmember-queryinterval: 1 s
Lastmember-query time: 2 s
Max-response-time: 10 s
Other-querier-present-timer-expiry: off
Prompt-leave: disabled
Require-router-alert: disabled
Robust-count: 2
Send-router-alert: enabled
Ssm-mapping: disabled
Startup-query-timer-expiry: off
Static-group: disabled
Timer other-querier-present: 125 s
Timer query: 60 s
Version: 2
Ip-source-policy: disabled
```

Table 8-1 Description of the **display default-parameter igmp** command output

Item	Description
IGMP View Default Configurations	Default configurations in the IGMP view. The default configurations take effect globally.
Lastmember-queryinterval	Interval for sending IGMP Group-Specific Query messages. This parameter is configured using the **lastmember-queryinterval (IGMP view)** command in the IGMP view or the **igmp lastmember-queryinterval** command in the interface view.
Max-response-time	Maximum response time for IGMP Query messages. This parameter is configured using the **max-response-time (IGMP view)** command in the IGMP view or the **igmp max-response-time** command in the interface view.
Require-router-alert	Whether the device checks for the Router-Alert option in the received IGMP message. This parameter is configured using the **require-router-alert (IGMP view)** command in the IGMP view or the **igmp require-router-alert** command in the interface view.
Robust-count	Robustness variable of an IGMP querier. This parameter is configured using the **robust-count (IGMP view)** command in the IGMP view or the **igmp robust-count** command in the interface view.

Item	Description
Send-router-alert	Whether the IGMP messages sent from the device carry the Router-Alert option. This parameter is configured using the **send-router-alert (IGMP view)** command in the IGMP view or the **igmp send-router-alert** command.
Ssm-mapping	Status of the SSM mapping function. The value can be: ● enabled: This function is enabled. ● disabled: This function is disabled. SSM mapping can be configured using the **igmp ssm-mapping enable** command.
Timer other-querier-present	Length of the other querier present timer. This parameter is configured using the **timer other-querier-present (IGMP view)** command in the IGMP view or the **igmp timer other-querier-present** command in the interface view.
Timer query	Interval for sending IGMP General Query messages. This parameter is configured using the **timer query (IGMP view)** command in the IGMP view or the **igmp timer query** command in the interface view.
Interface View Default Configurations	Default configurations in the interface view. The configurations take effect only for IGMP-enabled interfaces.
Group-policy	Whether a multicast group policy is configured. The value can be: ● enabled: A multicast group policy is configured. ● disabled: No multicast group policy is configured. A multicast group policy is configured using the **igmp group-policy** command.
Lastmember-query time	Last member query time, calculated using the following formula: Last member query time = Last member query interval x Robustness variable The last member query time is not defined in IGMPv1.

Item	Description
Other-querier-present-timer-expiry	Status of the other querier present timer: ● off: The interface considers itself a querier and no other queriers exist. ● on: The interface no longer considers itself a querier and another querier exists.
Prompt-leave	Status of the fast leave function. The value can be: ● enabled: This function is enabled. ● disabled: This function is disabled. This function is configured using the **igmp prompt-leave** command.
Startup-query-timer-expiry	Startup query interval of the querier. The interface sends Query messages at this interval when it starts to function as a querier. The value is expressed in seconds and is 1/4 of the query interval (Timer query). The value **off** indicates that the interface has not started to send Query messages as a querier. The startup query timer is enabled only when the interface starts as a querier.
Static-group	Whether static multicast groups are configured. The value can be: ● enabled: Static multicast groups are configured. ● disabled: No static multicast groups are configured. A static multicast group is configured using the **igmp static-group** command.
Version	IGMP version number. IGMP has three versions: IGMPv1, IGMPv2, and IGMPv3, which is configured using the **igmp version** command.
Ip-source-policy	Status of IGMP Report/Leave message filtering based on host addresses. The value can be: ● enabled: This function is enabled. ● disabled: This function is disabled. This function is configured using the **igmp ip-source-policy** command.

8.1.3 display igmp control-message counters

Function

The **display igmp control-message counters** command displays statistics about IGMP control messages.

Format

display igmp [**vpn-instance** *vpn-instance-name* | **all-instance**] **control-message counters** [**interface** *interface-type interface-number*] [**message-type** { **query** | **report** }]

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Displays IGMP message statistics in a specified VPN instance.	The value must be an existing VPN instance name.
all-instance	Displays IGMP message statistics in all instances.	-
interface *interface-type interface-number*	Displays IGMP message statistics on a specified interface. If this parameter is not specified, the command displays IGMP message statistics on all interfaces.	-
message-type	Indicates the IGMP message type. If this parameter is not specified, the command displays statistics about all types of IGMP messages.	-
query	Displays statistics about Query messages received by the interface. Query messages are sent from a querier.	-
report	Displays statistics about Report messages received by the interface. Report messages are sent by hosts to join a multicast group.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can use this command to check the number of IGMP control messages sent and received on the device.

Example

Display statistics about the IGMP messages sent and received by VLANIF100.

```
<HUAWEI> display igmp control-message counters interface vlanif 100
Interface message counter information
 Vlanif100(192.168.2.1):
 Message Type              Sent       Valid      Invalid    Ignore
 ------------------------------------------------------------------
 General Query             1144       638186     0          0
 Group Query               0          0          0          0
 Source Group Query        0          0          0          0
 ------------------------------------------------------------------
 IGMPV1V2
 Report ASM                0          0          0          0
 Report SSM                0          0          0          0
 ------------------------------------------------------------------
 LEAVE ASM                 0          0          0          0
 LEAVE SSM                 0          0          0          0
 ------------------------------------------------------------------
 IGMPV3
 ISIN Report               0          0          0          0
 ISEX Report               0          0          0          0
 TOIN Report               0          0          0          0
 TOEX Report               0          0          0          0
 ALLOW Report              0          0          0          0
 BLOCK Report              0          0          0          0
 Source Records Total      0          0          0          0
 ------------------------------------------------------------------
 Others                    -          -          0          0
 ------------------------------------------------------------------
```

Table 8-2 Description of the **display igmp control-message counters interface vlanif 100** command output

Item	Description
Interface message counter information	IGMP packet information on an interface.
Vlanif100(192.168.2.1)	Type, number, and IP address of the interface.
Message Type	Type of IGMP messages.
Sent	Number of IGMP messages sent from the interface.
Valid	Number of valid IGMP messages received by the interface.
Invalid	Number of wrong IGMP messages received by the interface.
Ignore	Number of received IGMP messages ignored by the interface.
General Query	Number of IGMP General Query messages.

Item	Description
Group Query	Number of IGMP Group-Specific Query messages.
Source Group Query	Number of IGMP Group-and-Source-Specific Query messages.
Report ASM	Number of IGMPv1 and IGMPv2 Report messages with multicast group addresses in the ASM group address range.
Report SSM	Number of IGMPv1 and IGMPv2 Report messages with multicast group addresses in the SSM group address range.
LEAVE ASM	Number of IGMPv2 Leave messages with multicast group addresses in the ASM group address range.
LEAVE SSM	Number of IGMPv2 Leave messages with multicast group addresses in the SSM group address range.
ISIN Report	Number of IGMPv3 IS_IN Report messages.
ISEX Report	Number of IGMPv3 IS_EX Report messages.
TOIN Report	Number of IGMPv3 TO_IN Report messages.
TOEX Report	Number of IGMPv3 TO_EX Report messages.
ALLOW Report	Number of IGMPv3 ALLOW Report messages.
BLOCK Report	Number of IGMPv3 BLOCK Report messages.
Source Records Total	Number of multicast sources carried in IGMPv3 messages.
Others	Number of invalid and ignored IGMP messages of unknown types.

8.1.4 display igmp explicit-tracking

Function

The **display igmp explicit-tracking** command displays explicit (S, G) entries of IGMPv3 hosts, that is, (S, G) entries that IGMPv3 hosts have joined in Include mode.

Format

display igmp [**vpn-instance** *vpn-instance-name* | **all-instance**] **explicit-tracking** [**interface** *interface-type interface-number* [**host-address** *host-address* | **group** *group-address* **source** *source-address*]]

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Displays information about IGMPv3 hosts that join a specified multicast source in INCLUDE mode in a specified VPN instance.	The value must be an existing VPN instance name.
all-instance	Displays information about IGMPv3 hosts that join a specified multicast source in INCLUDE mode in all instances.	-
interface *interface-type interface-number*	Displays information about IGMPv3 hosts that join a specified multicast source in INCLUDE mode on a specified interface.	-
host-address *host-address*	Specifies the address of an IGMP host.	The address is in dotted decimal notation.
group *group-address*	Specifies the address of a multicast group.	The value ranges from 224.0.1.0 to 239.255.255.255, in dotted decimal notation.
source *source-address*	Specifies the address of a multicast source.	The address is in dotted decimal notation.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can use this command to view information about IGMPv3 hosts that have dynamically joined specified sources/groups in Include mode.

Example

Display information about the IGMPv3 hosts that have joined specified source/group in Include mode.

```
<HUAWEI> display igmp explicit-tracking
Explicit-tracking information
 Total 1 host, 2 entries

 Vlanif100(192.168.0.12)
  0001.Host: 192.168.0.28
       Uptime: 00:02:47
```



```
    Expires: 00:01:33
    (S, G) List:
      Group: 232.1.1.1
          Source: 10.12.12.12
            Uptime: 00:02:47
            Time since last refresh: 00:02:47
          Source: 10.13.13.13
            Uptime: 00:02:47
            Time since last refresh: 00:02:47
```

Table 8-3 Description of the **display igmp explicit-tracking** command output

Item	Description
Explicit-tracking information	IGMP host information.
Total 1 host, 2 entries	There is one IGMP host and two (S, G) entries.
Vlanif100(192.168.0.12)	Interface connected to IGMPv3 hosts that have joined a group with source addresses specified in Include mode.
Host	IGMP host address.
Uptime	Running time since an IGMP host joins a multicast group. The time format is as follows: • If the time is shorter than or equal to 24 hours, the format is hours:minutes:seconds. • If the time is longer than 24 hours but shorter than or equal to one week, the format is days:hours. • If the time is longer than one week, the format is weeks:days.
Expires	Amount of time left before an IGMP host times out. After the IGMP host expires, it is deleted from the IGMP member host list. The time format is as follows: • If the time is shorter than or equal to 24 hours, the format is hours:minutes:seconds. • If the time is longer than 24 hours but shorter than or equal to one week, the format is days:hours. • If the time is longer than one week, the format is weeks:days.
(S, G) List	List of multicast sources and groups an IGMP host has joined.
Group	Multicast group address.
Source	Multicast source address.

Item	Description
Time since last refresh	Amount of time since an IGMP host last joins a group. The time format is as follows: • If the time is shorter than or equal to 24 hours, the format is hours:minutes:seconds. • If the time is longer than 24 hours but shorter than or equal to one week, the format is days:hours. • If the time is longer than one week, the format is weeks:days.

8.1.5 display igmp group

Function

The **display igmp group** command displays information about IGMP groups that hosts have dynamically joined by sending IGMP Report messages.

Format

display igmp [**vpn-instance** *vpn-instance-name* | **all-instance**] **group** [*group-address* | **interface** *interface-type interface-number*]* [**verbose**]

display igmp [**vpn-instance** *vpn-instance-name* | **all-instance**] **group** [**interface** *interface-type interface-number*] **entry-number**

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Displays information about IGMP groups in a VPN instance.	The value must be an existing VPN instance name.
all-instance	Displays information about IGMP groups in all instances.	-
group-address	Displays information about the IGMP group with a specified group address.	The value ranges from 224.0.1.0 to 239.255.255.255, in dotted decimal notation.
interface *interface-type interface-number*	Displays information about the IGMP group on the specified interface.	-

Parameter	Description	Value
verbose	Displays detailed information about IGMP groups. If the parameter is not specified, the command displays only the summary of IGMP groups.	-
entry-number	Displays statistics about IGMP multicast groups that hosts dynamically join.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

If a host wants to receive multicast data for a multicast group, the host must join the multicast group in either of the following modes:

- Dynamic mode: After you run the **igmp enable** command to enable IGMP on the interface connected to the network segment on which the host resides, the host can dynamically join the multicast group.
- Static mode: After you run the **igmp static-group** command to enable IGMP on the interface connected to the network segment on which the host resides, the host can statically join the multicast group.

To monitor the status of the multicast group or locate a fault in a dynamically joined multicast group, run the **display igmp group** command. This command displays information about the multicast group that hosts have dynamically joined.

Example

Display information about dynamic IGMP groups.

```
<HUAWEI> display igmp group
Interface group report information of VPN-Instance: public net
 Vlanif100(10.1.6.2):
  Total 1 IGMP Group reported
   Group Address   Last Reporter   Uptime      Expires
   225.1.1.2       10.1.6.10       00:02:04    00:01:17
```

Display detailed information about dynamic IGMP groups.

```
<HUAWEI> display igmp group verbose
Interface group report information of VPN-Instance: public net
 Limited entry of this VPN-Instance: -
 Vlanif100(10.1.6.2):
  Total entry on this interface: 1
  Limited entry on this interface: -
```



```
Total 1 IGMP Group reported
 Group: 225.1.1.2
   Uptime: 00:03:59
   Expires: off
   Last reporter: 10.1.6.10
   Last-member-query-counter: 0
   Last-member-query-timer-expiry: off
   Group mode: include
   Version1-host-present-timer-expiry: off
   Version2-host-present-timer-expiry: off
   Source list:
     Source: 192.168.232.1
       Uptime: 00:51:07
       Expires: 00:02:05
       Last-member-query-counter: 0
       Last-member-query-timer-expiry: off
```

Display statistics about IGMP multicast groups that hosts dynamically join.

```
<HUAWEI> display igmp group entry-number
Interface group report information of VPN-Instance: public net
  Total 4 IGMP Groups reported
 Vlanif200(10.36.1.10):
  Total 2 IGMP Groups reported
 Vlanif100(10.0.0.4):
  Total 2 IGMP Groups reported
```

Table 8-4 Description of the **display igmp group command** output

Item	Description
Interface group report information of VPN-Instance	VPN instance to which IGMP groups on an interface belong. **public net** indicates the public network instance.
Group Address	Address of a multicast group.
Last Reporter	Link-local address of the last host that sends a Multicast Listener Report message. **NOTE** When a host joins a multicast group through a sub-interface for QinQ or Dot1q VLAN tag termination, the Last Reporter field displays the address of the multicast proxy. By default, the address of the multicast proxy is 192.168.0.1.
Limited entry of this VPN-Instance	Maximum number of IGMP entries that can be created for this instance.
Vlanif100(10.1.6.2)	Interface type and interface number (IP address).
Total entry on this interface	Total number of IGMP entries on the current interface.
Limited entry on this interface	Maximum number of IGMP entries that the current interface can create.
Total 1 IGMP Group reported	Number of IGMP groups that the current interface has dynamically joined.

Item	Description
Group	Address of a multicast group.
Uptime	Amount of time since a multicast group is created. The time format is as follows: ● If the time is shorter than or equal to 24 hours, the format is hours:minutes:seconds. ● If the time is longer than 24 hours but shorter than or equal to one week, the format is days:hours. ● If the time is longer than one week, the format is weeks:days.
Expires	Time left before a group will be deleted from the IGMP group table. The time format is as follows: ● If the time is shorter than or equal to 24 hours, the format is hours:minutes:seconds. ● If the time is longer than 24 hours but shorter than or equal to one week, the format is days:hours. ● If the time is longer than one week, the format is weeks:days. "off" indicates that the group will never be aged out.
Last-member-query-counter	Number of times the querier will send Group-Specific Query messages after receiving a Leave message. The counter value decreases by 1 every time the querier sends a Group-Specific Query message. This parameter is configured using the **igmp robust-count** command. The value 0 indicates that the querier does not send Group-Specific Query messages after receiving a Leave message.
Last-member-query-timer-expiry	Length of the last member query timer. The timer starts only when a Leave message is received from a group member. The timer value is configured using the **igmp lastmember-queryinterval** command. The value **off** indicates that the last member query timer has not started.

Item	Description
Group mode	Multicast group record type, which can be Include or Exclude. It is displayed only when the interface is running IGMPv3.
Version1-host-present-timer-expiry	Timeout interval of IGMPv1 hosts. IGMPv1 does not define the Leave message; therefore, memberships of IGMPv1 hosts are aged using a timer. The device starts the timer when receiving a Report message from an IGMPv1 host. The timer value is calculated using the following formula: IGMPv1 timeout interval = General group query interval x Robustness variable + Maximum response time for Query messages The general group query interval is configured using the **igmp timer query** command. The robustness variable is configured using the **igmp robust-count** command. The maximum response time for Query messages is configured using the **igmp max-response-time** command. The value **off** indicates that the device has not received any Report messages from IGMPv1 hosts.
Version2-host-present-timer-expiry	Timeout interval of IGMPv2 hosts. It is displayed only when the interface is running IGMPv3. The value **off** indicates that the device has not received any Report messages from IGMPv2 hosts.
Source list	List of multicast sources. It is displayed only when the interface has IGMPv3 receiver hosts attached.
Source	IP address of a multicast source.

8.1.6 display igmp group ssm-mapping

Function

The **display igmp group ssm-mapping** command displays information about multicast group entries established with SSM mapping.

Format

display igmp [**vpn-instance** *vpn-instance-name* | **all-instance**] **group** [*group-address* | **interface** *interface-type interface-number*]* **ssm-mapping** [**verbose**]

display igmp [**vpn-instance** *vpn-instance-name* | **all-instance**] **group ssm-mapping** [**interface** *interface-type interface-number*] **entry-number**

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Displays group entries established with SSM mapping in a specified VPN instance.	The value must be an existing VPN instance name.
all-instance	Displays group entries established with SSM mapping in all instances.	-
group-address	Displays information about the specified multicast group entries established with SSM mapping. If this parameter is not specified, the command displays information about all multicast group entries established with SSM mapping.	The value ranges from 224.0.1.0 to 239.255.255.255, in dotted decimal notation.
interface *interface-type interface-number*	Displays information about multicast group entries established with SSM mapping on the specified interface. If this parameter is not specified, the command displays information about multicast group entries established with SSM mapping on all interfaces.	-
verbose	Displays detailed information about group membership established with SSM mapping. If the parameter is not specified, the command displays only the summary of group membership established with SSM mapping.	-
entry-number	Displays statistics about IGMP multicast groups established with SSM mapping.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can use the **display igmp group ssm-mapping** command to view information about multicast group entries that are established with SSM mapping. SSM mapping entries are configured using the **ssm-mapping** command.

Example

Display summary of all multicast group entries established with SSM mapping.

```
<HUAWEI> display igmp group ssm-mapping

IGMP SSM mapping interface group report information of VPN-Instance: public net
 Limited entry of this VPN-Instance: -
 Vlanif100(192.168.101.1):
  Total 1 IGMP SSM-Mapping Group reported
   Group Address   Last Reporter   Uptime      Expires
   232.0.0.1       192.168.101.2   00:00:02    00:02:08
```

Display detailed information about all multicast group entries established with SSM mapping.

```
<HUAWEI> display igmp group ssm-mapping verbose
Interface group report information of VPN-Instance: public net
 Limited entry of this VPN-Instance: -
 Vlanif100(192.168.101.1):
  Total entry on this interface: 1
  Limited entries on this interface: -
  Total 1 IGMP SSM-Mapping Group reported
   Group: 232.0.0.1
     Uptime: 00:00:15
     Expires: 00:01:55
     Last reporter: 192.168.101.2
     Last-member-query-counter: 0
     Last-member-query-timer-expiry: off
     Group mode: exclude
     Version1-host-present-timer-expiry: off
     Version2-host-present-timer-expiry: 00:01:55
```

Display detailed information about IGMP multicast groups established with SSM mapping.

```
<HUAWEI> display igmp group ssm-mapping entry-number
Interface group report information of VPN-Instance: public net
  Total 4 IGMP SSM-Mapping Groups reported
 Vlanif200(10.36.1.10):
  Total 2 IGMP SSM-Mapping Groups reported
 Vlanif100(10.0.0.4):
  Total 2 IGMP SSM-Mapping Groups reported
```

Table 8-5 Description of the **display igmp group ssm-mapping** command output

Item	Description
IGMP SSM mapping interface group report information of VPN-Instance	VPN instance to which IGMP groups on an interface belong. **public net** indicates the public network instance.

Item	Description
Group Address	Group address.
Last Reporter	Link-local address of the last host that sends a Multicast Listener Report message.
Limited entry of this VPN-Instance	Maximum number of entries that can be generated in the VPN instance.
Vlanif100(192.168.101.1)	Interface type and interface number (IP address).
Interface group report information of VPN-Instance	VPN instance to which IGMP groups on an interface belong.
Total entry on this interface	Total number of entries generated on the interface.
Limited entries on this interface	Maximum number of entries that can be generated on the interface.
Total 1 IGMP SSM-Mapping Group reported	Number of IGMP Report messages with SSM group addresses received on the interface.
Group	Group address.
Uptime	Amount of time since the last Report message is received. The time format is as follows: • If the time is shorter than or equal to 24 hours, the format is hours:minutes:seconds. • If the time is longer than 24 hours but shorter than or equal to one week, the format is days:hours. • If the time is longer than one week, the format is weeks:days.
Expires	Timeout period of a group. The time format is as follows: • If the time is shorter than or equal to 24 hours, the format is hours:minutes:seconds. • If the time is longer than 24 hours but shorter than or equal to one week, the format is days:hours. • If the time is longer than one week, the format is weeks:days.
Last-member-query-counter	Number of times Group-Specific Query messages are sent.

Item	Description
Last-member-query-timer-expiry	Length of the last member query timer. The timer starts only when a Leave message is received from a group member. The timer value is configured using the **igmp lastmember-queryinterval** command. The value **off** indicates that the last member query timer has not started.
Group mode	Filter mode of a group, which can be Include or Exclude. It is displayed only when the interface is running IGMPv3.
Version1-host-present-timer-expiry	Timeout interval of IGMPv1 hosts. IGMPv1 does not define the Leave message; therefore, memberships of IGMPv1 hosts are aged using a timer. The device starts the timer when receiving a Report message from an IGMPv1 host. The timer value is calculated using the following formula: IGMPv1 timeout interval = General group query interval x Robustness variable + Maximum response time for Query messages The general group query interval is configured using the **igmp timer query** command. The robustness variable is configured using the **igmp robust-count** command. The maximum response time for Query messages is configured using the **igmp max-response-time** command. The value **off** indicates that the device has not received any Report messages from IGMPv1 hosts.
Version2-host-present-timer-expiry	Timeout interval of IGMPv2 hosts. It is displayed only when the interface is running IGMPv3. The value **off** indicates that the device has not received any Report messages from IGMPv2 hosts.

8.1.7 display igmp group static

Function

The **display igmp group static** command displays information about static IGMP entries.

Format

display igmp [**vpn-instance** *vpn-instance-name* | **all-instance**] **group** [*group-address*] **static** [**up** | **down**] [**verbose**]

display igmp [**vpn-instance** *vpn-instance-name* | **all-instance**] **group** [*group-address* | **interface** *interface-type interface-number*]* **static** [**verbose**]

display igmp [**vpn-instance** *vpn-instance-name* | **all-instance**] **group** [*group-address*] **static interface-number**

display igmp [**vpn-instance** *vpn-instance-name* | **all-instance**] **group static interface** *interface-type interface-number* **entry-number**

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Displays information about static IGMP entries in a specified VPN instance.	The value must be an existing VPN instance name.
all-instance	Displays information about static IGMP entries in all instances.	-
group-address	Displays information about static IGMP entries of a specified group. If this parameter is not specified, the command displays static IGMP entries of all groups.	The address is in dotted decimal notation and ranges from 224.0.1.0 to 239.255.255.255.
up | **down**	Displays information about interfaces in Up or Down state. If this parameter is not specified, the command displays all interfaces in IGMP entries.	-
verbose	Displays detailed interface list in a static IGMP group. If the parameter is not specified, the command displays only summary of static IGMP entries.	-
interface-number	Displays the number of interfaces in a static IGMP group.	-
interface *interface-type interface-number*	Displays information about the static IGMP groups on a specified interface. *interface-type interface-number* specifies the type and number of an interface.	-

Parameter	Description	Value
entry-number	Displays the number of static IGMP groups on an interface.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

This command displays information about static IGMP entries configured using the **igmp static-group** command.

Example

Display information about all static IGMP entries.

```
<HUAWEI> display igmp group static
Static join group information
 Total 2 entries, Total 2 active entries
  Group Address   Source Address  Interface         State     Expires
  225.1.1.1       10.1.1.1        Vlanif10          UP        never
  225.1.1.2       10.1.1.1        Vlanif20          UP        never
```

Table 8-6 Description of the **display igmp group static** command output

Item	Description
Static join group information	information about static IGMP groups.
Total 2 entries, Total 2 active entries	Number of static IGMP entries and active IGMP entries on the interface.
Group Address	Multicast group address.
Source Address	Multicast source address.
Interface	Interface type and number.
State	Status of an interface, which can be: • UP: The interface is operating normally. • DOWN: An error occurs on the physical link of the interface.
Expires	Amount of time left before a group entry times out. If this field displays **never**, the corresponding multicast group is a static group and will never age out.

Display detailed information about static IGMP entries.

```
<HUAWEI> display igmp group static verbose
Static join group information
 Total 2 entries
  00001.(*, 225.1.1.1)
     Total List of 1 joined interface
     1.Vlanif10
        State:            UP
        Reference Count:   1
        Multicast Boundary:NO
        Outgoing Interface:YES
  00002.(*, 225.1.1.2)
     Total List of 1 joined interface
     1.Vlanif20
        State:            UP
        Reference Count:   1
        Multicast Boundary:NO
        Outgoing Interface:YES
```

Table 8-7 Description of the display igmp group static verbose command output

Item	Description
Static join group information	information about static IGMP groups.
Total 2 entries	Number of static IGMP entries on the interface.
00001.(*, 225.1.1.1)	(*, G) entry ID.
Total List of 1 joined interface	Downstream interface list of the (*, G) entry.
1.Vlanif10	Interface type and interface number.
State	Status of an interface, which can be: ● UP: The interface is operating normally. ● DOWN: An error occurs on the physical link of the interface.
Reference Count	Number of the IGMP entry on the current interface is referenced.
Multicast Boundary	Whether the multicast forwarding boundary is configured: ● YES ● NO This function is configured using the **multicast boundary** *group-address* { *mask* | *mask-length* } command.
Outgoing Interface	Whether downstream interfaces exist: ● YES ● NO

Display lists of Up interfaces in static IGMP entries.


```
<HUAWEI> display igmp group static up
Static join group information
 Total 4 entries
 00001.(*,225.1.1.1)
     Total List of 2 joined interfaces
     Total Matched 2 interfaces
     1.Vlanif10
     2.Vlanif20
 00002.(*,225.1.1.2)
     Total List of 2 joined interfaces
     Total Matched 2 interfaces
     1.Vlanif10
     2.Vlanif20
```

Table 8-8 Description of the display igmp group static up command output

Item	Description
Total List of 2 joined interfaces	Number of interfaces in a static group.
Total Matched 2 interfaces	List of Up interfaces in a static group.

Display information about IGMP groups statically configured on VLANIF100.

```
<HUAWEI> display igmp group interface vlanif 100 static
Static join group information
 Total 2 entries
 Specified interface state:UP
 Total 2 entries matched
   Group Address   Source Address  Expires
   226.0.0.1       10.0.5.120      never
   226.0.0.2       0.0.0.0         never
```

Table 8-9 Description of the display igmp group interface vlanif 100 static command output

Item	Description
Static join group information	information about static IGMP groups.
Total 2 entries	Number of static IGMP entries on the interface.
Specified interface state	Status of an interface, which can be: • UP: The interface is operating normally. • DOWN: An error occurs on the physical link of the interface.
Total 2 entries matched	Number of IGMP groups that meet the query conditions.
Group Address	Multicast group address.
Source Address	Multicast source address.

Item	Description
Expires	Amount of time left before a group entry times out. If this field displays **never**, the corresponding multicast group is a static group and will never age out.

8.1.8 display igmp interface

Function

The **display igmp interface** command displays information about IGMP interfaces.

Format

display igmp [**vpn-instance** *vpn-instance-name* | **all-instance**]**interface** [*interface-type interface-number* | **up** | **down**] [**verbose**]

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Displays information about IGMP interfaces in a VPN instance.	The value must be an existing VPN instance name.
all-instance	Displays information about IGMP interfaces in all instances.	-
interface-type interface-number	Displays information about a specified IGMP interface. If this parameter is not specified, the command displays information about all IGMP interfaces.	-
up	Displays information about the IGMP interfaces with the IP protocol in Up state and the IGMP protocol in Active state.	-
down	Displays information about the IGMP interfaces with the IP protocol in Down state and the IGMP protocol in Inactive state.	-
verbose	Displays detailed information about IGMP interfaces.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

To check the IGMP configuration and running information on an interface, run the **display igmp interface** command. This command displays IGMP information only when IGMP is enabled on the interface.

Example

Display the IGMP configuration and running information on VLANIF100.

```
<HUAWEI> display igmp interface vlanif 100
Interface information of VPN-Instance: public net
 Vlanif100(192.168.1.2):
   IGMP is enabled
   Current IGMP version is 2
   IGMP state: up
   IGMP group policy: none
   IGMP limit: -
   Value of query interval for IGMP (negotiated): -
   Value of query interval for IGMP (configured): 60 s
   Value of other querier timeout for IGMP: 0 s
   Value of maximum query response time for IGMP: 10 s
   Querier for IGMP: 192.168.1.2 (this router)
  Total 1 IGMP Group reported
```

Display IGMP parameters on all interfaces.

```
<HUAWEI> display igmp interface verbose
Interface information of VPN-Instance: public net
 Vlanif100(192.168.1.2):
   IGMP is enabled
   Current IGMP version is 2
   IGMP state: up
   IGMP group policy: none
   IGMP limit: -
   Value of query interval for IGMP (negotiated): -
   Value of query interval for IGMP (configured): 60 s
   Value of other querier timeout for IGMP: 0 s
   Value of maximum query response time for IGMP: 10 s
   Value of last member query time: 2 s
   Value of last member query interval: 1 s
   Value of startup query interval: 15 s
   Value of startup query count: 2
   General query timer expiry (hours:minutes:seconds): 00:00:44
   Querier for IGMP: 192.168.1.2 (this router)
   IGMP activity: 1 joins, 0 leaves
   Robustness (negotiated): -
   Robustness (configured): 2
   Require-router-alert: disabled
   Send-router-alert: enabled
   Ip-source-policy: disabled
   Query Ip-source-policy: disabled
   Prompt-leave: disabled
   SSM-Mapping: enabled
   Startup-query-timer-expiry: off
   Other-querier-present-timer-expiry: off
```



```
 TTL-check: disabled
Total 1 IGMP Group reported
```

Table 8-10 Description of the **display igmp interface** command output

Item	Description
Interface information of VPN-Instance	VPN instance to which IGMP interface information belongs. **public net** indicates the public network instance.
Vlanif100(192.168.1.2)	Interface type and interface number (IP address).
IGMP is enabled	IGMP has been enabled on an interface. IGMP can be enabled on an interface using the **igmp enable** command.
Current IGMP version is 2	IGMP version running on an interface. IGMP has three versions: IGMPv1, IGMPv2, and IGMPv3. This parameter is configured using the **igmp version** command.
IGMP state	Status of an IGMP interface, which can be up or down.
IGMP group policy	Number of the ACL used in an IGMP group policy, which is used to control the number of groups that an interface can join. The ACL is specified by using the **igmp group-policy** command. The value **none** indicates that no ACL is applied to the interface.
IGMP limit	Maximum number of IGMP group memberships that the current interface can maintain. This parameter is configured using the **igmp limit** command.
Value of query interval for IGMP (negotiated)	Interval negotiated by non-queriers for sending Query messages. The negotiated value is only supported by IGMPv3.
Value of query interval for IGMP (configured)	Configured interval for sending IGMP Query messages. This parameter is configured using the **igmp timer query** command.
Value of other querier timeout for IGMP	Length of the other querier present timer. This parameter is configured using the **igmp timer other-querier-present** command. The value is 0 on the interface that functions as the querier.

Item	Description
Value of maximum query response time for IGMP	Maximum response time carried by an IGMP Query message. This parameter is configured using the **igmp max-response-time** command.
Value of last member query time	Last member query time, calculated using the following formula: Last member query time = Last member query interval x Robustness variable The last member query time is not defined in IGMPv1.
Value of last member query interval	Interval for sending Group-Specific Query messages. The value is configured using the **igmp lastmember-queryinterval** command. This interval is not defined in IGMPv1.
Value of startup query interval	Startup query interval of the querier. The interface sends Query messages at this interval when it starts to function as a querier. The value is 1/4 of the query interval configured using the **igmp timer query** command. The startup query interval is not defined in IGMPv1.
Value of startup query count	Number of query messages the querier interface sends at startup. The value is configured using the **igmp robust-count** command. The startup query count is not defined in IGMPv1.
General query timer expiry (hours:minutes:seconds)	Timeout interval of a general query timer.
Querier for IGMP	Link-local address of the IGMP querier. In IGMPv1, the querier is selected based on the multicast routing protocol. In IGMPv2, the multicast switch with the smallest IP address functions as the querier on the shared network segment.
IGMP activity: 1 joins, 0 leaves	Active group memberships on an interface. • joins: indicates the number of IGMP groups that the interface has joined. When the interface joins a new group, the value increases by 1. When the interface leaves a group, the value remains unchanged. • leaves: indicates the number of groups that the interface has left. When the interface leaves a group, the value increases by 1.

Item	Description
Robustness (negotiated)	Robustness variable negotiated by non-queriers. The negotiated value is only supported by IGMPv3.
Robustness (configured)	Robustness variable configured on an interface. This parameter is configured using the **igmp robust-count** command.
Require-router-alert	Whether the switch discards IGMP packets that do not contain the Router-Alert option in IP packet headers. ● enable: The switch discards IGMP packets that do not contain the Router-Alert option in IP packet headers. ● disable: The switch does not discard IGMP packets that do not contain the Router-Alert option in IP packet headers. This function is configured using the **igmp require-router-alert** command.
Send-router-alert	Whether the switch sends IGMP packets with the Router-Alert option. ● enabled: The switch sends IGMP packets with the Router-Alert option. ● disabled: The switch sends IGMP packets without the Router-Alert option. This function is configured using the **igmp send-router-alert** command.
Ip-source-policy	Whether to filter IGMP Report/Leave messages based on host addresses. ● enabled: The switch filters IGMP Report/Leave messages based on host addresses. ● disabled: The switch does not filter IGMP Report/Leave messages based on host addresses. This function is configured using the **igmp ip-source-policy** command.
Query Ip-source-policy	Whether to filter IGMP Query messages based on source addresses. ● enabled: The switch filters IGMP Query messages based on source addresses. ● disabled: The switch does not filter IGMP Query messages based on source addresses. This function is configured using the **igmp query ip-source-policy** command.

Item	Description
Prompt-leave	Whether fast leave is enabled. • enabled: Fast leave is enabled. • disabled: Fast leave is disabled. This function is configured using the **igmp prompt-leave** command.
SSM-Mapping	Whether SSM mapping is enabled. • enabled: SSM mapping is enabled. • disabled: SSM mapping is disabled. This function is enabled using the **igmp ssm-mapping enable** command.
Startup-query-timer-expiry	Interval at which the interface sends Query messages when it starts to function as a querier. The value is 1/4 of Timer query. The value **off** indicates that the interface has not started to send Query messages. The startup query timer is enabled only when the interface starts as a querier.
Other-querier-present-timer-expiry	Status of the other querier present timer: • off: The interface considers itself a querier and no other queriers exist. • on: The interface no longer considers itself a querier and another querier exists.
TTL-check	Whether the function to check the TTL values in received IGMP Report, Leave, and Query messages is enabled: • enabled • disabled This function is configured using the **igmp ttl-check** command.
Total 1 IGMP Group reported	Indicates the number of IGMP groups that the interface dynamically joins.

8.1.9 display igmp invalid-packet

Function

The **display igmp invalid-packet** command displays statistics and details about invalid IGMP packets received by the switch.

Format

display igmp [**vpn-instance** *vpn-instance-name* | **all-instance**] **invalid-packet** [**interface** *interface-type interface-number* | **message-type** { **leave** | **query** | **report** }] *

display igmp invalid-packet [*packet-number*] **verbose**

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Displays statistics about invalid IGMP messages received in a specified VPN instance.	The value must be an existing VPN instance name.
all-instance	Displays statistics about invalid IGMP messages received in all VPN instances.	-
interface *interface-type interface-number*	Displays statistics about invalid IGMP messages received on a specified interface. If this parameter is not specified, the command displays statistics about IGMP messages received on all interfaces.	-
message-type	Displays statistics about invalid IGMP messages of a specific type.	-
leave	Displays statistics about invalid Leave messages.	-
query	Displays statistics about invalid Query messages.	-
report	Displays statistics about invalid Report messages.	-
packet-number	Displays details about a specified number of invalid, recently received IGMP messages.	The value is an integer that ranges from 1 to 100. By default, details about all invalid, currently stored IGMP messages are displayed.
verbose	Displays details about invalid IGMP messages.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display igmp invalid-packet** command to view statistics and details about invalid IGMP messages for fault location and rectification.

If IGMP entries fail to be generated on a multicast network, you can run the **display igmp invalid-packet** command to check whether devices have received invalid IGMP messages. If the command output contains statistics about invalid IGMP messages, run the **display igmp invalid-packet** [*packet-number*] **verbose** command to view details about invalid IGMP messages to locate faults.

You can run the following commands to view information about specific invalid IGMP messages:

- Run the **display igmp invalid-packet interface** *interface-type interface-number* command to view statistics about invalid IGMP messages received by a specified interface.
- Run the **display igmp invalid-packet** *packet-number* **verbose** command to view details about invalid, recently received IGMP messages. Currently, the command output can contain details about a maximum of 100 invalid IGMP messages.

Example

Display statistics about invalid IGMP messages received by the switch.

```
<HUAWEI> display igmp invalid-packet

          Statistics of invalid packets for public net:
------------------------------------------------------------------------------
IGMP Query invalid packet:
Unwanted Source List    : 1000        Zero Max Resp Code      : 0
Fault Length            : 1000        Invalid Multicast Group : 0
Bad Checksum            : 0

IGMP Report invalid packet:
Fault Length            : 0           Invalid Multicast Group : 0
Invalid Multicast Source: 0           Bad Checksum            : 0
Illegal Report Type     : 0

IGMP Leave invalid packet:
Invalid Multicast Group : 0           Bad Checksum            : 0
------------------------------------------------------------------------------
```

Table 8-11 Description of the **display igmp invalid-packet** command output

Item	Description
Statistics of invalid packets for public net	Statistics of invalid IGMP messages in public network.
IGMP Query invalid packet	Number of invalid IGMP Query messages.
Unwanted Source List	Number of messages with unwanted source lists.

Item	Description
Zero Max Resp Code	Number of messages whose Max Resp Code field is 0.
Fault Length	Number of messages with invalid lengths.
Invalid Multicast Group	Number of messages with invalid group addresses.
Bad Checksum	Number of messages with checksum errors.
IGMP Report invalid packet	Number of invalid IGMP Report messages.
Invalid Multicast Source	Number of messages with invalid multicast source addresses.
Illegal Report Type	Number of IGMP Report messages of invalid types.
IGMP Leave invalid packet	Number of invalid IGMP Leave messages.

Display details of one invalid recently received IGMP message.

```
<HUAWEI> display igmp invalid-packet 1 verbose
      Detailed information of invalid packets
-------------------------------------------------------
Packet information (Index 6):
-------------------------------------------------------
Interface          :  Vlanif100
Time               :  2010-06-09 11:03:51 UTC-08:00
Message Length     :  24
Invalid Type       :  Invalid Multicast Group
0000: 16 3c 00 00 01 34 04 04
-------------------------------------------------------
```

Table 8-12 Description of the **display igmp invalid-packet 1 verbose** command output

Item	Description
Detailed information of invalid packets	Details about the invalid IGMP message.
Packet information (Index 6)	Sequence number of the invalid IGMP message, which is numbered in the opposite order in which the message is received.
Interface	Interface receiving invalid IGMP messages.

Item	Description
Time	Time when the invalid IGMP message is received, in any of the following formats: ● YYYY-MM-DD HH:MM:SS ● YYYY-MM-DD HH:MM:SS UTC±HH:MM DST ● YYYY-MM-DD HH:MM:SS UTC±HH:MM ● YYYY-MM-DD HH:MM:SS DST UTC±HH:MM indicates that a time zone is configured using the **clock timezone** command; DST indicates that the daylight saving time is configured using **clock daylight-saving-time** command.
Message Length	Length of the invalid IGMP message.
Invalid Type	Type of the invalid IGMP message.
0000: 16 3c 00 00 01 34 04 04	Contents of the invalid IGMP message.

8.1.10 display igmp proxy group

Function

The **display igmp proxy group** command displays information about IGMP proxy groups.

Format

display igmp proxy [**vpn-instance** *vpn-instance-name* | **all-instance**] **group** [*group-address*] [**interface** *interface-type interface-number*] [**verbose**]

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Displays information about IGMP proxy groups in a specific VPN instance.	The value must be an existing VPN instance name.
all-instance	Displays information about IGMP proxy groups in all VPN instances.	-

Parameter	Description	Value
group-address	Specifies a multicast group address. If you specify *group-address* in this command, the command displays information about a specified multicast group.	The value ranges from 224.0.1.0 to 239.255.255.255, in dotted decimal notation.
interface *interface-type interface-number*	Displays information about IGMP proxy groups in the specified instances.	-
verbose	Displays detailed information about IGMP proxy groups. If you specify **verbose** in this command, the command displays status parameters of IGMP groups.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

To check the status of an IGMP proxy group or find out the cause of a fault in an IGMP proxy group, run the **display igmp proxy group** command.

Example

Display information about IGMP proxy groups.

```
<HUAWEI> display igmp proxy group
Interface group report information
   Vlanif100(10.1.6.2):
    Total 2 IGMP proxy Groups
     Group Address   Filter mode
     225.1.1.1       exclude
     225.1.1.2       include
```

Display details of IGMP proxy groups.

```
<HUAWEI> display igmp proxy group verbose
Interface group report information
      Vlanif100(10.1.6.2):
       Total 2 IGMP proxy Groups
       Group: 225.1.1.1
         Filter mode: exclude
         Query Response Expiry: 00:00:02
         Source list (total 1 source)
           Source: 2.1.1.1
       Group: 225.1.1.2
         Filter mode: include
         Query Response Expiry: off
         Source list (total 1 source)
           Source: 2.1.1.2
```


Table 8-13 Description of the **display igmp proxy group** command output

Item	Description
Interface group report information	-
Vlanif100(10.1.6.2)	Interface type and interface number (IP address).
Total 2 IGMP proxy Groups	Total two IGMP proxy groups on an interface.
Group Address	Multicast group address.
Filter mode	Filter mode of a group, which can be exclude or include.
Query Response Expiry	Amount of time before the query response time expires.
Source list (total 1 source)	Multicast source list (number of sources in the source list).
Source	Multicast source address.
Group	Multicast group address.

8.1.11 display igmp proxy interface

Function

The **display igmp proxy interface** command displays information about IGMP proxy interfaces.

Format

display igmp proxy [**vpn-instance** *vpn-instance-name* | **all-instance**] **interface** [*interface-type interface-number*]

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Displays information about IGMP proxy interfaces in a specific VPN instance. If neither **vpn-instance** nor **all-instance** is specified, the command displays only IGMP proxy interfaces in the public network instance.	The value must be an existing VPN instance name.
all-instance	Displays information about IGMP proxy interfaces in all VPN instances.	-
interface-type interface-number	Displays information about IGMP proxy interfaces in a specific interface.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

To check the status of an IGMP proxy interface or find out the cause of a fault in an IGMP proxy interface, run the **display igmp proxy interface** command.

Example

Display information about IGMP proxy interfaces.

```
<HUAWEI> display igmp proxy interface
Interface information of VPN-Instance: public net
 Vlanif100(192.168.1.2):
   IGMP proxy is enabled
   Current IGMP proxy version (negotiated) is 2
   Current IGMP proxy version (configured) is 2
   IGMP proxy state: up
   Value of query interval for IGMP (negotiated): 60 s
   Value of query interval for IGMP (configured): 60 s
   Value of querier present timeout for IGMPv1: off
   Value of querier present timeout for IGMPv2: 168 s
   Value of querier present timeout for IGMPv3: 124 s
   General query response expiry: off
   Querier for IGMP: 192.168.1.1
   Robustness (negotiated): 3
   Robustness (configured): 3
   Require-router-alert: disabled
   Send-router-alert: enabled
   Ip-source-policy: disabled
   Query ip-source-policy: 2000
   TTL-check: disabled
```


Table 8-14 Description of the **display igmp proxy interface** command output

Item	Description
Interface information of VPN-Instance: public net	VPN instance to which IGMP proxy interface information belongs. **public net** indicates the public network instance.
Vlanif100(192.168.1.2)	Interface type and interface number (IP address).
IGMP proxy is enabled	IGMP proxy is enabled on the interface.
Current IGMP proxy version (negotiated) is	Negotiated IGMP version on the IGMP proxy interface .
Current IGMP proxy version (configured) is	Configured IGMP version on the IGMP proxy interface.
IGMP proxy state	Status of the IGMP proxy interface, which can be Up or Down.
Value of query interval for IGMP (negotiated)	Query interval negotiated between the query interval configured on the IGMP proxy interface and the query interval carried in a Query message, in seconds. Only IGMPv3 Query messages carry this field. This field takes effect only in IGMPv3.
Value of query interval for IGMP (configured)	Interval at which the IGMP proxy interface sends IGMP Query messages, in seconds.
Value of querier present timeout for IGMPv1	Timeout period of an IGMPv1 querier.
Value of querier present timeout for IGMPv2	Timeout period of an IGMPv2 querier.
Value of querier present timeout for IGMPv3	Timeout period of an IGMPv3 querier.
General query response expiry	Timeout period of a general group query timer.
Querier for IGMP	Address of an IGMP querier. In IGMPv1, a querier is selected based on a multicast routing protocol; in IGMPv2 and IGMPv3, the switch with the lowest IP address acts as the querier on the shared network segment. If no querier exists, this field is displayed as "-".
Robustness (negotiated)	Robustness variable negotiated between the robustness variable configured on an IGMP proxy interface and the robustness variable carried in a Query message. This field takes effect only in IGMPv3.

Item	Description
Robustness (configured)	Robustness variable configured on the IGMP proxy interface.
Require-router-alert	Whether the switch discards IGMP packets that do not contain the Router-Alert option in IP packet headers. ● enable: The switch discards IGMP packets that do not contain the Router-Alert option in IP packet headers. ● disable: The switch does not discard IGMP packets that do not contain the Router-Alert option in IP packet headers. This function is configured using the **igmp require-router-alert** command.
Send-router-alert	Whether the switch sends IGMP packets with the Router-Alert option. ● enabled: The switch sends IGMP packets with the Router-Alert option. ● disabled: The switch sends IGMP packets without the Router-Alert option. This function is configured using the **igmp send-router-alert** command.
Ip-source-policy	Whether to filter IGMP Report/Leave messages based on host addresses. ● enabled: The switch filters IGMP Report/Leave messages based on host addresses. ● disabled: The switch does not filter IGMP Report/Leave messages based on host addresses. This function is configured using the **igmp ip-source-policy** command.
Query ip-source-policy	Whether to filter IGMP Query messages based on source addresses. ● enabled: The switch filters IGMP Query messages based on source addresses. ● disabled: The switch does not filter IGMP Query messages based on source addresses. This function is configured using the **igmp query ip-source-policy** command.

Item	Description
TTL-check	Whether the function to check the TTL values in received IGMP Report, Leave, and Query messages is enabled: • enabled • disabled This function is configured using the **igmp ttl-check** command.

8.1.12 display igmp proxy routing-table

Function

The **display igmp proxy routing-table** command displays information about an IGMP proxy routing table.

Format

display igmp proxy [**vpn-instance** *vpn-instance-name* | **all-instance**] **routing-table** [*group-address* [**mask** { *group-mask-length* | *group-mask* }] | *source-address* [**mask** { *source-mask-length* | *source-mask* }] | **outgoing-interface** { **include** | **exclude** | **match** } { *interface-type interface-number* | **none** } | **incoming-interface** *interface-type interface-number* | **flags** *flag-value* | **fsm**] * [**outgoing-interface-number** [*number*]]

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Displays information about an IGMP proxy routing table in a specific VPN instance. If you specify neither **vpn-instance** nor **all-instance** in this command, the command displays only the IGMP proxy routing table in the public network instance.	The value must be an existing VPN instance name.
all-instance	Displays information about IGMP proxy routing tables in all VPN instances.	-

Parameter	Description	Value
group-address	Displays information about the routing entry of a specified group.	The value ranges from 224.0.1.0 to 239.255.255.255, in dotted decimal notation.
mask	Indicates the mask of a multicast group address or a source address.	-
group-mask-length	Specifies the mask length of a multicast group address.	The value is an integer that ranges from 4 to 32.
group-mask	Specifies the mask of a multicast group address.	The value is in dotted decimal notation.
source-address	Displays the routing entry for a multicast source.	The value is in dotted decimal notation.
source-mask-length	Specifies the mask length of a multicast source address.	The value is an integer that ranges from 0 to 32.
source-mask	Specifies the mask of a multicast source address.	The value is in dotted decimal notation.
outgoing-interface	Displays the routing entries with a specific interface as the outbound interface.	-
include	Displays the routing entries of which the downstream interface list has a specific interface.	-
exclude	Displays the routing entries of which the downstream interface list does not have a specific interface.	-
match	Displays the routing entries of which the downstream interface list has only a specific interface.	-
interface-type interface-number	Specifies the type and number of an interface.	-

Parameter	Description	Value
none	Displays the routing entries with an empty downstream interface list.	-
incoming-interface	Displays the routing entries with a specific interface as the inbound interface.	-
flags *flag-value*	Indicates an IGMP proxy routing entry with a specific type. *flag-value* specifies the flag of a routing entry. If you specify **flags** *flag-value* in this command, the command displays IGMP proxy routing entries with the flag.	*flag-value* can be act, del, join, none, niif, sgjoin, wcjoin, upchg, or wc. For information about each value, see the flag-value field description in the **display pim routing-table** command output.
fsm	Displays detailed information about a finite state machine (FSM).	-
outgoing-interface-number	Displays the number of downstream interfaces in an IGMP proxy routing entry.	-
number	Specifies the number of downstream interfaces in an entry to be queried.	The value is an integer that ranges from 0 to 2048.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

To find information about an IGMP proxy routing table, run the **display igmp proxy routing-table** command. You can specify different parameters in this command to view specific routing information. This command helps you find specific routes and locate faults.

Example

Display details of an FSM in an IGMP proxy routing table.

```
<HUAWEI> display igmp proxy routing-table fsm
Routing table
```



```
Total 1 (*, G) entry; 1 (S, G) entry

(*, 225.1.1.1)
    Flag: WC, UpTime: 6d:10h
    Upstream interface: Vlanif100
    Downstream interface(s) information:
    Total number of downstreams: 1
        1: Vlanif200
            Protocol: igmp, UpTime: 17:27:13
            IGMP querier: 10.1.1.1(this router)
            IGMP state: EXCLUDE

    FSM information for non-downstream interfaces: None

(10.3.3.100, 225.1.1.1)
    Flag: JOIN ACT, UpTime: 6d:17h
    Upstream interface: GigabitEthernetVlanif100
    Downstream interface(s) information:
    Total number of downstreams: 1
        1: Vlanif200
            Protocol: igmp, UpTime: 17:27:13
            IGMP querier: 10.1.1.1(this router)
            IGMP state: NI

    FSM information for non-downstream interfaces: None
```

Table 8-15 Description of the **display igmp proxy routing-table fsm** command output

Item	Description
Routing table	-
Total 1 (*, G) entry; 1 (S, G) entry	Total number of (*, G) and (S, G) entries in the IGMP proxy routing table.
(*, 225.1.1.1)	(*, G) or (S, G) entry in the IGMP proxy routing table.
Flag	Flag of a (*, G) or an (S, G) entry in the IGMP proxy routing table.
UpTime	Amount of time since a (*, G) or an (S, G) entry is created.
Upstream interface	Upstream interface of a (*, G) or an (S, G) entry.
Downstream interface(s) information	Information about downstream interfaces.
Total number of downstreams	Total number of downstream interfaces.
Vlanif200	Name of a downstream interface.
Protocol	Protocol of a downstream interface.

Item	Description
UpTime	Amount of time a downstream interface has been in Up state, expressed in hh:mm:ss format. The time format is as follows: • If the time is shorter than or equal to 24 hours, the format is hours:minutes:seconds. • If the time is longer than 24 hours but shorter than or equal to one week, the format is days:hours. • If the time is longer than one week, the format is weeks:days.
IGMP querier	Address of an IGMP querier
IGMP state	IGMP status on a downstream interface: • NI: indicates that an (S, G) entry inherits the downstream interfaces of a (*, G) entry. • BLOCK: indicates that the interface does not forward traffic based on an (S, G) entry. • INCLUDE: indicates that the interface needs to join the specified group and source. • EXCLUDE: indicates that the interface does not join the specified group and source.
FSM information for non-downstream interfaces	Interfaces that do not forward multicast data packets matching (*, G) or (S, G) entries.

8.1.13 display igmp routing-table

Function

The **display igmp routing-table** command displays the IGMP routing table.

Format

display igmp [**vpn-instance** *vpn-instance-name* | **all-instance**] **routing-table** [*group-address* [**mask** { *group-mask* | *group-mask-length* }] | *source-address* [**mask** { *source-mask* | *source-mask-length* }]] * [**static**] [**outgoing-interface-number** [*number*]]

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Displays IGMP routing information in a specified VPN instance.	The value must be an existing VPN instance name.
all-instance	Displays IGMP routing information in all instances.	-
group-address	Displays IGMP routing information of a specified multicast group.	The address is in dotted decimal notation and ranges from 224.0.1.0 to 239.255.255.255.
mask	Indicates the mask of a multicast group address or a multicast source address.	-
group-mask	Specifies the mask of a multicast group address.	It is in dotted decimal notation.
group-mask-length	Specifies the mask length of a multicast group address.	The value is an integer that ranges from 4 to 32.
source-address	Displays IGMP routing information of a specified multicast source.	It is in dotted decimal notation.
source-mask	Specifies the mask of a multicast source address.	It is in dotted decimal notation.
source-mask-length	Specifies the mask length of a multicast source address.	The value is an integer that ranges from 0 to 32.
static	Displays static IGMP routing entries.	-
outgoing-interface-number	Displays the number of the outbound interfaces in IGMP routing entries.	-
number	Specifies the number of outbound interfaces. If this parameter is specified, the command displays the specified number of outbound interfaces.	The value is an integer that ranges from 1 to 2048.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The **display igmp routing-table** command provides IGMP routing information. You can specify different parameters to view specific IGMP routing information and locate faults.

NOTE

This command provides output information only when PIM is not enabled on the IGMP-capable interface.

Example

Display the IGMP routing table.

```
<HUAWEI> display igmp routing-table
Routing table
 Total 2 entries

 00001. (10.10.10.10, 232.1.1.3)
      List of 1 downstream interface in include mode
       Vlanif100 (10.20.20.1),
                Protocol: SSM-MAP

 00002. (*, 225.1.1.1)
      List of 1 downstream interface
       Vlanif100 (10.20.20.1),
                Protocol: IGMP
```

Table 8-16 Description of the **display igmp routing-table** command output

Item	Description
Routing table	IGMP routing table.
Total 2 entries	Total number of IGMP routing entries.
00001. (10.10.10.10, 232.1.1.3)	Entry 00001. (S, G) indicates that data is transmitted from S to G. (*, G) indicates that data is transmitted from any source to G.
List of 1 downstream interface in include mode	List of the downstream interfaces that join the multicast group in INCLUDE mode.
Vlanif100 (10.20.20.1)	Interface type and interface number (IP address).
Protocol	Protocol type, including: • SSM-MAP: Entries are generated using SSM mapping. • IGMP: Entries are generated using IGMP. • STATIC: Entries are generated by configuring static IGMP groups.

8.1.14 display igmp ssm-mapping

Function

The **display igmp ssm-mapping** command displays configuration of IGMP SSM mapping.

Format

display igmp [**vpn-instance** *vpn-instance-name* | **all-instance**] **ssm-mapping** { **group** [*group-address*] | **interface** [*interface-type interface-number*] }

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Displays SSM mapping entries in a specified VPN instance.	The value must be an existing VPN instance name.
all-instance	Displays SSM mapping entries in all instances.	-
group [*group-address*]	Displays the SSM mapping entries of a specified group. If *group-address* is not specified, the command displays SSM mapping entries of all groups.	The value ranges from 224.0.1.0 to 239.255.255.255, in dotted decimal notation.
interface [*interface-type interface-number*]	Displays whether SSM mapping is enabled on a specified interface. If *interface-type interface-number* is not specified, the command displays all the interfaces that are in Up state and have SSM mapping enabled.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

This command displays mapping between multicast groups and multicast sources configured using the **ssm-mapping** command. You can also use this command to check the SSM mapping configuration on an interface. To enable SSM mapping on an interface, run the **igmp ssm-mapping enable** command in the interface view.

Example

Display SSM mapping entries of all the multicast sources and multicast groups.

```
<HUAWEI> display igmp ssm-mapping group
IGMP SSM-Mapping conversion table
 Total 2 entries    2 entries matched

 00001. (10.1.0.2, 225.1.1.0/24)

 00002. (10.1.0.2, 239.255.255.0/24)

 Total 2 entries matched
```

Table 8-17 Description of the **display igmp ssm-mapping group** command output

Item	Description
IGMP SSM-Mapping conversion table	IGMP SSM mapping table.
Total 2 entries 2 entries matched	Total number of SSM mapping entries and total number of entries matching the query conditions.
00001. (10.1.0.2, 225.1.1.0/24) 00002. (10.1.0.2, 239.255.255.0/24)	Number of an (S, G) entry.
Total 2 entries matched	Number of SSM mapping entries matching the query conditions.

Display whether IGMP SSM mapping is enabled on VLANIF100.

```
<HUAWEI> display igmp ssm-mapping interface vlanif 100
IGMP SSM-Mapping is enabled
```

Table 8-18 Description of the display igmp ssm-mapping interface vlanif 100 command output

Item	Description
IGMP SSM-Mapping is enabled	SSM mapping is enabled on the interface.

8.1.15 igmp

Function

The **igmp** command displays the IGMP view.

The **undo igmp** command deletes all configurations in the IGMP view.

Format

igmp [**vpn-instance** *vpn-instance-name*]

undo igmp [**vpn-instance** *vpn-instance-name*]

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Specifies the name of a VPN instance.	The value must be an existing VPN instance name.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Global IGMP parameters must be configured in the IGMP view.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command.

Precautions

NOTE

Running the **undo igmp** command in the system view may interrupt IGMP services and deletes all global IGMP configurations of the public network instance. To restore the IGMP function, you have to re-run the deleted commands.

Example

Enter the IGMP view.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] igmp
[HUAWEI-igmp]
```

8.1.16 igmp enable

Function

The **igmp enable** command enables IGMP on an interface.

The **undo igmp enable** command disables IGMP on an interface.

By default, IGMP is disabled on an interface.

Format

igmp enable

undo igmp enable

Parameters

None

Views

GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, GE sub-interface view, XGE sub-interface view, MultiGE sub-interface view, 25GE sub-interface view, 40GE sub-interface view, 100GE sub-interface view, Eth-Trunk sub-interface view, VLANIF interface view, loopback interface view, VBDIF interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

User hosts and Layer 3 multicast devices directly connected to user network segments must run IGMP. A multicast device can process IGMP messages sent from user hosts only after IGMP is enabled on the interfaces connected to user network segments.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command.

If IGMPv1 is run on an interface, you must enable **pim dm** or **pim sm**. This is because IGMPv1 does not the querier election. In IGMPv1, the querier is specified by Protocol Independent Multicast (PIM).

If IGMPv2/v3 is run on an interface, **pim dm** or **pim sm** is recommended. Although IGMPv2/v3 supports the querier election, enabling PIM improves the system stability.

Precautions

- If PIM and IGMP need to be enabled on the same interface, enable PIM, and then IGMP.
- If IGMP parameters are configured on an interface, the parameter settings take effect only after IGMP is enabled.
- Running the **igmp enable** command failed on the VLANIF interface because Layer 2 multicast querier or report-suppress is enabled for this VLAN.

- When Layer 2 and Layer 3 multicast are both deployed, pay attention to the following points:
  - If both Layer 2 and Layer 3 multicast services are required in a VLAN, enable IGMP on the corresponding VLANIF interface first, and then enable IGMP snooping in the VLAN. If IGMP snooping is enabled in the VLAN first, IGMP cannot be enabled on the VLANIF interface.
  - If Layer 2 and Layer 3 multicast are both configured in a VLAN, you must delete the Layer 2 multicast configuration before you can modify or delete the Layer 3 multicast configuration. This means that you must disable IGMP snooping in the VLAN first, then modify or disable the IGMP and PIM (IPv4) configuration in the VLANIF interface view, and finally enable IGMP snooping in the VLAN. Otherwise, the Layer 3 multicast configuration cannot be modified or deleted on the corresponding VLANIF interface.
  - If a VLANIF interface is shut down in the VLANIF interface view, Layer 2 multicast in the corresponding VLAN becomes ineffective accordingly. To make Layer 2 multicast effective, you must disable IGMP snooping in the VLAN first, then disable IGMP and PIM (IPv4) in the VLANIF interface view, and finally enable IGMP snooping in the VLAN.
  - When both Layer 2 and Layer 3 multicast services are configured, traffic is forwarded based on Layer 3 multicast forwarding entries instead of Layer 2 multicast forwarding entries. This means that Layer 2 multicast provides physical outbound interfaces for Layer 3 multicast, implementing accurate forwarding of multicast data. In addition, the maximum number of Layer 3 multicast forwarding entries depends on the maximum number of Layer 2 multicast forwarding entries.

Example

Enable IGMP on VLANIF100 connected to a user network segment.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] igmp enable
```

Enable IGMP on GE0/0/1 connected to a user network segment.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] igmp enable
```

8.1.17 igmp global limit

Function

The **igmp global limit** command sets the maximum number of IGMP entries that can be created on the switch.

The **undo igmp global limit** command deletes the configured maximum number of IGMP entries.

The following lists the maximum number of IGMP entries allowed on each model by default:

- S5720-LI, S5720S-LI: 1022
- S5731-S, S5731S-S, S5720I-SI: 1024
- S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735S-S, S5735-S-I: 1500
- S5735S-H, S5736-S, S6720S-S: 1536
- S6730-S, S6730S-S: 4096
- S5731-H, S5731S-H, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H: 8192

Format

igmp global limit *number*

undo igmp global limit

Parameters

Parameter	Description	Value
number	Specifies the maximum number of IGMP entries that can be created on the switch.	The value is an integer that ranges from 1 to *The maximum number of IGMP entries allowed by default*. **NOTE** The value range of S5731-H, S5731S-H, S5732-H, S6730S-H, and S6730-H are expanded after the high specification mode is configured for multicast forwarding using the **set multicast forwarding-table super-mode** command. The actual value range depends on the specification of the device.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the number of IGMP entries reaches the limit, the system does not create any new IGMP entries. To enable the switch to create new IGMP entries, delete unnecessary entries or increase the limit. Alternatively, you can configure static IGMP entries or source-groups.

The number of IGMP entries is counted as follows:

- Each (*, G) entry is counted as one entry.
- Each (S, G) entry is counted as one entry.

- Each (*, G) entry established with SSM mapping is counted as one entry.

Precautions

You can also run the **limit (IGMP view)** command in the IGMP view to set the maximum number of IGMP group memberships in the system. If both the **igmp global limit** and **limit (IGMP view)** commands are run, the smaller value takes effect.

Example

Set the maximum number of IGMP entries that can be created on the switch to 248.

```
<HUAWEI> system-view
[HUAWEI] igmp global limit 248
```

8.1.18 igmp group-policy

Function

The **igmp group-policy** command configures an IGMP group policy on an interface to limit the range of multicast groups that the hosts can join.

The **undo igmp group-policy** command deletes the IGMP group policy.

By default, no IGMP group policy is configured on an interface, and the hosts can join any multicast groups.

Format

igmp group-policy *acl-number* [**1** | **2** | **3**]

undo igmp group-policy

Parameters

Parameter	Description	Value
acl-number	Specifies the number of a basic ACL or an advanced ACL. The ACL defines a multicast group range.	The number of a basic ACL is an integer that ranges from 2000 to 2999. The number of an advanced ACL ranges from 3000 to 3999.
1	Sets the range of multicast groups that IGMPv1 hosts can join.	-
2	Sets the range of multicast groups that IGMPv2 hosts can join.	-
3	Sets the range of multicast groups that IGMPv3 hosts can join.	-

Views

GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, GE sub-interface view, XGE sub-interface view, MultiGE sub-interface view, 25GE sub-interface view, 40GE sub-interface view, 100GE sub-interface view, Eth-Trunk sub-interface view, VLANIF interface view, loopback interface view, VBDIF interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To control the multicast groups that hosts on the network attached to an interface can join, specify an ACL in the **igmp group-policy** command on the interface. This configuration improves security of the IGMP application. You can also use this command to prevent the switch from receiving Join messages for specified groups.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command.

Precautions

- Before running the **igmp group-policy** command, run the **acl** command to configure the ACL that you want to apply to the group policy to limit the range of multicast groups that hosts connected to the interface can join.
  - In the basic ACL view, set **source** in the **rule** command to the range of multicast groups that an interface can join.
  - In the advanced ACL view, set **source** in the **rule** command to the source address that is allowed to send multicast data to the specified multicast groups, and set **destination** to the range of multicast groups that an interface can join.
- After the **igmp group-policy** command is executed on an interface:
  - The interface filters the received Report messages based on the ACL and maintains memberships only for the multicast groups permitted by the ACL.
  - The interface discards the Report messages that are denied by the ACL. If the entries of the multicast groups denied by the ACL exist on the switch, the switch deletes these entries when the aging time of the entries expires.
  - If the IGMP version is not specified, the specified ACL applies to IGMPv1, IGMPv2, and IGMPv3 hosts.

Example

Create ACL 2005, and configure a rule that allows hosts to receive data of multicast group 225.1.1.1. Configure an IGMP group policy on VLANIF100 and

reference ACL 2005 to allow hosts connected to the interface to join only multicast group 225.1.1.1.

```
<HUAWEI> system-view
[HUAWEI] acl number 2005
[HUAWEI-acl-basic-2005] rule permit source 225.1.1.1 0
[HUAWEI-acl-basic-2005] quit
[HUAWEI] multicast routing-enable
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] igmp group-policy 2005
```

Create ACL 2005, and configure a rule that allows hosts to receive data of multicast group 225.1.1.1. Configure an IGMP group policy on GE0/0/1 and reference ACL 2005 to allow hosts connected to the interface to join only multicast group 225.1.1.1.

```
<HUAWEI> system-view
[HUAWEI] acl number 2005
[HUAWEI-acl-basic-2005] rule permit source 225.1.1.1 0
[HUAWEI-acl-basic-2005] quit
[HUAWEI] multicast routing-enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] igmp group-policy 2005
```

8.1.19 igmp ip-source-policy

Function

The **igmp ip-source-policy** command enables filtering of IGMP Report/Leave messages based on source addresses.

The **undo igmp ip-source-policy** command disables filtering of IGMP Report/Leave messages based on source addresses.

By default, the switch does not filter IGMP Report/Leave messages based on source addresses.

Format

igmp ip-source-policy [*basic-acl-number*]

undo igmp ip-source-policy

Parameters

Parameter	Description	Value
basic-acl-number	Specifies the number of a basic ACL, which defines the range of source addresses.	The value is an integer that ranges from 2000 to 2999.

Views

GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, GE sub-interface view, XGE sub-interface view, MultiGE sub-interface view, 25GE sub-interface view, 40GE sub-interface view, 100GE sub-interface view, Eth-Trunk sub-

interface view, VLANIF interface view, loopback interface view, VBDIF interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

IGMP runs on member hosts and their directly connected multicast devices. A multicast device processes all received Report/Leave messages. For security purposes, you can configure the multicast device to filter Report/Leave messages received on an interface.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command.

Precautions

IGMP Report/Leave messages are encapsulated in IP packets. The **igmp ip-source-policy** command configures the switch to check the source address in the IP header of each received Report/Leave message. The switch filters Report/Leave messages based on the following rules (if ACL rules are not configured):

- If the source IP address of a Report/Leave message is 0.0.0.0 or on the same network segment as the IP address of the inbound interface, the switch processes the Report/Leave message.
- If the source IP address of a Report/Leave message is on a different network segment than the IP address of the inbound interface, the switch discards the Report/Leave message.

If you have specified an ACL rule, the interface filters out the IGMP Report/Leave messages whose source addresses do not match the ACL rule.

The **igmp ip-source-policy** command works with the **acl** command. For a numbered ACL, you can configure the source address of IGMP messages by specifying the **source** parameter in the **rule** command in the basic ACL view.

Example

Enable filtering of IGMP Report/Leave messages based on source addresses on VLANIF100.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] igmp ip-source-policy
```

Configure VLANIF100 to accept the IGMP Report/Leave messages with the source address 10.10.1.1.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] acl number 2001
[HUAWEI-acl-basic-2001] rule permit source 10.10.1.1 0
[HUAWEI-acl-basic-2001] quit
```



```
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] igmp ip-source-policy 2001
```

Enable filtering of IGMP Report/Leave messages based on source addresses on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] igmp ip-source-policy
```

8.1.20 igmp lastmember-queryinterval

Function

The **igmp lastmember-queryinterval** command configures interval at which an IGMP querier interface sends IGMP Group-Specific Query messages or IGMP Group-and-Source-Specific Query messages after receiving IGMP Leave messages from hosts.

The **undo igmp lastmember-queryinterval** command restores the default value.

By default, the interval at which an IGMP querier interface sends IGMP Group-Specific Query messages or IGMP Group-and-Source-Specific Query messages is 1s.

Format

igmp lastmember-queryinterval *interval*

undo igmp lastmember-queryinterval

Parameters

Parameter	Description	Value
interval	Specifies the interval at which an IGMP querier sends IGMP Group-Specific Query messages or IGMP Group-and-Source-Specific Query messages.	The value is an integer that ranges from 1 to 5, in seconds.

Views

GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, GE sub-interface view, XGE sub-interface view, MultiGE sub-interface view, 25GE sub-interface view, 40GE sub-interface view, 100GE sub-interface view, Eth-Trunk sub-interface view, VLANIF interface view, loopback interface view, VBDIF interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When a querier receives a Leave message for a group, the querier periodically sends IGMP Group-Specific Query messages or IGMP Group-and-Source-Specific Query messages to check for other members in the group. The **igmp lastmember-queryinterval** command sets the interval at which the querier sends Last Member Query messages. The querier stops forwarding multicast data to the group if it receives no Report message from the group within the period specified by *interval* x *robust-value*. Here, *robust-value* is the robustness variable configured using the **igmp robust-count** or **robust-count** command.

If the querier receives at least one more Report message from the group within the specified period, the querier continues maintaining memberships of the group. Otherwise, the querier considers that the last member has left the group and no longer maintains memberships of the group.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command.

Precautions

- The **igmp lastmember-queryinterval** command is valid only when the IGMP querier runs IGMPv2 or IGMPv3.
- The **igmp lastmember-queryinterval** command has the same function as the **lastmember-queryinterval** command used in the IGMP view. The configuration in the IGMP view takes effect for all interfaces, whereas the configuration in the interface view takes effect only for the specified interface. The configuration in the interface view takes precedence over the configuration in the IGMP view. The configuration in the IGMP view is used only when no configuration is performed in the interface view.

Example

Set the interval for sending IGMP Group-Specific Query messages or IGMP Group-and-Source-Specific Query messages to 3 seconds on VLANIF100.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] igmp lastmember-queryinterval 3
```

Set the interval for sending IGMP Group-Specific Query messages or IGMP Group-and-Source-Specific Query messages to 3 seconds on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] igmp lastmember-queryinterval 3
```


8.1.21 igmp limit

Function

The **igmp limit** command sets the maximum number of IGMP group memberships allowed on an interface.

The **undo igmp limit** command restores the maximum number of IGMP group memberships allowed on an interface to the default value.

The following lists the maximum number of IGMP group memberships allowed on an interface of each model by default:

- S5720-LI, S5720S-LI: 1022
- S5731-S, S5731S-S, S5720I-SI: 1024
- S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735S-S, S5735-S-I: 1500
- S5735S-H, S5736-S, S6720S-S: 1536
- S6730-S, S6730S-S, S5731-H, S5731S-H, S5732-H, S6730-H, S6730S-H: 2048
- S6720S-EI, S6735-S, S6720-EI: 4096

Format

igmp limit *number* [**except** *acl-number*]

undo igmp limit

Parameters

Parameter	Description	Value
number	Specifies the maximum number of IGMP group memberships allowed on an interface.	The value is an integer that ranges from 1 to *The maximum number of IGMP group memberships allowed on an interface by default.* **NOTE** The value range of S5731-H, S5731S-H, S5732-H, S6730S-H, and S6730-H are expanded after the high specification mode is configured for multicast forwarding using the **set multicast forwarding-table super-mode** command. The actual value range depends on the specification of the device.
except	Specifies the range of multicast groups whose IGMP entries are not limited by the IGMP limit.	-

Parameter	Description	Value
acl-number	Specifies a basic ACL or an advanced ACL.	The value is an integer. The basic ACL number ranges from 2000 to 2999. A basic ACL filters group addresses only. The advanced ACL number ranges from 3000 to 3999. An advanced ACL filters (S, G) entries as well as group addresses.

Views

GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, GE sub-interface view, XGE sub-interface view, MultiGE sub-interface view, 25GE sub-interface view, 40GE sub-interface view, 100GE sub-interface view, Eth-Trunk sub-interface view, VLANIF interface view, loopback interface view, VBDIF interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the number of IGMP entries reaches the limit, the system does not create any IGMP entries. To allow the switch to create more IGMP entries, delete useless entries or increase the limit. Alternatively, you can configure static IGMP entries.

The number of IGMP entries is counted as follows:

- Each (*, G) entry is counted as one entry.
- Each (S, G) entry is counted as one entry.
- Each (*, G) entry for SSM mapping is counted as one entry.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command.

Precautions

If **except** is not specified in the command, the maximum number of all dynamic IGMP (*, G) or (S, G) entries is the configured IGMP limit. Before setting **except**, configure the associated ACL. The interface then uses the ACL to filter the received IGMP Report messages. The number of entries corresponding to the multicast groups that match the ACL is not limited.

The **igmp limit** command must be used with ACL configuration commands. When configuring ACL rules, note that:

- In the basic ACL view, specify the **source** parameter in the **rule** command to set the range of multicast groups whose IGMP entries are not limited.

- In the advanced ACL view, specify the **source** parameter in the **rule** command to set the range of sources that send multicast data to the multicast groups. Specify the **destination** parameter to set the range of multicast groups whose IGMP entries are not limited.

Example

Set the maximum number of IGMP entries that can be created on the VLANIF100 to 220.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] igmp limit 220
```

Set the maximum number of IGMP entries that can be created on the GE0/0/1 to 220.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] igmp limit 220
```

8.1.22 igmp max-response-time

Function

The **igmp max-response-time** command sets the maximum response time for IGMP General Query messages on an interface.

The **undo igmp max-response-time** command restores the default maximum response time for General IGMP Query messages.

By default, the maximum response time for IGMP General Query messages is 10s on an interface.

Format

igmp max-response-time *interval*

undo igmp max-response-time

Parameters

Parameter	Description	Value
interval	Specifies the maximum response time for IGMP General Query messages.	The value is an integer that ranges from 1 to 25, in seconds.

Views

GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, GE sub-interface view, XGE sub-interface view, MultiGE sub-interface view, 25GE sub-interface view, 40GE sub-interface view, 100GE sub-interface view, Eth-Trunk sub-

interface view, VLANIF interface view, loopback interface view, VBDIF interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If hosts send IGMP Report messages immediately after they receive IGMP General Query messages, the querier on a shared network segment may receive a large number of Report messages sent from many hosts at the same time. This may cause congestion on the network.

To avoid such situations, IGMPv2 and IGMPv3 messages specify the maximum response time for IGMP General Query messages. When a host running IGMPv2 or IGMPv3 receives an IGMP General Query message, it starts a timer for the group it wants to join. The timer length is a random value between 0 and the maximum response time. When the timer times out, the host sends a Report message.

The maximum response time specifies the deadline for the host to send a Report message. An appropriate maximum response time allows hosts to respond to Query messages quickly and prevents hosts from sending Report messages at the same time.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command.

Precautions

- This command is valid only for IGMPv2 and IGMPv3.
- A shorter response time allows a multicast device to obtain multicast group member information more quickly, but consumes more bandwidth and system resources.
- The **igmp max-response-time** command has the same function as the **max-response-time** command used in the IGMP view. The configuration in the IGMP view takes effect for all interfaces, whereas the configuration in the interface view takes effect only for the specified interface. The configuration in the interface view takes precedence over the configuration in the IGMP view. The configuration in the IGMP view is used only when no configuration is performed in the interface view.

Example

Set the maximum response time for IGMP General Query messages to 8 seconds on VLANIF100.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] igmp max-response-time 8
```


Set the maximum response time for IGMP General Query messages to 8 seconds on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] igmp max-response-time 8
```

8.1.23 igmp on-demand

Function

The **igmp on-demand** command enables the IGMP on-demand function. This function enables a querier to maintain group memberships according to requirements of group members, without sending Query messages. After IGMP on-demand is enabled on an interface, dynamic IGMP entries on the interface will never age out.

The **undo igmp on-demand** command restores the default configuration.

By default, a querier does not maintain group memberships according to requirements of group members, and dynamic entries are aged out when the aging time expires.

Format

igmp on-demand

undo igmp on-demand

Parameters

None

Views

GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, VLANIF interface view, loopback interface view, VBDIF interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In a standard IGMP working process, a querier sends General Query messages periodically and collects group membership information based on received Report and Leave messages. Multicast group members respond to every Query message they receive. After IGMP on-demand is configured on the querier, the querier does not send Query messages, reducing IGMP packets exchanged between the querier and member hosts.

The IGMP on-demand function enables a querier to maintain group memberships based on requirements of members, without sending Query messages.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command.

Precautions

- IGMP on-demand applies only to IGMPv2 and IGMPv3.
- This command cannot be configured on a VLANIF interface if IGMP snooping is enabled in the VLAN corresponding to the VLANIF interface.
- If dynamic IGMP entries have been generated on the querier, run the **reset igmp group** command to clear these dynamic IGMP entries before running the **igmp on-demand** command.
- After the **igmp on-demand** command is executed on an interface (IGMP querier):
  - The interface does not send IGMP Query messages
  - IGMP group entries are generated after the interface receives IGMP Report messages and will never age out.
  - When the interface receives an IGMP Leave message, it deletes the corresponding IGMP entry.

Example

Enable the IGMP on-demand function on VLANIF100.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] igmp on-demand
```

Enable the IGMP on-demand function on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] igmp on-demand
```

8.1.24 igmp prompt-leave

Function

The **igmp prompt-leave** command enables the fast leave function on an interface. This function enables an IGMP querier to delete IGMP entries immediately after receiving Leave messages from group members, without sending Group-Specific Query messages.

The **undo igmp prompt-leave** command disables fast leave on an interface.

By default, an IGMP querier sends a Group-Specific Query message after receiving a Leave message for a specific multicast group.

Format

igmp prompt-leave [**group-policy** *acl-number*]

undo igmp prompt-leave

Parameters

Parameter	Description	Value
group-policy	Specifies an IGMP group policy. If this parameter is specified, the fast leave function takes effect only for multicast groups specified in the policy. When specifying this parameter, ensure that the referenced ACL has been configured. The device filters Leave messages on the interface based on the ACL. • If a host leaves a multicast group in the range permitted by the ACL, the device immediately deletes the multicast group entry without sending a Group-Specific Query message. • If a host leaves a multicast group out of the range permitted by the ACL, the device sends a Group-Specific Query message. If this parameter is not specified, the fast leave function takes effect for all multicast groups.	-
acl-number	Specifies the number of a basic ACL or an advanced ACL. This ACL defines a range of multicast groups. The specified ACL is configured using the **acl** command.	The number of a basic ACL is an integer that ranges from 2000 to 2999. The number of an advanced ACL ranges from 3000 to 3999.

Views

GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, GE sub-interface view, XGE sub-interface view, MultiGE sub-interface view, 25GE sub-interface view, 40GE sub-interface view, 100GE sub-interface view, Eth-Trunk sub-interface view, VLANIF interface view, loopback interface view, VBDIF interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In some scenarios, a querier interface connects to only one receiver host. If the host frequently switches between multiple multicast groups, you can configure the fast leave function on the interface so that the interface can quickly respond to Leave messages sent from the host. After the fast leave function is configured, the querier does not send a Group-Specific Query message after receiving a Leave message. Instead, the querier directly notifies the upstream multicast device that the host has left the multicast group. The fast leave function reduces delay in response to Leave messages and saves network bandwidth.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command.

Precautions

- IGMP fast leave applies only to IGMPv2 and IGMPv3.
- When an interface has more than one receiver connected, enabling the fast leave function interrupts multicast traffic of the other receivers in the multicast group. It is recommended that you enable this function only on interfaces with one receiver.
- This command functions in the same way as the **prompt-leave** command used in the IGMP view, except that the configuration in the IGMP view is globally valid, whereas the configuration in the interface view is valid only for the specific interface. The configuration in the interface view takes precedence over the configuration in the IGMP view. The configuration in the IGMP view is used only when the configuration in the interface view is not done.

Example

Create ACL 2005 and configure a rule that allows hosts to fast leave multicast groups in the range of 225.1.0.0/16. Configure fast leave on VLANIF100.

```
<HUAWEI> system-view
[HUAWEI] acl number 2005
[HUAWEI-acl-basic-2005] rule permit source 225.1.0.0 0.0.255.255
[HUAWEI-acl-basic-2005] quit
[HUAWEI] multicast routing-enable
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] igmp prompt-leave group-policy 2005
```

Create ACL 2005 and configure a rule that allows hosts to fast leave multicast groups in the range of 225.1.0.0/16. Configure fast leave on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] acl number 2005
[HUAWEI-acl-basic-2005] rule permit source 225.1.0.0 0.0.255.255
[HUAWEI-acl-basic-2005] quit
[HUAWEI] multicast routing-enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] igmp prompt-leave group-policy 2005
```


8.1.25 igmp proxy

Function

The **igmp proxy** command enables IGMP proxy on an interface.

The **undo igmp proxy** command disables IGMP proxy on an interface.

By default, IGMP proxy is disabled on an interface.

Format

igmp proxy [**track nqa** *admin-name test-name*]

undo igmp proxy

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Parameters

Parameter	Description	Value
track nqa *admin-name test-name*	Specifies the administrator name and test name of an NQA test instance.	The value of either *admin-name* or *test-name* is a string of 1 to 32 case-sensitive characters, and spaces are not supported. **NOTE** When double quotation marks are used around the string, spaces are allowed in the string.

Views

GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, VLANIF interface view, loopback interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In a simple tree topology, multicast switches directly connected to user network segments do not need to run any complicated multicast routing protocol (such as PIM). However, the upstream access devices have to manage many users because the multicast switches transparently transmit all IGMP messages from hosts. To reduce the load on the upstream device, configure IGMP proxy on the multicast

switches. The multicast switches then collect and summarize Report/Leave messages received from downstream hosts before sending them to the upstream device. The multicast switches also maintain group memberships and forward multicast packets based on the group memberships. The upstream device considers the multicast switches as hosts.

IGMP proxy lacks a fault detection mechanism to trigger link switchover quickly. Therefore, multicast services will be interrupted for a long time when a link failure occurs. You can solve this problem by associating IGMP proxy with a network quality analysis (NQA) test instance. If you specify **track nqa** *admin-name test-name* in the command, IGMP proxy will be associated with the specified NQA test instance for end-to-end link status monitoring. When the NQA test instance detects a link failure on the active IGMP proxy interface, the switch with the IGMP proxy interface protection mode configured can trigger a switchover between the active/standby or active/active links quickly to minimize the communication interruption time.

- If an NQA test instance detects a primary link Down event, the IGMP proxy-capable device switches traffic from the primary link to the backup link or to the other primary link.
- If an NQA test instance detects a primary link Up event or if the NQA test instance is ineffective or deleted, the IGMP proxy-capable device switches traffic back from the backup link to the primary link or balances traffic between the primary links based on the computing result of the group hash algorithm.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command.

Precautions

Only one active IGMP proxy interface and one backup IGMP proxy interface or two active IGMP proxy interfaces can be configured. Only the primary IGMP proxy interface can be associated with an NQA

IGMP proxy conflicts with the following features:

- PIM: If the **pim sm** or **pim dm** command has been configured on an interface, the **igmp proxy** command cannot be used on the interface. If the **igmp proxy** command is configured first, the **pim sm** or **pim dm** command cannot be used on the interface.
- IGMP: If the **igmp enable** command has been configured on an interface, the **igmp proxy** command cannot be used on the interface. If the **igmp proxy** command is configured first, the **igmp enable** command cannot be used on the interface.
- Static group: After a static group is configured on an interface, the **igmp proxy** command cannot be used on the interface. If the **igmp proxy** command has been configured, no static group can be configured on the interface.
- If two or more IGMP proxy interfaces have been configured on a device, the device's other interfaces cannot be configured as backup IGMP proxy interfaces.

Example

Enable IGMP proxy on VLANIF100.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] igmp proxy
```

Enable IGMP proxy on VLANIF100, and associate VLANIF100 with an NQA test instance named user test.

```
<HUAWEI> system-view
[HUAWEI] nqa test-instance user test
[HUAWEI-nqa-user-test] test-type icmp
[HUAWEI-nqa-user-test] destination-address ipv4 1.1.1.1
[HUAWEI-nqa-user-test] quit
[HUAWEI] multicast routing-enable
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] igmp proxy track nqa user test
```

8.1.26 igmp proxy backup

Function

The **igmp proxy backup** command configures a backup IGMP proxy interface.

The **undo igmp proxy backup** command cancels the configuration.

By default, no backup IGMP proxy interface is configured.

Format

igmp proxy backup

undo igmp proxy backup

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Parameters

None

Views

GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, VLANIF interface view, loopback interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Generally, the IGMP proxy function becomes unavailable if the upstream interface with IGMP proxy configured fails. To enhance reliability of the IGMP service, configure a backup IGMP proxy interface after configuring IGMP proxy on the upstream interface. If the upstream interface fails, the backup interface takes over the IGMP proxy service to resume multicast services.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command.

Precautions

An instance allows only one IGMP proxy interface and one backup IGMP proxy interface. Only one backup IGMP proxy interface can be configured on a device.

IGMP proxy conflicts with the following features:

- PIM: If the **pim sm** or **pim dm** command has been configured on an interface, the **igmp proxy backup** command cannot be used on the interface. If the **igmp proxy backup** command is configured first, the **pim sm** or **pim dm** command cannot be used on the interface.
- IGMP: If the **igmp enable** command has been configured on an interface, the **igmp proxy backup** command cannot be used on the interface. If the **igmp proxy backup** command is configured first, the **igmp enable** command cannot be used on the interface.
- Static group: After a static group is configured on an interface, the **igmp proxy backup** command cannot be used on the interface. If the **igmp proxy backup** command has been configured, no static group can be configured on the interface.
- If two or more IGMP proxy interfaces have been configured on a device, the device's other interfaces cannot be configured as backup IGMP proxy interfaces.

Example

Configure VLANIF100 as a backup IGMP proxy interface.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] igmp proxy backup
```

8.1.27 igmp proxy interface reroute

Function

The **igmp proxy interface reroute** command deletes switchback delay configurations of IGMP proxy interfaces, so that the interfaces enter the switchback state immediately after the switchback trigger conditions are met.

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Format

igmp proxy [**vpn-instance** *vpn-instance* | **all-instance**] **interface** [*interface-type interface-number*] **reroute**

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance*	Specifies a VPN instance.	The value must be an existing VPN instance name.
all-instance	Indicates all VPN instances.	-
interface [*interface-type interface-number*]	Specifies an IGMP proxy interface. If *interface-type interface-number* is not specified, the command deletes switchback delay configuration of all interfaces.	-

Views

User view

Default Level

2: Configuration level

Usage Guidelines

To delete switchback delay configurations of IGMP proxy interfaces, run the **igmp proxy interface reroute** command, after which the IGMP proxy interfaces enter the switchback state immediately after the switchback trigger conditions are met.

If neither **vpn-instance** *vpn-instance* nor **all-instance** is specified, the command deletes switchback delay configurations of IGMP proxy interfaces in the public network instance only.

Example

Delete switchback delay configurations of IGMP proxy interfaces in the public network instance.

```
<HUAWEI> igmp proxy interface reroute
Warning: This operation will lead to reroute IGMP proxy in the instance to which the interface belongs.
Continue? [Y/N]:Y
```


8.1.28 igmp proxy reroute delay

Function

The **igmp proxy reroute delay** command sets a switchback delay for an IGMP proxy interface.

The **undo igmp proxy reroute delay** command restores the default configuration.

By default, an IGMP proxy interface never enters the switchback state.

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Format

igmp proxy reroute delay { *delay-time* | **never** }

undo igmp proxy reroute delay [*delay-time* | **never**]

Parameters

Parameter	Description	Value
delay-time	Sets a switchback delay for an IGMP proxy interface.	The value is an integer ranging from 10 to 86400, in seconds.
never	Indicates that an IGMP proxy interface never enters the switchback state.	-

Views

GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, VLANIF interface view, loopback interface view

Default Level

2: Configuration level

Usage Guidelines

After a primary IGMP proxy interface recovers, multicast routing entries are updated. If the primary IGMP proxy interface fails again during an entry update, multicast traffic may be lost. To resolve such issues in primary IGMP proxy interface flapping scenarios, run the **igmp proxy reroute delay** command to set a switchback delay for the IGMP proxy interface. The multicast routing entry update process then starts only after the specified switchback delay expires.

Example

Set the switchback delay to 100s for an IGMP proxy interface.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] igmp proxy reroute delay 100
```

8.1.29 igmp query ip-source-policy

Function

The **igmp query ip-source-policy** command configures IGMP Query message filtering based on source addresses.

The **undo igmp query ip-source-policy** command restores the default configuration.

By default, no source address-based IGMP Query message filtering is configured.

Format

igmp query ip-source-policy *basic-acl-number*

undo igmp query ip-source-policy

Parameters

Parameter	Description	Value
basic-acl-number	Specifies the number of a basic ACL, which defines the range of source addresses.	The value is an integer that ranges from 2000 to 2999.

Views

GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, GE sub-interface view, XGE sub-interface view, MultiGE sub-interface view, 25GE sub-interface view, 40GE sub-interface view, 100GE sub-interface view, Eth-Trunk sub-interface view, VLANIF interface view, loopback interface view, VBDIF interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If an attacker sends forged IGMP Query messages with an IP address smaller than the querier IP address, the querier will be replaced by the attacker. As a result, the

real querier cannot respond to Report messages from group members and bandwidth is wasted. Source address-based IGMP Query message filtering can protect the querier from such attacks. After this function is configured on a switch, the switch accepts only the IGMP Query messages with source addresses permitted by the specified ACL. This function controls querier election.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command.

Precautions

IGMP Query messages are encapsulated into IP messages. This command configures a policy to filter IGMP Query messages based on source addresses in IP headers, allowing only the source addresses that are in the ACL referenced in the policy.

The **igmp query ip-source-policy** command works with the **acl** command. For a numbered ACL, you can configure the source address of IGMP Query messages by specifying the **source** parameter in the **rule** command in the basic ACL view.

Example

Configure VLANIF100 to accept only the IGMP Query messages with the source address 10.10.1.1.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] acl number 2001
[HUAWEI-acl-basic-2001] rule permit source 10.10.1.1 0
[HUAWEI-acl-basic-2001] quit
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] igmp query ip-source-policy 2001
```

Configure GE0/0/1 to accept only the IGMP Query messages with the source address 10.10.1.1.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] acl number 2001
[HUAWEI-acl-basic-2001] rule permit source 10.10.1.1 0
[HUAWEI-acl-basic-2001] quit
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] igmp query ip-source-policy 2001
```

8.1.30 igmp require-router-alert

Function

The **igmp require-router-alert** command configures an interface to discard IGMP messages without the Router-Alert Option.

The **undo igmp require-router-alert** command disables an interface from checking for the Router-Alert Option in IGMP messages.

By default, the device does not check for the Router-Alert Option in IGMP messages and processes all the IGMP messages received on an interface.

Format

igmp require-router-alert

undo igmp require-router-alert

Parameters

None

Views

GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, GE sub-interface view, XGE sub-interface view, MultiGE sub-interface view, 25GE sub-interface view, 40GE sub-interface view, 100GE sub-interface view, Eth-Trunk sub-interface view, VLANIF interface view, loopback interface view, VBDIF interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Generally, a network device sends a packet to the corresponding protocol module for processing only when the destination address of the packet is a local interface address. Destination addresses of IGMP packets are multicast addresses but not interface addresses of multicast devices. Therefore, multicast devices do not send IGMP packets to the IGMP module, and the IGMP module cannot maintain group memberships.

The Router-Alert option in the IP header of an IGMP message solves this problem. If an IGMP message contains the Router-Alert option, the device sends the message to the routing protocol module.

You can configure the device to accept only IGMP messages with the Router-Alert option to improve IGMP security.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command.

Precautions

This command has the same function as the **require-router-alert** command used in the IGMP view. The configuration in the IGMP view takes effect for all interfaces, whereas the configuration in the interface view takes effect only for the specified interface. The configuration in the interface view takes precedence over the configuration in the IGMP view. The configuration in the IGMP view is used only when no configuration is performed in the interface view.

Example

Configure VLANIF100 to discard IGMP messages without the Router-Alert option.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] igmp require-router-alert
```

Configure GE0/0/1 to discard IGMP messages without the Router-Alert option.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] igmp require-router-alert
```

8.1.31 igmp robust-count

Function

The **igmp robust-count** command sets an IGMP querier robustness variable on an interface.

The **undo igmp robust-count** command restores the default IGMP querier robustness variable on an interface.

By default, the IGMP querier robustness variable is 2.

Format

igmp robust-count *robust-value*

undo igmp robust-count

Parameters

Parameter	Description	Value
robust-value	Specifies the IGMP querier robustness variable.	The value is an integer that ranges from 2 to 5.

Views

GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, GE sub-interface view, XGE sub-interface view, MultiGE sub-interface view, 25GE sub-interface view, 40GE sub-interface view, 100GE sub-interface view, Eth-Trunk sub-interface view, VLANIF interface view, loopback interface view, VBDIF interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The IGMP querier robustness variable specifies the retransmission count of IGMP packets to minimize the impact of packet loss on the network.

On a shared network segment, a querier maintains IGMP-attached group memberships. The robustness variable affects the timeout interval of group memberships. The timeout interval of group memberships is calculated using the formula:

Timeout interval of group memberships = Interval for sending IGMP General Query messages x Robustness variable + Maximum response time

The robustness variable determines the following values:

- Number of times the querier sends General Query messages when the querier starts

  When a querier starts, it sends General Query messages a certain number of times specified by the robustness variable to query the multicast groups that have members on the shared network segment. The message sending interval during this process is 1/4 of the query interval configured using the **igmp timer query** or **timer query** command.
- Number of times the querier sends IGMPv2 Group-Specific Query messages or IGMPv3 Source-and-Group-Specific Query messages when the querier receives a Leave message

  When receiving an IGMP Leave message of a multicast group, the querier sends Group-Specific Query messages certain times specified by the robustness variable to check whether the group has members. When the querier receives a Report message indicating that source-group mapping changes, the querier sends Source-and-Group-Specific Query messages a certain number of times specified by the robustness variable. The interval for sending Group-Specific Query messages and Source-and-Group-Specific Query messages can set using the **igmp lastmember-queryinterval** or **lastmember-queryinterval** command.
- Number of times for a querier to send IGMPv3 group/source-specific query messages after receiving the Report message about the change of the relationship between the multicast group and its source list.

  When receiving a Report message, the querier sends group/source-specific query messages for the "robustness variable" times. The interval for sending group/source-specific query messages can be set using the **igmp lastmember-queryinterval** command or the **lastmember-queryinterval** command.

A larger robustness variable makes an IGMP querier more robust, but increases the timeout interval of group memberships.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command.

Precautions

The **igmp robust-count** command has the same function as the **robust-count** command used in the IGMP view. The configuration in the IGMP view takes effect for all interfaces, whereas the configuration in the interface view takes effect only for the specified interface. The configuration in the interface view takes precedence over the configuration in the IGMP view. The configuration in the IGMP view is used only when no configuration is performed in the interface view.

Example

Set the querier robustness variable on VLANIF100 to 3.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] igmp robust-count 3
```

Set the querier robustness variable on GE0/0/1 to 3.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] igmp robust-count 3
```

8.1.32 igmp send-router-alert

Function

The **igmp send-router-alert** command configures an interface to send IGMP messages containing the Router-Alert option in IP headers.

The **undo igmp send-router-alert** command disables an interface from sending IGMP messages containing the Router-Alert option in IP headers.

By default, the IP headers of IGMP messages sent by an interface contain the Router-Alert option.

Format

igmp send-router-alert

undo igmp send-router-alert

Parameters

None

Views

GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, GE sub-interface view, XGE sub-interface view, MultiGE sub-interface view, 25GE sub-interface view, 40GE sub-interface view, 100GE sub-interface view, Eth-Trunk sub-interface view, VLANIF interface view, loopback interface view, VBDIF interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

By default, the switch sends IGMP messages that contain the Router-Alert option in IP headers. If the switch needs to communicate with a device that does not support the Router-Alert option, run the **undo igmp send-router-alert** command to configure the switch to send IGMP messages without the Router-Alert option. The **igmp send-router-alert** command is usually used together with the **igmp require-router-alert** command.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command.

Precautions

The **igmp send-router-alert** command has the same function as the **send-router-alert** command used in the IGMP view. The configuration in the IGMP view takes effect for all interfaces, whereas the configuration in the interface view takes effect only for the specified interface. The configuration in the interface view takes precedence over the configuration in the IGMP view. The configuration in the IGMP view is used only when no configuration is performed in the interface view.

Example

Configure VLANIF100 to send IGMP messages without the Router-Alert option.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] undo igmp send-router-alert
```

Configure GE0/0/1 to send IGMP messages without the Router-Alert option.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] undo igmp send-router-alert
```

8.1.33 igmp ssm-mapping enable

Function

The **igmp ssm-mapping enable** command enables SSM mapping on an interface.

The **undo igmp ssm-mapping enable** command disables SSM mapping on an interface.

By default, SSM mapping is disabled on an interface.

Format

igmp ssm-mapping enable

undo igmp ssm-mapping enable

Parameters

None

Views

GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, GE sub-interface view, XGE sub-interface view, MultiGE sub-interface view, 25GE sub-interface view, 40GE sub-interface view, 100GE sub-interface view, Eth-Trunk sub-interface view, VLANIF interface view, loopback interface view, VBDIF interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The SSM model allows only IGMPv3 hosts to specify the multicast sources which they want to receive data from. However, some hosts can only run IGMPv1 or IGMPv2. To enable these hosts to use the SSM service, configure IGMP SSM mapping on the switch. IGMP SSM mapping is implemented based on static SSM mapping entries on the switch. The switch converts (*, G) information in IGMPv1 and IGMPv2 Report messages to (S, G) information according to static SSM mapping entries to provide the SSM service for IGMPv1 and IGMPv2 hosts.

The **igmp ssm-mapping enable** command enables SSM mapping on an interface. The mappings between multicast source addresses and group addresses take effect only when SSM mapping is enabled on an interface. SSM mappings are configured using the **ssm-mapping** command.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command.

Precautions

The SSM mapping function takes effect on an interface only when the interface runs IGMPv3.

Example

Enable SSM mapping on VLANIF100.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] igmp ssm-mapping enable
```

Enable SSM mapping on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
```



```
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] igmp ssm-mapping enable
```

8.1.34 igmp static-group

Function

The **igmp static-group** command configures a static multicast group on an interface.

The **undo igmp static-group** command deletes a static multicast group from an interface.

By default, no static multicast group is configured on an interface.

Format

igmp static-group *group-address* [**inc-step-mask** { *group-mask* | *group-mask-length* } **number** *group-number*] [**source** *source-address*]

undo igmp static-group { **all** | *group-address* [**inc-step-mask** { *group-mask* | *group-mask-length* } **number** *group-number*] [**source** *source-address*] }

igmp static-group *group-address* [**inc-step-mask** { *group-mask* | *group-mask-length* } **number** *group-number*] [**source** *source-address*] { **qinq pe-vid** *pe-vid* **ce-vid** *low-ce-vid* [**to** *high-ce-vid*] | **dot1q vid** *low-pe-vid* [**to** *high-pe-vid*] } (S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S)

undo igmp static-group *group-address* [**inc-step-mask** { *group-mask* | *group-mask-length* } **number** *group-number*] [**source** *source-address*] { **qinq pe-vid** *pe-vid* **ce-vid** *low-ce-vid* [**to** *high-ce-vid*] | **dot1q vid** *low-pe-vid* [**to** *high-pe-vid*] } (S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S)

Parameters

Parameter	Description	Value
group-address	Specifies a multicast group address. In batch configuration mode, this parameter specifies the start address of the multicast group range.	The value ranges from 224.0.1.0 to 239.255.255.255, in dotted decimal notation.
inc-step-mask	Sets the step mask of group addresses in batch configuration mode.	-

Parameter	Description	Value
group-mask	Specifies the step mask of a group address in batch configuration mode, that is, the gap between two consecutive group addresses.	The value is a wildcard mask format that ranges from 0.0.0.1 to 15.255.255.255, in dotted decimal notation.
group-mask-length	Specifies the step mask length in batch configuration mode.	The value is an integer that ranges from 4 to 32. If *group-mask-length* is used to configure the step mask and the **display current-configuration** command is used to display related configurations, the step mask of group addresses is displayed in *group-mask* format.
number *group-number*	Specifies the number of group addresses in batch configuration mode.	The value is an integer that ranges from 2 to 512.
source *source-address*	Specifies a multicast source address. If the specified static group address is an SSM group address, you must specify a multicast source address for the group.	The address is in dotted decimal notation.
all	Indicates all multicast groups that an interface statically joins.	-
qinq	Statically adds a sub-interface for QinQ Virtual Local Area Network (VLAN) tag termination to a multicast group.	-
pe-vid *pe-vid*	Specifies the ID of the outer VLAN tag.	The value is a decimal integer that ranges from 1 to 4094.
ce-vid	Indicates the ID of the inner VLAN tag.	-
low-ce-vid	Specifies the lower limit of the CE-VLAN ID (inner VLAN tag).	The value is a decimal integer that ranges from 1 to 4094.

Parameter	Description	Value
to	Indicates a value range.	-
high-ce-vid	Specifies the upper limit of the CE-VLAN ID (inner VLAN tag).	The value is a decimal integer that ranges from 1 to 4094. The value of *high-ce-vid* cannot be smaller than that of *low-ce-vid*. By default, the values of *high-ce-vid* and *low-ce-vid* are the same.
dot1q	Statically adds a sub-interface for dot1q VLAN tag termination to a multicast group.	-
vid	Indicates the VLAN ID.	-
low-pe-vid	Specifies the lower limit of PE-VLAN ID (outer VLAN tag).	The value is a decimal integer that ranges from 1 to 4094.
high-pe-vid	Specifies the upper limit of PE-VLAN ID (outer VLAN tag).	The value is a decimal integer that ranges from 1 to 4094. The value of *high-pe-vid* cannot be smaller than that of *low-pe-vid*. By default, the values of *high-pe-vid* and *low-pe-vid* are the same.

Views

GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, GE sub-interface view, XGE sub-interface view, MultiGE sub-interface view, 25GE sub-interface view, 40GE sub-interface view, 100GE sub-interface view, Eth-Trunk sub-interface view, VLANIF interface view, loopback interface view, VBDIF interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The following are two scenarios in which you can configure static multicast groups on user-side interfaces of the switch:

- There are long-term group members on a shared network segment, and the switch needs to forward multicast data to these group members quickly and steadily.
- A network segment has no group member or hosts on the network segment cannot send Report messages, but multicast data needs to be sent to this network segment.

After a static multicast group is configured on an interface, the switch considers that the multicast group always has members on the network segment of the interface. Therefore, the switch always forwards multicast data of the multicast group.

The **igmp static-group** command is used on an interface connected to user hosts. The command can configure a single group or source-group binding on an interface or configure multiple groups or source-group bindings in a batch.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command.

Follow-up Procedure

If a user host no longer needs to receive multicast data of a static group, delete the static group configuration.

Precautions

- The IGMP entries of static groups configured on an interface never time out. The switch considers that this interface is always connected to group members, and keeps forwarding multicast packets of the specified multicast groups to the network segment of the interface.
- After you run the **igmp static-group** command without specifying the **qinq** or **dot1q** keyword to configure batch multicast static groups for the first time and when you run this command again, the new configuration overwrites the previous one if only the value of **group-number** is changed but the values of *group-address* and *group-mask* | *group-mask-length* are the same.

  After you run the **igmp static-group** command with specifying the **qinq** or **dot1q** keyword to configure batch multicast static groups for the first time and when you run this command again, the new configuration overwrites the previous one if only the value of **group-number** is changed but the values of *group-address* and *group-mask* | *group-mask-length* and the values of tag parameters the same. If the values of tag parameters are different, the device considers that the later command is different from the first one and the new configuration does not overwrite the previous configuration.
- You can specify the **qinq** keyword for only the sub-interface for QinQ VLAN tag termination and **dot1q** keyword for only the sub-interface for dot1q VLAN tag termination. The static group with tag parameters can be configured only on the sub-interface for QinQ VLAN tag termination or the sub-interface for dot1q VLAN tag termination.
- When the interface is configured with multiple VLAN tags, you must specify the **qinq** or **dot1q** keyword. The multicast source address cannot be specified in such a case. That is, source address and the **qinq** or **dot1q** keyword cannot be specified at the same time.

- The specified range of VLAN IDs must be consistent with that specified in the **dot1q termination vid** command or the **qinq termination pe-vid ce-vid** command. If they are inconsistent, only the intersected tag values take effect.
- When the interface that connects a multicast device to the user network segment joins a multicast group in both dynamic and static modes, the interface preferentially joins the multicast group in static mode if a conflict occurs.
- You can configure overlapping multicast group addresses in different batch configurations. When you configure multiple static multicast groups in a batch on an interface, do not delete any static group configuration before the system completes the batch static group configuration.
- Do not statically add an interface to multicast groups if the interface is in the PIM NDR or assert loser state, because such an interface will not be added to the PIM outbound interface list.

Example

Configure static multicast group 224.1.1.1 on VLANIF100.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] igmp static-group 224.1.1.1
```

Configure the switch to forward multicast packets from multicast source 192.168.11.1 to multicast group 232.1.1.1 through VLANIF100.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] igmp static-group 232.1.1.1 source 192.168.11.1
```

Configure 10 static multicast groups on VLANIF100 in a batch. Set the start multicast group address to 225.1.1.1 and the step mask length to 32.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] igmp static-group 225.1.1.1 inc-step-mask 32 number 10
```

Configure 10 source-group bindings on VLANIF100 in a batch. Set the start multicast group address to 232.1.1.1, the source address to 192.168.11.1, and the step mask length to 32.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] igmp static-group 232.1.1.1 inc-step-mask 32 number 10 source 192.168.11.1
```

Configure static multicast group 224.1.1.1 on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] igmp static-group 224.1.1.1
```

Configure the sub-interface for QinQ VLAN tag termination GE 0/0/1.1 to statically join multicast groups in batches, with the start group address of 225.0.0.0, the incremental mask length of 32, and the number of group addresses of 2. The outer VLAN tag is 1 and the inner VLAN tag ranges from 1 to 3.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
```



```
[HUAWEI] vcmp role silent
[HUAWEI] interface gigabitethernet0/0/1
[HUAWEI-GigabitEthernet0/0/1] port link-type hybrid
[HUAWEI-GigabitEthernet0/0/1] quit
[HUAWEI] interface gigabitethernet0/0/1.1
[HUAWEI-GigabitEthernet0/0/1.1] igmp static-group 225.0.0.0 inc-step-mask 32 number 2 qinq pe-vid 1 ce-vid 1 to 3
```

8.1.35 igmp timer other-querier-present

Function

The **igmp timer other-querier-present** command sets the other querier present timer on an interface.

The **undo igmp timer other-querier-present** command restores the default value of the other querier present timer on an interface.

The formula used to calculate the other querier present timer value is:

Other querier present timer = Robustness variable x Interval for sending IGMP General Query messages + 1/2 x Maximum response time for IGMP query messages

If the default values of the robustness variable, the interval for sending IGMP General Query messages, and the maximum response time for IGMP query messages are used, the other querier present timer value is 125s.

Format

igmp timer other-querier-present *interval*

undo igmp timer other-querier-present

Parameters

Parameter	Description	Value
interval	Specifies the other querier present timer.	The value is an integer that ranges from 60 to 300, in seconds.

Views

GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, GE sub-interface view, XGE sub-interface view, MultiGE sub-interface view, 25GE sub-interface view, 40GE sub-interface view, 100GE sub-interface view, Eth-Trunk sub-interface view, VLANIF interface view, loopback interface view, VBDIF interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When a user network segment connects to multiple Layer 3 multicast devices, only one Layer 3 multicast device is elected as the IGMP querier to send Query messages to hosts on the network segment. If the querier fails to send Query messages, group memberships cannot be created or maintained. Non-queriers running IGMPv2 or IGMPv3 start the other querier present timer after they fail in the querier election. If the non-queriers do not receive Query messages from the querier before the timer times out, they consider the querier failed and start a new querier election.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command.

Precautions

- The **igmp timer other-querier-present** command applies only to IGMPv2 and IGMPv3.
- The **igmp timer other-querier-present** command has the same function as the **timer other-querier-present** command used in the IGMP view. The configuration in the IGMP view takes effect for all interfaces, whereas the configuration in the interface view takes effect only for the specified interface. The configuration in the interface view takes precedence over the configuration in the IGMP view. The configuration in the IGMP view is used only when no configuration is performed in the interface view.

NOTICE

If the other querier present timer value is shorter than the interval for sending IGMP General Query messages, the querier election is triggered frequently.

Example

On VLANIF100, set the other querier present timer to 200 seconds.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] igmp timer other-querier-present 200
```

On GE0/0/1, set the other querier present timer to 200 seconds.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] igmp timer other-querier-present 200
```


8.1.36 igmp timer query

Function

The **igmp timer query** command sets the interval at which an interface sends IGMP General Query messages.

The **undo igmp timer query** command restores the default interval at which an interface sends IGMP General Query messages.

By default, an interface sends IGMP General Query messages at an interval of 60s.

Format

igmp timer query *interval*

undo igmp timer query

Parameters

Parameter	Description	Value
interval	Specifies the interval at which an interface sends IGMP General Query messages.	The value is an integer that ranges from 1 to 18000, in seconds.

Views

GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, GE sub-interface view, XGE sub-interface view, MultiGE sub-interface view, 25GE sub-interface view, 40GE sub-interface view, 100GE sub-interface view, Eth-Trunk sub-interface view, VLANIF interface view, loopback interface view, VBDIF interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

An IGMP querier checks whether a local network segment has group members by sending IGMP General Query messages at an interval, known as the general query interval. You can set the general query interval based on the needs of your network. The general query interval affects the following processes:

- When a querier starts, it sends General Query messages a certain number of times specified by the robustness variable to query the multicast groups that have members on the shared network segment. The message sending interval during this process is 1/4 of the general query interval. The robustness variable can be set using the **igmp robust-count** command or the **robust-count** command.

- After the startup process is complete, the querier sends General Query messages at intervals to maintain the group memberships on the interface.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command.

Precautions

- The querier is more sensitive when it sends General Query messages at a shorter interval, but more bandwidth and resources are consumed.
- The function of the **igmp timer query** command is the same as that of the **timer query** command used in the IGMP view. The configuration in the IGMP view takes effect for all interfaces, whereas the configuration in the interface view takes effect only for the specified interface. The configuration in the interface view takes precedence over the configuration in the IGMP view. The configuration in the IGMP view is used only when no configuration is performed in the interface view.

NOTE

The default *interval* value in this command is 60 seconds, which is different than the default value 125 seconds defined by the RFC standard. A Huawei querier and a non-Huawei querier must send IGMP general query messages at the same interval.

Example

Set the interval at which VLANIF100 sends General Query messages to 50 seconds.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] igmp timer query 50
```

Set the interval at which GE0/0/1 sends General Query messages to 50 seconds.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] igmp timer query 50
```

8.1.37 igmp ttl-check

Function

The **igmp ttl-check** command enables the device to check the TTL values in received IGMP Report, Leave, and Query messages on a specific interface.

The **undo igmp ttl-check** command restores the default configuration.

By default, the device does not check the TTL values in received IGMP Report, Leave, and Query messages on an interface.

Format

igmp ttl-check

undo igmp ttl-check

Parameters

None

Views

GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, GE sub-interface view, XGE sub-interface view, MultiGE sub-interface view, 25GE sub-interface view, 40GE sub-interface view, 100GE sub-interface view, Eth-Trunk sub-interface view, VLANIF interface view, loopback interface view, VBDIF interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

This command enables TTL check for IGMP Report, Leave, and Query messages on an interface. This function protects the system against attacking IGMP messages by dropping the messages of which the TTL value is not 1. By default, TTL values of IGMP messages are not checked on an interface.

You can also configure TTL check for IGMP Report, Leave, and Query messages by using the **ttl-check** command in the IGMP view. This command takes effect for all IGMP-enabled interfaces.

Precautions

If both the **igmp ttl-check** and **ttl-check** commands are run, the **igmp ttl-check** configuration in the interface view takes precedence over the **ttl-check** configuration in the IGMP view.

Example

Enable TTL check for IGMP Report, Leave, and Query messages on a physical interface.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] igmp ttl-check
```

Enable TTL check for IGMP Report, Leave, and Query messages on a VLANIF interface.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] vlan 2
[HUAWEI-vlan2] quit
[HUAWEI] interface vlanif 2
[HUAWEI-Vlanif2] igmp ttl-check
```


8.1.38 igmp version

Function

The **igmp version** command specifies an IGMP version on an interface.

The **undo igmp version** command restores the default IGMP version on an interface.

By default, an interface runs IGMPv2.

Format

igmp version *version*

undo igmp version

Parameters

Parameter	Description	Value
version	Specifies the IGMP version running on the interface.	The value is integer that ranges from 1 to 3.

Views

GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, GE sub-interface view, XGE sub-interface view, MultiGE sub-interface view, 25GE sub-interface view, 40GE sub-interface view, 100GE sub-interface view, Eth-Trunk sub-interface view, VLANIF interface view, loopback interface view, VBDIF interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The switch can only identify IGMP messages of a version earlier than its own IGMP version. To ensure normal IGMP operation, set on the switch an IGMP version the same as or alter than that running on member hosts.

If multiple switches exist on a shared network segment, configure the same IGMP version on all switch interfaces connected to hosts. Otherwise, errors may occur in IGMP operation because interfaces running different IGMP versions send packets with different formats.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command.

Precautions

This command functions in the same way as the **version** command used in the IGMP view, except that the configuration in the IGMP view is globally valid, whereas the configuration in the interface view is valid only for the specified interface. The configuration in the interface view takes precedence over the configuration in the IGMP view. The configuration in the IGMP view is used only when the configuration in the interface view is not done.

Example

Configure IGMPv1 on VLANIF100.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] igmp version 1
```

Configure IGMPv1 on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] igmp version 1
```

8.1.39 lastmember-queryinterval (IGMP)

Function

The **lastmember-queryinterval** command configures interval at which an IGMP querier sends IGMP Group-Specific Query messages or IGMP Group-and-Source-Specific Query messages after receiving IGMP Leave messages from hosts.

The **undo lastmember-queryinterval** command restores the default value.

By default, the interval at which an IGMP querier sends IGMP Group-Specific Query messages or IGMP Group-and-Source-Specific Query messages is 1 second.

Format

lastmember-queryinterval *interval*

undo lastmember-queryinterval

Parameters

Parameter	Description	Value
interval	Specifies the interval for sending IGMP Group-Specific Query messages or IGMP Group-and-Source-Specific Query messages.	The value is an integer that ranges from 1 to 5, in seconds.

Views

IGMP view of the public network instance, IGMP view of a VPN instance

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the querier receives a Leave message that a host sends to leave a multicast group, the querier periodically sends IGMP Group-Specific Query messages or IGMP Group-and-Source-Specific Query messages to check for other members in the multicast group. The **lastmember-queryinterval** command sets the interval at which the querier sends Last Member Query messages. The querier stops forwarding multicast data to the group if it receives no Report message from the group within the period specified by *interval* x *robust-value*. Here, *robust-value* is the robustness variable configured using the **igmp robust-count** or **robust-count** command.

If the querier does not receive any Report message within the specified period, it considers that the last member has left the group and no longer maintains the membership of this group.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command.

Precautions

- The **igmp lastmember-queryinterval** command is valid only when the IGMP querier runs IGMPv2 or IGMPv3.
- This command has the same function as the **igmp lastmember-queryinterval** command used in the interface view. The configuration in the IGMP view is globally valid, whereas the configuration in the interface view takes effect only for the specified interface. The configuration in the interface view takes precedence over the configuration in the IGMP view. The configuration in the IGMP view is used only when no configuration is performed in the interface view.

Example

In the IGMP view, set the interval for sending IGMP Group-Specific Query messages or IGMP Group-and-Source-Specific Query messages to 3 seconds.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] igmp
[HUAWEI-igmp] lastmember-queryinterval 3
```

8.1.40 limit (IGMP)

Function

The **limit** command sets the maximum number of IGMP entries that can be created globally or in an instance.

The **undo limit** command restores the maximum number of IGMP entries that can be created globally or in an instance to the default value.

The following lists the maximum number of IGMP entries that can be created globally or in an instance on each model by default:

- S5720-LI, S5720S-LI: 1022
- S5731-S, S5731S-S, S5720I-SI: 1024
- S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735S-S, S5735-S-I: 1500
- S5735S-H, S5736-S, S6720S-S: 1536
- S6730-S, S6730S-S: 4096
- S5731-H, S5731S-H, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H: 8192

Format

limit *number*

undo limit

Parameters

Parameter	Description	Value
number	Specifies the maximum number of IGMP entries that can be created globally or in the current instance.	The value is an integer that ranges from 1 to *The maximum number of IGMP entries that can be created globally or in an instance by default*. **NOTE** The value range of S5731-H, S5731S-H, S5732-H, S6730S-H, and S6730-H are expanded after the high specification mode is configured for multicast forwarding using the **set multicast forwarding-table super-mode** command. The actual value range depends on the specification of the device.

Views

IGMP view of the public network instance, IGMP view of a VPN instance

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

This command sets the maximum number of IGMP entries supported globally or in an instance.

When the number of IGMP entries reaches the limit, the system does not create any IGMP entries. To enable the switch to create more IGMP entries, delete useless entries or increase the limit. Alternatively, create static IGMP entries.

The number of IGMP entries is counted as follows:

- Each (*, G) entry is counted as one entry.
- Each (S, G) entry is counted as one entry.
- Each (*, G) entry established with SSM mapping is counted as one entry.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command.

Precautions

You can also run the **igmp global limit** *number* command in the system view to set the maximum number of global IGMP group memberships. If both the **limit** and **igmp global limit** *number* commands are executed, the smaller value takes effect.

Example

Set the maximum number of IGMP entries that can be created globally to 248.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] igmp
[HUAWEI-igmp] limit 248
```

8.1.41 max-response-time (IGMP)

Function

The **max-response-time** command sets a global maximum response time for IGMP General Query messages.

The **undo max-response-time** command restores the global maximum response time for IGMP General Query messages to the default value.

By default, the global maximum response time for IGMP General Query messages is 10 seconds.

Format

max-response-time *interval*

undo max-response-time

Parameters

Parameter	Description	Value
interval	Specifies the maximum response time for IGMP General Query messages.	The value is an integer that ranges from 1 to 25, in seconds.

Views

IGMP view of the public network instance, IGMP view of a VPN instance

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If hosts send IGMP Report messages immediately after they receive IGMP General Query messages, the querier on a shared network segment may receive a large number of Report messages sent from many hosts at the same time. This may cause congestion on the network.

To avoid such situations, IGMPv2 and IGMPv3 messages specify the maximum response time for IGMP General Query messages. When a host running IGMPv2 or IGMPv3 receives an IGMP General Query message, it starts a timer for the group it wants to join. The timer length is a random value between 0 and the maximum response time. When the timer times out, the host sends a Report message.

The maximum response time specifies the deadline for the host to send a Report message. An appropriate maximum response time allows hosts to respond to Query messages quickly and prevents hosts from sending Report messages at the same time.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command.

Precautions

- This command applies only to IGMPv2 and IGMPv3.
- A smaller response time allows the switch to learn multicast memberships more quickly but occupies more bandwidth and system resources.
- This command has the same function as the **igmp max-response-time** command used in the interface view. The configuration in the IGMP view is globally valid, whereas the configuration in the interface view takes effect only for the specified interface. The configuration in the interface view takes precedence over the configuration in the IGMP view. The configuration in the IGMP view is used only when no configuration is performed in the interface view.

Example

In the IGMP view, set the maximum response time for IGMP General Query messages to 8 seconds.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] igmp
[HUAWEI-igmp] max-response-time 8
```

8.1.42 prompt-leave (IGMP)

Function

The **prompt-leave** command enables the fast leave function globally. After receiving a Leave message for a group, the device immediately deletes the group entry, without sending an IGMP Group-Specific Query message or IGMP Group-and-Source-Specific Query message.

The **undo prompt-leave** command restores the default configuration.

By default, a multicast device sends an IGMP Group-Specific Query message or IGMP Group-and-Source-Specific Query message after receiving a Leave message from a host.

Format

prompt-leave [**group-policy** *acl-number*]

undo prompt-leave

Parameters

Parameter	Description	Value
group-policy	Specifies a group policy that controls the range of groups to which the fast leave takes effect.	-
acl-number	Specifies the number of a basic or advanced ACL. This list specifies the range of multicast groups.	The number of a basic ACL is an integer that ranges from 2000 to 2999. The number of an advanced ACL ranges from 3000 to 3999.

Views

IGMP view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In most cases, after receiving a Leave message of a group or source-specific group, a multicast device sends an IGMP Group-Specific Query message or IGMP Group-and-Source-Specific Query message to check whether this group has other members. To minimize the response delay and save network bandwidth, configure fast leave on multicast devices. This function enables a multicast device to delete a group or source/group entry immediately after receiving a Leave message, without sending an IGMP Group-Specific Query message or IGMP Group-and-Source-Specific Query message.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command.

Precautions

IGMP fast leave applies only to IGMPv2 and IGMPv3.

This command functions in the same way as the **igmp prompt-leave** command used in the interface view, except that the configuration in the IGMP view is globally valid, whereas the configuration in the interface view is valid only for the specified interface. The configuration in the interface view takes precedence over the configuration in the IGMP view. The configuration in the IGMP view is used only when the configuration in the interface view is not done.

Example

Enable IGMP fast leave in the IGMP view.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] igmp
[HUAWEI-igmp] prompt-leave
```

In the IGMP view, create ACL 2000, configure an ACL rule that permits group 225.1.0.0/16, and enable IGMP fast leave for the group.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] acl number 2000
[HUAWEI-acl-basic-2000] rule permit source 225.1.0.0 0.0.255.255
[HUAWEI-acl-basic-2000] quit
[HUAWEI] igmp
[HUAWEI-igmp] prompt-leave group-policy 2000
```

8.1.43 proxy reroute delay

Function

The **proxy reroute delay** command sets a switchback delay for IGMP proxy interfaces in the IGMP view.

The **undo proxy reroute delay** command restores the default configuration.

By default, IGMP proxy interfaces never enter the switchback state.

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Format

proxy reroute delay { *delay-time* | **never** }

undo proxy reroute delay [*delay-time* | **never**]

Parameters

Parameter	Description	Value
delay-time	Sets a switchback delay for IGMP proxy interfaces.	The value is an integer ranging from 10 to 86400, in seconds.
never	Indicates that IGMP proxy interfaces never enter the switchback state.	-

Views

IGMP view of the public network instance or IGMP view of the VPN instance

Default Level

2: Configuration level

Usage Guidelines

After a primary IGMP proxy interface recovers, multicast routing entries are updated. If the primary IGMP proxy interface fails again during an entry update, multicast traffic may be lost. To resolve such issues in primary IGMP proxy interface flapping scenarios, run the **proxy reroute delay** command to set a switchback delay for IGMP proxy interfaces in the IGMP view. The multicast routing entry update process then starts only after the specified switchback delay expires.

The **proxy reroute delay** command configuration applies to all IGMP proxy interfaces in the public network instance or a VPN instance. If the **igmp proxy reroute delay** command is also run for a specific IGMP proxy interface, the **igmp proxy reroute delay** command takes precedence over the **proxy reroute delay** command configuration.

Example

Set the switchback delay to 100s for IGMP proxy interfaces in the public network instance.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
```



```
[HUAWEI] igmp
[HUAWEI-igmp] proxy reroute delay 100
```

8.1.44 proxy source-lifetime

Function

The **proxy source-lifetime** command sets the timeout period for an (S, G) entry that an IGMP proxy-capable switch generates.

The **undo proxy source-lifetime** command restores the default configuration.

By default, the timeout period of an (S, G) entry that an IGMP proxy-capable switch generates is 210 seconds.

Format

proxy source-lifetime *interval*

undo proxy source-lifetime

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Parameters

Parameter	Description	Value
interval	Specifies the timeout period of an (S, G) entry.	The value is an integer that ranges from 60 to 65535, in seconds. The default value is recommended for general use.

Views

IGMP view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

An IGMP proxy-capable switch starts a timer for each (S, G) entry and records the time when a multicast source S sends multicast packets. The **proxy source-lifetime** command sets the timeout period for (S, G) entries on an IGMP proxy-capable switch. An IGMP proxy interface starts a timer when it receives the first multicast packet from a multicast source and resets the timer every time it receives a multicast packet from the multicast source. If the interface does not receive any multicast packet from the multicast source within the timeout period, it considers the (S, G) entry invalid.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command.

Example

#Set the timeout period for (S, G) entries to 200s.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] igmp
[HUAWEI-igmp] proxy source-lifetime 200
```

In VPN instance mvpn, set the timeout period for (S, G) entries to 200s.

8.1.45 proxy source-policy

Function

The **proxy source-policy** command configures an IGMP proxy-capable router to filter received multicast data packets based on source addresses or source and group addresses.

The **undo proxy source-policy** command restores the default configuration.

By default, an IGMP proxy-capable router does not filter received multicast data packets.

Format

proxy source-policy *acl-number*

undo proxy source-policy

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Parameters

Parameter	Description	Value
acl-number	Specifies the number of a basic ACL or an advanced ACL. The ACL defines a multicast group range.	The number of a basic ACL is an integer in the range 2000 to 2999. The number of an advanced ACL is an integer in the range 3000 to 3999.

Views

IGMP view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If an IGMP proxy-capable device needs to restrict multicast data packets sent from some multicast sources, run the **proxy source-policy** command to configure the device to filter multicast data packets based on source addresses or source and group addresses. This command can also be used to filter the multicast data encapsulated in Register messages.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command.

Precautions

The **proxy source-policy** command takes effect only when IGMP proxy is enabled.

To reference a numbered ACL to a proxy source policy, run the **proxy source-policy** and **acl** commands together.

- In the basic ACL view, specify the **source** parameter in the **rule** command to set a multicast group range.
- In the advanced ACL view, specify **source** in the **rule** command to set a source address range and specify **destination** to set a group address range.

Named ACLs are classified into basic and advanced ACLs. The configuration rules of a named ACL are the same as that of a numbered ACL.

Example

Configure an IGMP proxy-capable router to accept the multicast data packets from multicast source 10.10.1.2 and to discard the multicast data packets from the multicast source 10.10.1.1.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] acl number 2001
[HUAWEI-acl-basic-2001] rule permit source 10.10.1.2 0
[HUAWEI-acl-basic-2001] rule deny source 10.10.1.1 0
[HUAWEI-acl-basic-2001] quit
[HUAWEI] igmp
[HUAWEI-igmp] proxy source-policy 2001
```

Configure an IGMP proxy-capable router to accept the multicast data packets sent from multicast source 10.10.1.2 to multicast group 232.1.0.0.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] acl name myacl
[HUAWEI-acl-adv-myacl] rule permit ip source 10.10.1.2 0 destination 232.1.0.0 0.0.255.255
[HUAWEI-acl-adv-myacl] quit
[HUAWEI] igmp
[HUAWEI-igmp] proxy source-policy acl-name myacl
```

8.1.46 proxy ssm-policy

Function

The **proxy ssm-policy** command configures an SSM group address range for IGMP proxy.

The **undo proxy ssm-policy** command restores the default configuration.

The default SSM group address range for IGMP proxy is 232.0.0.0/8.

Format

proxy ssm-policy *basic-acl-number*

undo proxy ssm-policy

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Parameters

Parameter	Description	Value
basic-acl-number	Specifies the number of a basic ACL. This ACL defines a range of multicast groups.	The sequence number is an integer that ranges from 2000 to 2999.

Views

IGMP view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The default SSM group address range is 232.0.0.0 to 232.255.255.255. Generally, an IGMP proxy device provides the SSM service for hosts only when it receives Report messages with a group address in this range. If the SSM group address range needs to be narrowed to ensure security of a multicast network or be expanded to increase the number of SSM group addresses, configure a new SSM group address range on the IGMP proxy device. Ensure that all the multicast devices on the network are configured with the same SSM group address range.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command.

Precautions

The SSM model can be used in the following situations:

- Multicast group addresses are in an SSM address range, IGMPv3 is running on the user network segment, and multicast source addresses are specified in Report messages.

- Multicast group addresses are in an SSM address range, IGMPv1 or IGMPv2 is running on the user network segment, and SSM mapping is configured.

The **proxy ssm-policy** command works with the **acl** command. If a basic ACL is configured, you can specify **source** in the **rule** command to configure an SSM address range.

Example

Set the SSM group address range for IGMP proxy to 232.1.0.0/16.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] acl number 2000
[HUAWEI-acl-basic-2000] rule permit source 232.1.0.0 0.0.255.255
[HUAWEI-acl-basic-2000] quit
[HUAWEI] igmp
[HUAWEI-igmp] proxy ssm-policy 2000
```

8.1.47 require-router-alert (IGMP)

Function

The **require-router-alert** command configures the switch to discard IGMP messages without the Router-Alert option.

The **undo require-router-alert** command disables the switch from checking for the Router-Alert option in IGMP messages.

By default, the switch does not check whether the received IGMP messages contain the Router-Alert option in IP headers, and it accepts all the received IGMP messages.

Format

require-router-alert

undo require-router-alert

Parameters

None

Views

IGMP view of the public network instance, IGMP view of a VPN instance

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Generally, a network device sends a packet to the corresponding protocol module for processing only when the destination address of the packet is a local interface

address. Destination addresses of IGMP packets are multicast addresses but not interface addresses of multicast devices. Therefore, multicast devices do not send IGMP packets to the IGMP module, and the IGMP module cannot maintain group memberships.

The Router-Alert option in IP packet headers solves this problem. This option indicates that a packet needs to be sent to the protocol module.

You can configure the switch to accept only IGMP messages with the Router-Alert option. This configuration improves security of the IGMP service.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command.

Precautions

This command has the same function as the **igmp require-router-alert** command used in the interface view. The configuration in the IGMP view is globally valid, whereas the configuration in the interface view takes effect only for the specified interface. The configuration in the interface view takes precedence over the configuration in the IGMP view. The configuration in the IGMP view is used only when no configuration is performed in the interface view.

Example

In the IGMP view, configure the switch to discard IGMP messages without the Router-Alert option.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] igmp
[HUAWEI-igmp] require-router-alert
```

8.1.48 reset igmp control-message counters

Function

The **reset igmp control-message counters** command clears statistics about IGMP messages.

Format

reset igmp [**vpn-instance** *vpn-instance-name* | **all-instance**] **control-message counters** [**interface** *interface-type interface-number*] [**message-type** { **query** | **report** }]

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Clears IGMP message statistics in a specified VPN instance.	The value must be an existing VPN instance name.

Parameter	Description	Value
all-instance	Clears IGMP message statistics in all instances.	-
interface *interface-type interface-number*	Clears IGMP message statistics on a specified interface. If this parameter is not specified, the command clears IGMP statistics on all interfaces.	-
message-type	Clears statistics about IGMP messages of a specified type. If this parameter is not specified, the command clears statistics about all IGMP messages.	-
query	Clears statistics about Query messages received by an interface.	-
report	Clears statistics about Report messages received by an interface.	-

Views

User view

Default Level

3: Management level

Usage Guidelines

IGMP still operates normally after IGMP message statistics are deleted.

Example

Clear statistics about IGMP messages on all interfaces.

```
<HUAWEI> reset igmp control-message counters
```

Clear statistics about IGMP messages on VLANIF100.

```
<HUAWEI> reset igmp control-message counters interface vlanif 100
```

8.1.49 reset igmp explicit-tracking

Function

The **reset igmp explicit-tracking** command deletes information about the hosts with dynamic group memberships established through IGMP on an interface.

Format

reset igmp [**vpn-instance** *vpn-instance-name* | **all-instance**] **explicit-tracking** { **all** | **interface** *interface-type interface-number* [**host** *host-address* [**group** *group-address* [**source** *source-address*]]] }

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Deletes information about the hosts with IGMP-attached group memberships on interfaces in a specified VPN instance.	The value must be an existing VPN instance name.
all-instance	Deletes information about the hosts with IGMP-attached group memberships on interfaces in all instances.	-
all	Deletes information about all the hosts.	-
interface *interface-type interface-number*	Deletes information about the hosts with IGMP-attached group memberships on a specified interface. If this parameter is not specified, the command deletes information about the hosts with IGMP-attached group memberships on all interfaces.	-
host *host-address*	Specifies the IP address of a host.	The address is in dotted decimal notation.
group *group-address*	Specifies the address of a multicast group.	The address is in dotted decimal notation and ranges from 224.0.1.0 to 239.255.255.255.
source *source-address*	Specifies the address of a multicast source.	The address is in dotted decimal notation.

Views

User view

Default Level

3: Management level

Usage Guidelines

You can use this command to delete information about the hosts with dynamic group memberships established on interfaces using IGMP.

Example

Delete information about IGMP host 192.168.0.12 in group 232.1.1.1 on VLANIF10.

```
<HUAWEI> reset igmp explicit-tracking interface vlanif 10 host 192.168.0.12 group 232.1.1.1
```


Delete information about IGMP host 192.168.0.12 in (10.12.12.12, 232.1.1.1) on VLANIF10.

```
<HUAWEI> reset igmp explicit-tracking interface vlanif 10 host 192.168.0.12 group 232.1.1.1 source 10.12.12.12
```

8.1.50 reset igmp group

Function

The **reset igmp group** command deletes dynamic IGMP entries on interfaces.

Format

reset igmp [**vpn-instance** *vpn-instance-name* | **all-instance**] **group** { **all** | **interface** *interface-type interface-number* { **all** | *group-address* [**mask** { *group-mask* | *group-mask-length* }] [*source-address* [**mask** { *source-mask* | *source-mask-length* }]] } }

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Deletes dynamic IGMP entries in a specified VPN instance.	The value must be an existing VPN instance name.
all-instance	Deletes dynamic IGMP entries in all instances.	-
all	The first **all** deletes dynamic IGMP entries on all interfaces. The second **all** deletes all dynamic IGMP entries on a specified interface.	-
interface *interface-type interface-number*	Deletes dynamic IGMP entries on a specified interface.	-
group-address	Deletes dynamic IGMP entries of a specified group.	The value ranges from 224.0.1.0 to 239.255.255.255, in dotted decimal notation.
mask	Sets the mask of a multicast source address or group address.	-
group-mask	Specifies the mask of a multicast group address.	The mask is in dotted decimal notation.
group-mask-length	Specifies the mask length of a multicast group address.	The value is an integer that ranges from 4 to 32.
source-address	Specifies a multicast source address.	The address is in dotted decimal notation.

Parameter	Description	Value
source-mask	Specifies the mask of a multicast source address.	The mask is in dotted decimal notation.
source-mask-length	Specifies the mask length of a multicast source address.	The value is an integer that ranges from 0 to 32.

Views

User view

Default Level

3: Management level

Usage Guidelines

This command does not delete static group memberships configured on interfaces.

Deleting IGMP entries on an interface does not prevent the interface from joining the involved groups again.

NOTICE

After IGMP group memberships are deleted, group members may fail to receive multicast data. Therefore, exercise caution when using this command.

Example

Delete dynamic IGMP entries on all interfaces.

```
<HUAWEI> reset igmp group all
```

Delete all dynamic IGMP entries on VLANIF100.

```
<HUAWEI> reset igmp group interface vlanif 100 all
```

Delete the IGMP entries of group 225.0.0.1 on VLANIF100.

```
<HUAWEI> reset igmp group interface vlanif 100 225.0.0.1
```

Delete IGMP entries of groups 225.1.1.0 to 225.1.1.255 on VLANIF100.

```
<HUAWEI> reset igmp group interface vlanif 100 225.1.1.0 mask 255.255.255.0
```

8.1.51 reset igmp group ssm-mapping

Function

The **reset igmp group ssm-mapping** command deletes group memberships established with SSM mapping.

Format

reset igmp [**vpn-instance** *vpn-instance-name* | **all-instance**] **group ssm-mapping** { **all** | **interface** *interface-type interface-number* { **all** | *group-address* [**mask** { *group-mask* | *group-mask-length* }] } }

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Deletes group memberships established with SSM mapping in a specified VPN instance.	The value must be an existing VPN instance name.
all-instance	Deletes group memberships established with SSM mapping in all instances.	-
all	First **all**: deletes group memberships established with SSM mapping on all interfaces. Second **all**: deletes all group membership established with SSM mapping on the specified interface.	-
interface *interface-type interface-number*	Deletes group memberships established with SSM mapping on a specified interface.	-
group-address	Deletes the group membership established with SSM mapping for a specified group.	The address is in dotted decimal notation and ranges from 224.0.1.0 to 239.255.255.255.
mask	Sets the mask of a multicast group address.	-
group-mask	Specifies the mask of a multicast group address.	The mask is in dotted decimal notation.
group-mask-length	Specifies the mask length of a multicast group address.	The value is an integer that ranges from 4 to 32.

Views

User view

Default Level

3: Management level

Usage Guidelines

You can use this command to delete group memberships established with SSM mapping.

NOTICE

After IGMP group memberships are cleared, group members may fail to receive multicast data. Therefore, confirm your operation before clearing IGMP group information.

Example

Delete group memberships established with SSM mapping on all the interfaces.

```
<HUAWEI> reset igmp group ssm-mapping all
```

8.1.52 robust-count (IGMP)

Function

The **robust-count** command sets a global robustness variable for an IGMP querier.

The **undo robust-count** command restores the default robustness variable.

By default, the robustness variable of an IGMP querier is 2.

Format

robust-count *robust-value*

undo robust-count

Parameters

Parameter	Description	Value
robust-value	Specifies the robustness variable of an IGMP querier.	The value is an integer that ranges from 2 to 5.

Views

IGMP view of the public network instance, IGMP view of a VPN instance

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The IGMP querier robustness variable specifies the retransmission count of IGMP packets to minimize the impact of packet loss on the network.

On a shared network, a querier maintains IGMP-attached group memberships on an interface. The robustness variable determines the timeout interval of group memberships. The timeout interval of group memberships is calculated using the following formula:

Timeout interval of group memberships = Interval for sending IGMP General Query messages x Robustness variable + Maximum response time

The robustness variable determines the following values:

- Number of times the querier sends General Query messages at startup

  When the querier starts, it sends General Query messages a certain number of times specified by the robustness variable to query members of multicast groups. The interval for sending General Query messages during this process is 1/4 of the interval configured using the **igmp timer query** or **timer query** command.
- In IGMPv2 and IGMPv3, the robustness variable determines the number of times the querier sends Group-Specific Query or Source-and-Group-Specific Query messages.

  When receiving an IGMP Leave message of a multicast group, the querier sends Group-Specific Query messages a certain number of times specified by the robustness variable to check whether the group has members. When the querier receives a Report message indicating that source-group mapping changes, the querier sends Source-and-Group-Specific Query messages a certain number of times specified by the robustness variable. The interval for sending Group-Specific Query messages and Source-and-Group-Specific Query messages can be set using the **igmp lastmember-queryinterval** or **lastmember-queryinterval** command.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command.

Precautions

- A larger robustness variable makes an IGMP querier more robust, but increases the timeout interval of group memberships.
- This command has the same function as the **igmp robust-count** command used in the interface view. The configuration in the IGMP view is globally valid, whereas the configuration in the interface view is valid only for the current interface. The configuration in the interface view takes precedence over the configuration in the IGMP view. The configuration in the IGMP view is used only when no configuration is performed in the interface view.

Example

In the IGMP view, set the robustness variable of an IGMP querier to 3.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] igmp
[HUAWEI-igmp] robust-count 3
```


8.1.53 send-router-alert (IGMP)

Function

The **send-router-alert** command configures the switch to send IGMP messages with the Router-Alert option in IP headers.

The **undo send-router-alert** command configures the switch to send IGMP messages without the Router-Alert option.

By default, IGMP messages sent by the switch contain the Router-Alert option.

Format

send-router-alert

undo send-router-alert

Parameters

None

Views

IGMP view of the public network instance, IGMP view of a VPN instance

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

By default, IGMP messages sent by the switch contain the Router-Alert option in their IP headers. If the switch needs to communicate with a device that does not support the Router-Alert option, run the **undo send-router-alert** command to configure the switch to send IGMP messages without the Router-Alert option. The **send-router-alert** command is usually used together with the **require-router-alert** command.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command.

Precautions

This command has the same function as the **igmp send-router-alert** command used in the interface view. The configuration in the IGMP view is globally valid, whereas the configuration in the interface view takes effect only for the specified interface. The configuration in the interface view takes precedence over the configuration in the IGMP view. The configuration in the IGMP view is used only when no configuration is performed in the interface view.

Example

In the IGMP view, configure the switch to send IGMP messages without the Router-Alert option.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] igmp
[HUAWEI-igmp] undo send-router-alert
```

8.1.54 ssm-mapping (IGMP)

Function

The **ssm-mapping** command configures an SSM mapping rule to map a multicast source to a group address.

The **undo ssm-mapping** command deletes an SSM mapping rule.

By default, no SSM mapping rule is configured.

Format

ssm-mapping *group-address* { *group-mask* | *group-mask-length* } *source-address*

undo ssm-mapping { *group-address* { *group-mask* | *group-mask-length* } [*source-address*] | **static all** }

Parameters

Parameter	Description	Value
group-address	Specifies a multicast group address.	The value ranges from 224.0.1.0 to 239.255.255.255, in dotted decimal notation.
group-mask	Specifies the mask of a multicast group address.	The mask is in dotted decimal notation.
group-mask-length	Specifies the mask length of a multicast group address.	The value is an integer that ranges from 4 to 32.
source-address	Specifies a multicast source address.	The address is in dotted decimal notation.
static all	Deletes all the configured static SSM mapping entries.	-

Views

IGMP view of the public network instance, IGMP view of a VPN instance

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Hosts that support only IGMPv1 and IGMPv2 cannot join SSM groups. To enable multicast devices to provide the SSM service for these hosts, configure SSM mapping on the multicast devices. An SSM mapping entry maps a multicast source to a multicast group. After SSM mapping entries are configured on a multicast device, the device can convert (*, G) information in Report messages of IGMPv1 and IGMPv2 to (S, G) information.

The default range of SSM group addresses is 232.0.0.0 to 232.255.255.255. You can use the **ssm-policy** command to change the address range. All multicast groups out of this range are ASM groups.

The configured SSM mapping entries take effect only after the **igmp ssm-mapping enable** command is run on the interface.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command.

Precautions

- You can configure multiple static SSM mapping entries by running this command several times.
- To delete an SSM mapping entry, run the **undo ssm-mapping** *group-address* { *group-mask* | *group-mask-length* } *source-address* command. The **undo ssm-mapping static all** command deletes all the SSM mapping entries. Do not use this command unless necessary.

Example

In the public network instance, configure an SSM mapping entry to map multicast source address 10.8.8.8 to group address 225.5.5.5/32.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] igmp
[HUAWEI-igmp] ssm-mapping 225.5.5.5 32 10.8.8.8
```

8.1.55 timer other-querier-present (IGMP)

Function

The **timer other-querier-present** command sets the other querier present timer.

The **undo timer other-querier-present** command restores the default value of the other querier present timer.

The formula used to calculate the other querier present timer value is:

Other querier present timer = Robustness variable x Interval for sending IGMP General Query messages + 1/2 x Maximum response time for IGMP query messages

If the robustness variable, the interval for sending IGMP General Query messages, and the maximum response time for IGMP Query messages all use default values, the other querier present timer value is 125 seconds.

Format

timer other-querier-present *interval*

undo timer other-querier-present

Parameters

Parameter	Description	Value
interval	Specifies the other querier present timer value.	The value is an integer that ranges from 60 to 300, in seconds.

Views

IGMP view of the public network instance, IGMP view of a VPN instance

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When a user network segment connects to multiple Layer 3 multicast devices, only one Layer 3 multicast device is elected as the IGMP querier to send Query messages to hosts on the network segment. If the querier fails to send Query messages, group memberships cannot be created or maintained. Non-queriers running IGMPv2 or IGMPv3 start the other querier present timer after they fail in the querier election. If the non-queriers do not receive Query messages from the querier before the timer times out, they consider the querier failed and start a new querier election.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command.

Precautions

- This command applies only to IGMPv2 and IGMPv3.
- This command has the same function as the **igmp timer other-querier-present** command used in the interface view. The configuration in the IGMP view is globally valid, whereas the configuration in the interface view takes effect only for the specified interface. The configuration in the interface view takes precedence over the configuration in the IGMP view. The configuration in the IGMP view is used only when the configuration in the interface view is not done.

NOTICE

If the other querier present timer value is shorter than the interval for sending IGMP General Query messages, the querier election is triggered frequently.

Example

In the IGMP view, set the other querier present timer to 200 seconds.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] igmp
[HUAWEI-igmp] timer other-querier-present 200
```

8.1.56 timer query (IGMP)

Function

The **timer query** command sets a global interval for sending IGMP General Query messages.

The **undo timer query** command restores the default interval for sending IGMP General Query messages.

By default, the interval for sending IGMP General Query messages is 60 seconds.

Format

timer query *interval*

undo timer query

Parameters

Parameter	Description	Value
interval	Specifies the interval for sending IGMP General Query messages	The value is an integer that ranges from 1 to 18000, in seconds.

Views

IGMP view of the public network instance, IGMP view of a VPN instance

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

An IGMP querier checks whether a local network segment has group members by sending IGMP General Query messages at an interval, known as the general query

interval. You can set the general query interval based on needs of your network. The general query interval affects the following processes:

- When the querier starts, it sends General Query messages a certain number of times specified by the robustness variable to query members of multicast groups. The message sending interval during this process is 1/4 of the interval for sending General Query messages. The robustness variable is configured using the **igmp robust-count** or **robust-count** command.
- After the startup process is complete, the querier sends General Query messages at intervals to maintain the group memberships on the interface.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command.

Precautions

- The querier is more sensitive when it sends General Query messages at a shorter interval. However, more bandwidth and switch resources are consumed in this case.
- This command has the same function as the **igmp timer query** command used in the interface view. The configuration in the IGMP view is globally valid, whereas the configuration in the interface view takes effect only for the specified interface. The configuration in the interface view takes precedence over the configuration in the IGMP view. The configuration in the IGMP view is used only when no configuration is performed in the interface view.

Example

In the IGMP view, set the global interval for sending IGMP General Query messages to 125 seconds.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] igmp
[HUAWEI-igmp] timer query 125
```

8.1.57 ttl-check (IGMP)

Function

The **ttl-check** command enables the device to check the TTL values in received IGMP Report, Leave, and Query messages on all interfaces.

The **undo ttl-check** command restores the default configuration.

By default, the device does not check the TTL values in received IGMP Report, Leave, and Query messages.

Format

ttl-check

undo ttl-check

Parameters

None

Views

IGMP view of the public network instance or IGMP view of the VPN instance

Default Level

2: Configuration level

Usage Guidelines

To protect a device against IGMP message attacks, run the **ttl-check** command to enable the device to check the TTL values in received IGMP Report, Leave, and Query messages on all interfaces and discard such a message if its TTL value is not 1.

Example

Enable TTL check for IGMP Report, Leave, and Query messages in the IGMP view.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] igmp
[HUAWEI-igmp] ttl-check
```

8.1.58 version (IGMP)

Function

The **version** command configures a global IGMP version.

The **undo version** command restores the default configuration.

By default, the IGMP version is IGMPv2.

Format

version *version*

undo version

Parameters

Parameter	Description	Value
version	Specifies the IGMP version running on the interface.	The value is integer that ranges from 1 to 3.

Views

IGMP view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The switch can identify IGMP messages of a version earlier than its own IGMP version. To ensure normal IGMP operation, set on the switch an IGMP version the same as or later than that running on user hosts.

If multiple switches exist on a shared network segment, configure the same IGMP version on all switch interfaces connected to hosts. Otherwise, errors may occur in IGMP operation because interfaces running different IGMP versions send packets with different formats.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command.

Precautions

This command functions in the same way as the **igmp version** command used in the interface view, except that the configuration in the IGMP view is globally valid, whereas the configuration in the interface view is valid only for the specified interface. The configuration in the interface view takes precedence over the configuration in the IGMP view. The configuration in the IGMP view is used only when the configuration in the interface view is not done.

Example

Set the IGMP version to IGMPv3 globally.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] igmp
[HUAWEI-igmp] version 3
```

8.2 MLD Configuration Commands

8.2.1 MLD Configuration Commands

Product	Support
S1700	Not supported.
S300	Supported.
S500	Supported.
S2700	Supported.
S5700	Supported except S5731-L and S5731S-L.

Product	Support
S6700	Supported.

8.2.2 display default-parameter mld

Function

The **display default-parameter mld** command displays default MLD configurations.

Format

display default-parameter mld

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run this command to check default MLD parameter settings even after MLD parameters are modified. This command helps you determine which MLD parameters have been modified.

Example

Display default MLD configurations.

```
<HUAWEI> display default-parameter mld
 MLD View Default Configurations:
 --------------------------------
 Lastmember-queryinterval: 1 s
 Lastmember-query time: 2 s
 Max-response-time: 10 s
 Require-router-alert: disabled
 Robust-count: 2
 Send-router-alert: enabled
 Ssm-mapping: disabled
 Timer query: 125 s

 Interface View Default Configurations:
 --------------------------------------
 Group-policy: disabled
 Last listener query time: 2 s
 Lastlistener-query-interval: 1 s
 Max-response-time: 10 s
```



```
Other-querier-present-timer-expiry: off
Prompt-leave: disabled
Require-router-alert: disabled
Robust-count: 2
Send-router-alert: enabled
Ssm-mapping: disabled
Startup-query-timer-expiry: off
Static-group:  disabled
Timer query: 125 s
Version: 2
Ipsec sa: disabled
```

Table 8-19 Description of the **display default-parameter mld** command output

Item	Description
MLD View Default Configurations	Default configurations in the MLD view.
Lastmember-queryinterval	Interval for sending Multicast Address Specific Query messages or Multicast Address and Source Specific Query messages. This parameter is configured using the **lastlistener-queryinterval (MLD view)** command in the MLD view or the **mld lastlistener-queryinterval** command in the interface view.
Lastmember-query time	Last listener query time, equaling Lastmember-query-interval x Robust-count.
Max-response-time	Maximum response time for MLD Query messages. This parameter is configured using the **max-response-time (MLD view)** command in the MLD view or the **mld max-response-time** command in the interface view.
Require-router-alert	Whether the switch checks the Router-Alert option in received MLD messages. This function is configured using the **require-router-alert (MLD view)** command in the MLD view or the **mld require-router-alert** command in the interface view.
Robust-count	Robustness variable of the MLD querier. This parameter is configured using the **robust-count (MLD view)** command in the MLD view or the **mld robust-count** command in the interface view.
Send-router-alert	Whether the MLD messages sent from the switch carry the Router-Alert option. This function is configured using the **send-router-alert (MLD view)** command in the MLD view or the **mld send-router-alert** command in the interface view.

Item	Description
Ssm-mapping	Status of the MLD SSM mapping function. The value can be: ● enabled: This function is enabled. ● disabled: This function is disabled. This function is configured using the **mld ssm-mapping enable** command in the interface view.
Timer query	Interval for sending MLD General Query messages. This parameter is configured using the **timer query (MLD view)** command in the MLD view or the **mld timer query** command in the interface view.
Interface View Default Configurations	Default configurations in the interface view.
Group-policy	Whether a multicast group policy is configured. ● enabled: A multicast group policy is configured. ● disabled: No multicast group policy is configured. A multicast group policy is configured using the **mld group-policy** command.
Last listener query time	Last listener query time, equaling Lastlistener-query-interval x Robust-count.
Lastlistener-query-interval	Interval for sending Multicast Address Specific Query messages or Multicast Address and Source Specific Query messages.
Other-querier-present-timer-expiry	Status of the other querier present timer. ● off: The interface considers itself a querier and no other queriers exist. ● on: The interface no longer considers itself a querier and another querier exists.
Prompt-leave	Whether the fast leave function is configured. This function is configured using the **mld prompt-leave** command.
Startup-query-timer-expiry	Status of the query timer on the interface that functions as the querier. ● off: The interface has sent Query messages. ● on: The interface has not finished sending Query messages.

Item	Description
Static-group	Whether static multicast groups are configured. • enabled: Static multicast groups are configured. • disabled: No static multicast groups are configured. A static multicast group is configured on an interface using the **mld static-group** command.
Version	MLD version number. MLD has two versions: MLDv1 and MLDv2. This parameter is configured using the **mld version** command.
Ipsec sa	Whether IPSec is enabled on the interface. The switch does not support this function.

8.2.3 display mld control-message counters

Function

The **display mld control-message counters** command displays statistics about MLD control messages.

Format

display mld control-message counters [**interface** *interface-type interface-number*] [**message-type** { **query** | **report** }]

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Displays statistics about MLD messages on a specified interface. If this parameter is not specified, the command displays statistics about MLD messages on all interfaces.	-
message-type	Displays statistics about MLD messages of a specified type. If this parameter is not specified, the command displays statistics about all types of MLD messages.	-
query	Displays statistics about Query messages received by the interface. Query messages are sent from a querier.	-
report	Displays statistics about Report messages received by the interface. Report messages are sent by hosts to join a multicast group.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can use this command to check the number of MLD control messages sent and received on an interface.

Example

Display statistics about the MLD messages sent and received by VLANIF100.

```
<HUAWEI> display mld control-message counters interface vlanif 100
Interface message counter information
 Vlanif100(FE80::219:74FF:FE59:3302):
 Message Type              Sent       Valid      Invalid    Ignore
 ------------------------------------------------------------------------
 General Query             45         0          0          0
 Group Query               0          0          0          0
 Source Group Query        0          0          0          0
 ------------------------------------------------------------------------
 MLDV1
 Report ASM                0          35679      0          0
 Report SSM                0          0          0          0
 ------------------------------------------------------------------------
 DONE  ASM                 0          0          0          0
 DONE  SSM                 0          0          0          0
 ------------------------------------------------------------------------
 MLDV2
 ISIN Report               0          0          0          0
 ISEX Report               0          0          0          0
 TOIN Report               0          0          0          0
 TOEX Report               0          0          0          0
 ALLOW Report              0          0          0          0
 BLOCK Report              0          0          0          0
 Source Records Total      0          0          0          0
 ------------------------------------------------------------------------
 Others                    -          -          0          0
 ------------------------------------------------------------------------
```

Table 8-20 Description of the **display mld control-message counters interface vlanif 100** command output

Item	Description
Interface message counter information	Statistics about MLD messages on an interface.
Vlanif100(FE80::219:74FF:FE59:3302)	Interface type and interface number (IPv6 link-local address).
Message Type	Type of the MLD messages.
Sent	Number of MLD messages sent from the interface.

Item	Description
Valid	Number of valid MLD messages received by the interface.
Invalid	Number of invalid MLD messages received by the interface.
Ignore	Number of received MLD messages ignored by the interface.
General Query	Number of MLD General Query messages.
Group Query	Number of MLD Multicast Address Specific Query messages.
Source Group Query	Number of MLD Multicast Address and Source Specific Query messages.
Report ASM	Number of MLDv1 Multicast Listener Report messages with multicast group addresses in the ASM group address range.
Report SSM	Number of MLDv1 Multicast Listener Report messages with multicast group addresses in the SSM group address range.
DONE ASM	Number of MLDv1 Multicast Listener Done messages with multicast group addresses in the ASM group address range.
DONE SSM	Number of MLDv1 Multicast Listener Done messages with multicast group addresses in the SSM group address range.
ISIN Report	Number of MLDv2 Multicast Listener ISIN Report messages.
ISEX Report	Number of MLDv2 Multicast Listener ISEX Report messages.
TOIN Report	Number of MLDv2 Multicast Listener TOIN Report messages.
TOEX Report	Number of MLDv2 Multicast Listener TOEX Report messages.
ALLOW Report	Number of MLDv2 Multicast Listener ALLOW Report messages.
BLOCK Report	Number of MLDv2 Multicast Listener BLOCK Report messages.
Source Records Total	Number of multicast sources carried in MLDv2 messages.

Item	Description
Others	Total number of ignored MLD messages and invalid MLD messages whose types cannot be identified.

8.2.4 display mld explicit-tracking

Function

The **display mld explicit-tracking** command displays information about the MLDv2 hosts that have joined the specific source/group in Include mode.

Format

display mld explicit-tracking [**interface** *interface-type interface-number* [**host-address** *ipv6-host-address* | **group** *ipv6-group-address* **source** *ipv6-source-address*]]

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Displays information about MLDv2 hosts that join a specified multicast source in Include mode on a specified interface. If this parameter is not specified, the command displays information about MLDv2 hosts that join a specified multicast source in Include mode on all interfaces.	-
host-address *ipv6-host-address*	Specifies the link-local address of a host.	The value is a 32-digit hexadecimal number in X:X:X:X:X:X:X:X format. The value ranges from FE80:: to FE80:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF.
group *ipv6-group-address*	Specifies the IPv6 address of a multicast group.	The value is a 32-digit hexadecimal number in X:X:X:X:X:X:X:X format. The value ranges from FF00:: to FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF.

Parameter	Description	Value
source *ipv6-source-address*	Specifies the IPv6 address of a multicast source.	The value is a 32-digit hexadecimal number in X:X:X:X:X:X:X:X format.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can use this command to view information about MLDv2 hosts that have dynamically joined specified sources/groups in Include mode.

Example

Display information about the MLDv2 hosts that have joined the specific source/group in Include mode.

```
<HUAWEI> display mld explicit-tracking
Explicit-tracking information
 Total 2 hosts, 4 entries

 Vlanif100(FE80::2:4)
  0001.Host: FE80::224
       Uptime: 00:02:47
       Expires: 00:01:33
       (S, G) List:
         Group: FF44::1
             Source: FC00:0:0:1::1
               Uptime: 00:02:47
               Time since last refresh: 00:02:47
             Source: FC00:0:0:2222::3
               Uptime: 00:02:47
               Time since last refresh: 00:02:47
  0002.Host: FE80::225
       Uptime: 00:01:59
       Expires: 00:02:21
       (S, G) List:
         Group: FF44::1
             Source: FC00:0:0:1::1
               Uptime: 00:01:59
               Time since last refresh: 00:01:59
             Source: FC00:0:0:1::3
               Uptime: 00:01:59
               Time since last refresh: 00:01:59
```

Table 8-21 Description of the **display mld explicit-tracking** command output

Item	Description
Explicit-tracking information	Host information.

Item	Description
Total 2 hosts, 4 entries	Two hosts and four (S, G) entries in total.
Vlanif100(FE80::2:4)	Interface type and interface number (IPv6 link-local address).
Host	IPv6 host address.
Uptime	Running time after a host joins a multicast group. The time format is as follows: ● If the time is shorter than or equal to 24 hours, the format is hours:minutes:seconds. ● If the time is longer than 24 hours but shorter than or equal to one week, the format is days:hours. ● If the time is longer than one week, the format is weeks:days.
Expires	Predicted timeout period of a host. After the host times out, the host is deleted from the MLD member list. The time format is as follows: ● If the time is shorter than or equal to 24 hours, the format is hours:minutes:seconds. ● If the time is longer than 24 hours but shorter than or equal to one week, the format is days:hours. ● If the time is longer than one week, the format is weeks:days.
(S, G) List	List of (S, G) entries.
Group	IPv6 multicast group address.
Source	IPv6 unicast address of a multicast source.
Time since last refresh	Time since the host joins a multicast group last time. The time format is as follows: ● If the time is shorter than or equal to 24 hours, the format is hours:minutes:seconds. ● If the time is longer than 24 hours but shorter than or equal to one week, the format is days:hours. ● If the time is longer than one week, the format is weeks:days.

8.2.5 display mld group

Function

The **display mld group** command displays information about MLD groups that hosts have dynamically joined by sending Report messages.

Format

display mld group [*ipv6-group-address* | **interface** *interface-type interface-number*]* [**verbose**]

display mld group [**interface** *interface-type interface-number*] **entry-number**

Parameters

Parameter	Description	Value
ipv6-group-address	Specifies an IPv6 multicast group address.	The value is a 32-digit hexadecimal number in X:X:X:X:X:X:X:X format. The value ranges from FF00:: to FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF.
interface *interface-type interface-number*	Specifies the type and number of an interface. If this parameter is not specified, the command displays MLD group membership information on all interfaces.	-
verbose	Displays detailed information about a multicast group. If this parameter is not specified, the command displays only the summary of the MLD group.	-
entry-number	Displays statistics about MLD multicast groups that hosts dynamically join.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can use this command to check information about multicast groups that have established memberships.

Example

Display detailed information about all multicast groups that the interface dynamically joins.

```
<HUAWEI> display mld group verbose
Total entry on this router: 1
Interface group report information of VPN-Instance: public net
 Limited entry of this VPN-Instance: -
 Vlanif100(FE80::2E0:49FF:FE29:1103):
  Total entry on this interface: 1
  Limited entry on this interface: -
  Total 1 MLD Group reported
   Group: FF05::2
     Uptime: 00:01:07
     Expires: 00:03:45
     Last reporter: FE80::215:E9FF:FEAC:7666
     Last-listener-query-counter: 0
     Last-listener-query-timer-expiry: off
     Group mode: exclude
     Version1-host-present-timer-expiry: 00:03:45
```

Display statistics about MLD multicast groups that hosts dynamically join.

```
<HUAWEI> display mld group entry-number
Interface group report information of VPN-Instance: public net
  Total 100 MLD Groups reported
 Vlanif100(FE80:2300::4):
  Total 100 MLD Groups reported
```

Table 8-22 Description of the **display mld group** command output

Item	Description
Interface group report information of VPN-Instance	VPN instance to which MLD groups on an interface belong. **public net** indicates the public network instance.
Total entry on this router	Total number of dynamic MLD multicast groups on the switch.
Limited entry of this VPN-Instance	Maximum number of MLD entries that can be created for this instance.
Vlanif100(FE80::2E0:49FF:FE29:1103)	Interface type and interface number (IPv6 link-local address).
Total entry on this interface	Total number of dynamic MLD multicast groups on the interface.

Item	Description
Limited entry on this interface	Maximum number of MLD entries that the current interface can create.
Total 1 MLD Group reported	One MLD Report message is received on the interface.
Group	IPv6 address of an IPv6 multicast group.
Uptime	Time since a multicast group is discovered. The time format is as follows: ● If the time is shorter than or equal to 24 hours, the format is hours:minutes:seconds. ● If the time is longer than 24 hours but shorter than or equal to one week, the format is days:hours. ● If the time is longer than one week, the format is weeks:days.
Expires	Time left before a group will be deleted from the MLD group table. The time format is as follows: ● If the time is shorter than or equal to 24 hours, the format is hours:minutes:seconds. ● If the time is longer than 24 hours but shorter than or equal to one week, the format is days:hours. ● If the time is longer than one week, the format is weeks:days. "off" indicates that the group will never be aged out.
Last reporter	Link-local address of the last host that sends a Multicast Listener Report message.

Item	Description
Last-listener-query-counter	Number of Multicast Address and Source Specific Query messages sent by the querier. After the querier receives an MLD done message sent from a host leaving a group, it sends the specified number of Multicast Address and Source Specific Query messages to check whether this group has other members on the network segment. The Last-listener-query-counter value reduces by 1 every time the querier sends a Multicast Address and Source Specific Query message. The number of times is configured using the **mld robust-count** command.
Last-listener-query-timer-expiry	The timeout time of the Multicast Address and Source Specific Query timer. The timer starts when the querier receives an MLD done message sent from a host leaving a group. The timer value is configured using the **mld lastlistener-queryinterval** command.
Group mode	Filter mode of multicast groups, that is, exclude or include.
Version1-host-present-timer-expiry	Timeout time of MLDv1 hosts. The timer value is calculated using the following formula: Timer value = General query interval x Robustness variable + Maximum response time for Query messages. The three parameters used in the formula are configured using the **mld timer query**, **mld robust-count**, and **mld max-response-time** commands respectively.

8.2.6 display mld group ssm-mapping

Function

The **display mld group ssm-mapping** command displays information about multicast group entries established with MLD SSM mapping.

Format

display mld group [*ipv6-group-address* | **interface** *interface-type interface-number*]* **ssm-mapping** [**verbose**]

display mld group ssm-mapping [**interface** *interface-type interface-number*] **entry-number**

Parameters

Parameter	Description	Value
ipv6-group-address	Specifies an IPv6 multicast group address. If this parameter is not specified, the command displays information about all multicast group entries established with SSM mapping.	The value is a 32-digit hexadecimal number in X:X:X:X:X:X:X:X format. The value ranges from FF00:: to FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF.
interface *interface-type interface-number*	Displays information about the multicast group entries established with SSM mapping on a specified interface. If this parameter is not specified, the command displays information about multicast group entries established with SSM mapping on all interfaces.	-
verbose	Displays detailed information about multicast group entries established with SSM mapping. If this parameter is not specified, the command displays only the summary of multicast groups mapped by SSM mapping.	-
entry-number	Displays statistics about MLD multicast groups established with SSM mapping.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can use the **display mld group ssm-mapping** command to view information about multicast group entries that are established with SSM mapping. SSM mapping entries can be configured using the **ssm-mapping (MLD view)** command.

Example

Display detailed information about all multicast group entries established with SSM mapping.

```
<HUAWEI> display mld group ssm-mapping verbose
Total entry on this router: 1
Interface group report information of VPN-Instance: public net
 Limited entry of this VPN-Instance: -
 Vlanif100(FE80::DD:84):
  Total entry on this interface: 1
  Limited entry on this interface: -
  Total 1 MLD SSM-Mapping Group reported
   Group: FF36::1
     Uptime: 00:00:13
     Expires: 00:04:07
     Last reporter: FE80::10
     Last-listener-query-counter: 0
     Last-listener-query-timer-expiry: off
     Group mode: exclude
     Version1-host-present-timer-expiry: 00:04:07
```

Display detailed information about MLD multicast groups established with SSM mapping.

```
<HUAWEI> display mld group ssm-mapping entry-number
Interface group report information of VPN-Instance: public net
  Total 100 MLD SSM-Mapping Groups reported
 Vlanif100(FE80:2300::4):
  Total 100 MLD SSM-Mapping Groups reported
```

Table 8-23 Description of the **display mld group ssm-mapping** command output

Item	Description
Interface group report information of VPN-Instance	VPN instance to which MLD groups on an interface belong. **public net** indicates the public network instance.
Total entry on this router	Number of multicast group entries established with SSM mapping on the switch.
Limited entry of this VPN-Instance	Maximum number of multicast group entries that can be generated in the VPN instance.
Vlanif100(FE80::DD:84)	Interface type and interface number (IPv6 link-local address).

Item	Description
Total entry on this interface	Number of multicast group entries established with SSM mapping on the interface.
Limited entry on this interface	Maximum number of multicast group entries that can be generated on the interface.
Total 1 MLD SSM-Mapping Group reported	Total number of SSM mapping groups is 1.
Group	Multicast group address.
Uptime	Time since a multicast group is discovered. The time format is as follows: ● If the time is shorter than or equal to 24 hours, the format is hours:minutes:seconds. ● If the time is longer than 24 hours but shorter than or equal to one week, the format is days:hours. ● If the time is longer than one week, the format is weeks:days.
Expires	Timeout period of a group. The time format is as follows: ● If the time is shorter than or equal to 24 hours, the format is hours:minutes:seconds. ● If the time is longer than 24 hours but shorter than or equal to one week, the format is days:hours. ● If the time is longer than one week, the format is weeks:days.
Last reporter	Link-local address of the last host that sends a Multicast Listener Report message.
Last-listener-query-counter	Number of times for sending Multicast Address Specific Query messages or Multicast Address and Source Specific Query messages.
Last-listener-query-timer-expiry	Interval for sending Multicast Address Specific Query messages or Multicast Address and Source Specific Query messages.
Group mode	Filter mode of the multicast group, that is, include or exclude.
Version1-host-present-timer-expiry	Timeout period of an MLDv1 host.

8.2.7 display mld group static

Function

The **display mld group static** command displays information about static MLD multicast groups on interfaces.

Format

display mld group [*ipv6-group-address*] **static** [**up** | **down**] [**verbose**]

display mld group [*ipv6-group-address*] **static interface-number**

display mld group [*ipv6-group-address* | **interface** *interface-type interface-number*]* **static** [**verbose**]

display mld group static interface *interface-type interface-number* **entry-number**

Parameters

Parameter	Description	Value
ipv6-group-address	Specifies an IPv6 multicast group address. If this parameter is not specified, the command displays information about all multicast groups with memberships.	The value is a 32-digit hexadecimal number in X:X:X:X:X:X:X:X format. The value ranges from FF00:: to FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF.
up | **down**	Displays information about an Up or Down interface. If this parameter is not specified, the command displays information about all interfaces.	-
verbose	Displays detailed information about the interfaces that statically join MLD multicast groups or source-specific multicast groups. If this parameter is not specified, the command displays only the summary of the MLD group.	-

Parameter	Description	Value
interface-number	Displays the number of the interfaces that statically join MLD multicast groups.	-
interface *interface-type interface-number*	Displays information about the MLD multicast groups that the specified interface statically joins.	-
entry-number	Displays the number of the MLD multicast groups that the interface statically joins.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display mld group static** command to view information about the multicast groups and the interfaces that statically join MLD multicast groups or source-specific multicast groups. To configure a static multicast group on an interface, run the **mld static-group** command.

Example

Display information about statically joined MLD groups.

```
<HUAWEI> display mld group static
Static join group information
 Total 2 entries, Total 2 active entries
  (*, FF25::1)
  Interface:Vlanif10
  State:UP
  Expires:Never

  (*, FF25:100::1)
  Interface:Vlanif10
  State:UP
  Expires:Never
```


Table 8-24 Description of the **display mld group static** command output

Item	Description
Static join group information	Information about the MLD multicast groups that a switch statically joins.
Total 2 entries, Total 2 active entries	Total number of static multicast groups and active entries set on the switch.
(*, FF25::1)	(*, G) entry.
Interface:Vlanif10	Interface where the multicast group exists.
State	Status of an entry.
Expires	Timeout period of a multicast group.

Display detailed information about all static MLD multicast groups on an interface.

```
<HUAWEI> display mld group static verbose
Static join group information
 Total 1 entry
  00001.(*, FF25::1)
     Total List of 2 joined interfaces
     1.Vlanif10
        State:            UP
        Reference Count:   1
        Multicast Boundary:YES
        Outgoing Interface:YES
     2.Vlanif20
        State:            UP
        Reference Count:   1
        Multicast Boundary:YES
        Outgoing Interface:YES
```

Table 8-25 Description of the **display mld group static verbose** command output

Item	Description
Static join group information	Information about the multicast groups that an interface statically joins.
Total 1 entry	Number of static MLD group memberships on the device.
00001.(*, FF25::1)	(*, G) entry.
Total List of 2 joined interfaces	List of the interfaces that statically join multicast groups.
1.Vlanif10	Type and number of the interface.

Item	Description
State	Status of an interface, including: ● UP: The interface is working properly. ● DOWN: An error occurs on the physical link of the interface.
Reference Count	Number of times when a multicast group on the current interface is referenced.
Multicast Boundary	Whether the multicast forwarding boundary is configured. ● YES ● NO This function is configured using the **multicast boundary** *ipv6-group-address ipv6-group-mask-length* command.
Outgoing Interface	Whether downstream interfaces are available. ● YES ● NO

Display information about all the interfaces that statically join multicast groups and are in Up state.

```
<HUAWEI> display mld group static up
Static join group information
 Total 4 entries
  00001.(*,FF25::1)
     Total List of 2 joined interfaces
     Total Matched 2 interfaces
     1.Vlanif10
     2.Vlanif20
  00002.(FC00:0:0:1::1,FF25::1)
     Total List of 2 joined interfaces
     Total Matched 2 interfaces
     1.Vlanif10
     2.Vlanif20
```

Table 8-26 Description of the **display mld group static up** command output

Item	Description
Total List of 2 joined interfaces	Number of the interfaces that statically join multicast groups.
Total Matched 2 interfaces	List of the interfaces that statically join multicast groups and are in Up state.

Display the number of interfaces that statically join all multicast groups.

```
<HUAWEI> display mld group static interface-number
Static join group information
 Total 2 entries
  (*, FF25::1)
  Interface-Number:24

  (*, FF25::2)
  Interface-Number:24
```

Table 8-27 Description of the **display mld group static interface-number** command output

Item	Description
Interface-Number	Number of the interfaces that statically join multicast groups.

8.2.8 display mld interface

Function

The **display mld interface** command displays MLD information on an interface.

Format

display mld interface [*interface-type interface-number* | **up** | **down**] [**verbose**]

Parameters

Parameter	Description	Value
interface-type interface-number	Displays MLD information on a specified interface. If this parameter is not specified, the command displays MLD information on all interfaces.	-
up	Indicates that the status of the IPv6 protocol on the MLD interface is Up, that is, MLD is in Active state.	-
down	Indicates that the status of the IPv6 protocol on the MLD interface is Down, that is, MLD is in Inactive state.	-
verbose	Displays detailed information about MLD interfaces.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

To check the MLD configuration and running status on an interface, run the **display mld interface** command. This command displays MLD information only when MLD-enabled interfaces exist on the device.

Example

Display the MLD configuration and running status on VLANIF100.

```
<HUAWEI> display mld interface vlanif 100 verbose
Interface information
 Vlanif100(FE80::2E0:B4FF:FE35:FF01):
   MLD is enabled
   Current MLD version is 2
   MLD state: up
   MLD group policy: none
   MLD limit: -
   Value of query interval for MLD (negotiated): 125 s
   Value of query interval for MLD (configured): 125 s
   Value of other querier timeout for MLD: 0 s
   Value of maximum query response time for MLD: 10 s
   Value of last listener query time: 2 s
   Value of last listener query interval: 1 s
   Value of startup query interval: 31 s
   Value of startup query count: 2
   General query timer expiry (hours:minutes:seconds): 00:00:28
   Querier for MLD: FE80::2E0:B4FF:FE35:FF01 (this router)
   MLD activity: 2 joins, 0 dones
   Robustness (negotiated): 2
   Robustness (configured): 2
   Require-router-alert: disabled
   Send-router-alert: enabled
   Ip-source-policy: disabled
   Query Ip-source-policy: disabled
   Prompt-leave: disabled
   SSM-Mapping: enabled
   Startup-query-timer-expiry: off
   Other-querier-present-timer-expiry: off
    TTL-check: disabled
 Total 2 MLD Groups reported
```

Table 8-28 Description of the **display mld interface** command output

Item	Description
Vlanif100(FE80::2E0:B4FF:FE35:FF01)	Interface type and interface number (IPv6 link-local address).
MLD is enabled	MLD is enabled. To enable MLD, run the **mld enable** command.
Current MLD version is 2	MLD version is set to 2 on the interface. To set the MLD version, run the **mld version** command.
MLD state	Status of the MLD interface, that is, up or down.

Item	Description
MLD group policy	ACL6 number of the MLD group policy. To set ACL6 number of the MLD group policy, run the **mld group-policy** command.
MLD limit	Maximum number of MLD group members that the current interface can maintain. To set the maximum number of MLD group members that the current interface can maintain, run the **mld limit** command.
Value of query interval for MLD (negotiated)	Actual interval for sending MLD Query messages after negotiation, in seconds.
Value of query interval for MLD (configured)	Configured interval for sending MLD Query messages, in seconds. To set the interval for sending MLD Query messages, run the **mld timer query** command.
Value of other querier timeout for MLD	Timeout period of other MLD queriers, in seconds. To set the timeout period of an MLD querier, run the **mld timer other-querier-present** command.
Value of maximum query response time for MLD	Maximum response time for MLD Query messages, in seconds. To set the maximum response time for MLD Query messages, run the **mld max-response-time** command.
Value of last listener query time	Last listener query time, in seconds. The last listener query time is calculated by multiplying the interval for sending Multicast Address Specific Query messages or Multicast Address and Source Specific Query messages by the robustness variable.
Value of last listener query interval	Interval for sending Multicast Address Specific Query messages or Multicast Address and Source Specific Query messages (Last listener query), in seconds. To set the interval for sending Last listener query, run the **mld lastlistener-queryinterval** command.

Item	Description
Value of startup query interval	Interval for sending Query messages when a querier starts, in seconds. The interval is 1/4 the query interval configured using the **mld timer query** command.
Value of startup query count	Number of times the querier sends Query messages when a querier starts. To set the number of times for sending Query messages when the querier starts, run the **mld robust-count** command.
General query timer expiry (hours:minutes:seconds)	Timeout period of the general query timer.
Querier for MLD	Link-local address of the MLD querier.
MLD activity	Statistics about MLD activities (join or leave).
Robustness (negotiated)	Robustness variable after negotiation by the non-querier device.
Robustness (configured)	Robustness variable set on the interface. To set the robustness variable on an interface, run the **mld robust-count** command.
Require-router-alert	Whether the switch discards MLD packets that do not contain the Router-Alert option in IP packet headers. • enable: The switch discards MLD packets that do not contain the Router-Alert option in IP packet headers. • disable: The switch does not discard MLD packets that do not contain the Router-Alert option in IP packet headers. This function is configured using the **mld require-router-alert** command.

Item	Description
Send-router-alert	Whether the sent MLD packet carries the Router-Alert option. To configure whether the sent MLD packet carries the Router-Alert option, run the **mld send-router-alert** command.
Ip-source-policy	Whether to filter Multicast Listener Report/Done messages based on host addresses. ● enabled: The switch filters MLD Report/Leave messages based on host addresses. ● disabled: The switch does not filter MLD Report/Leave messages based on host addresses. This function is configured using the **mld ip-source-policy** command.
Query Ip-source-policy	Whether to filter MLD Query messages based on host addresses. To configure whether to filter MLD Query messages based on host addresses, run the **mld query ip-source-policy** command.
Prompt-leave	Whether fast leave is enabled. ● enabled: Fast leave is enabled. ● disabled: Fast leave is disabled. This function is configured using the **mld prompt-leave** command.
SSM-Mapping	Whether SSM mapping is enabled. ● enabled: SSM mapping is enabled. ● disabled: SSM mapping is disabled. This function is configured using the **mld ssm-mapping enable** command.

Item	Description
Startup-query-timer-expiry	Status of the timer for the interface functioning as the querier after startup to send Query messages. ● off: The interface sends Query messages immediately after startup. ● on: The interface delays sending Query messages after startup.
Other-querier-present-timer-expiry	Status of the timer identifying whether another querier is present. ● off: The interface considers itself a querier and no other queriers exist. ● on: The interface no longer considers itself a querier and another querier exists.
TTL-check	Whether the function to check the TTL values in received MLD Report, Leave, and Query messages is enabled: ● enabled ● disabled
Total 2 MLD Groups reported	Two Multicast Listener Report messages are received on the interface.

8.2.9 display mld invalid-packet

Function

The **display mld invalid-packet** command displays statistics and details about invalid MLD packets received by a device.

Format

display mld invalid-packet [**interface** *interface-type interface-number* | **message-type** { **done** | **query** | **report** }]*

display mld invalid-packet [*packet-number*] **verbose**

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Displays statistics about invalid MLD messages received by a specified interface. If this parameter is not specified, the command displays statistics about invalid MLD messages on all interfaces.	-
message-type	Displays statistics about invalid MLD messages of a specified type.	-
done	Displays statistics about invalid Multicast Listener Done messages.	-
query	Displays statistics about invalid Query messages.	-
report	Displays statistics about invalid Multicast Listener Report messages.	-
packet-number	Displays details of a specified number of invalid MLD messages recently received.	The value is an integer that ranges from 1 to 100.
verbose	Displays details of invalid MLD messages.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display mld invalid-packet** command to view statistics and details of invalid MLD messages for fault location and rectification.

If MLD entries fail to be generated on a multicast network, you can run the **display mld invalid-packet** command first to check whether devices have received invalid MLD messages. If the command output contains statistics about invalid MLD messages, you need to run the **display mld invalid-packet** [*packet-number*] **verbose** command to view details of invalid MLD messages to locate the fault.

You can run the following related commands to view information about specific invalid MLD messages:

- Run the **display mld invalid-packet** command to view statistics about invalid MLD messages received by a device.
- Run the **display mld invalid-packet interface** *interface-type interface-number* command to view statistics about invalid MLD messages received by a specified interface.

- Run the **display mld invalid-packet** *packet-number* **verbose** command to view details of invalid MLD messages recently received. Currently, details of a maximum of 100 invalid MLD messages can be displayed.

Example

Display statistics about invalid MLD messages received by the device.

```
<HUAWEI> display mld invalid-packet
        Statistics of invalid packets for public net:
------------------------------------------------------------------------------
MLD Query invalid packet:
Unwanted Source List    : 1000        Zero Max Resp Code      : 0
Fault Length            : 1000        Invalid Multicast Group : 0
Bad Checksum            : 0

MLD Report invalid packet:
Fault Length            : 0           Invalid Multicast Group : 0
Invalid Multicast Source: 0           Bad Checksum            : 0
Illegal Report Type     : 0

MLD Done invalid packet:
Invalid Multicast Group : 0           Bad Checksum            : 0
------------------------------------------------------------------------------
```

Table 8-29 Description of the **display mld invalid-packet** command output

Item	Description
Statistics of invalid packets for public net	Invalid packets received in the public net.
MLD Query invalid packet	Invalid MLD Query messages.
Unwanted Source List	Messages with unwanted source lists.
Zero Max Resp Code	Messages with the Max Resp Code fields being 0.
Fault Length	Messages with invalid lengths.
Invalid Multicast Group	Messages with invalid multicast group addresses.
Bad Checksum	Messages with checksum errors.
MLD Report invalid packet	Invalid MLD Report messages.
Invalid Multicast Source	Messages with invalid multicast source addresses.
Illegal Report Type	Messages with the illegal Report message type.
MLD Done invalid packet	Invalid Multicast Listener Done messages.

Display details of one invalid MLD message recently received by the device.

```
<HUAWEI> display mld invalid-packet 1 verbose
    Detailed information of invalid packets
```



```
-------------------------------------------------------
Packet information (Index 1):
-------------------------------------------------------
Interface          : Vlanif100
Time               : 2012-06-09 11:03:51 UTC-08:00
Message Length     : 24
Invalid Type       : Invalid Multicast Group
0000: 84 00 4c d7 00 00 00 00 11 17 00 00 00 00 00 00
0010: 00 00 00 00 00 01 00 01
-------------------------------------------------------
```

Table 8-30 Description of the **display mld invalid-packet 1 verbose** command output

Item	Description
Detailed information of invalid packets	Details of the invalid MLD message.
Packet information (Index 1)	Sequence number of the invalid MLD message (numbered in the opposite order that the message is received).
Interface	Interface receiving the invalid MLD message.
Time	Time when the invalid MLD message is received, in any of the following formats: ● YYYY-MM-DD HH:MM:SS ● YYYY-MM-DD HH:MM:SS UTC±HH:MM DST ● YYYY-MM-DD HH:MM:SS UTC±HH:MM ● YYYY-MM-DD HH:MM:SS DST UTC±HH:MM indicates that a time zone is configured using the **clock timezone** command; DST indicates that the daylight saving time is configured using **clock daylight-saving-time** command.
Message Length	Length of the invalid MLD message.
Invalid Type	Type of the invalid MLD message: ● Unwanted Source List ● Zero Max Resp Code ● Fault Length ● Invalid Multicast Group ● Bad Checksum ● Invalid Multicast Source ● Illegal Report Type
0000: 84 00 4c d7 00 00 00 00 11 17 00 00 00 00 00 00 0010: 00 00 00 00 00 01 00 01	Contents of the invalid MLD message.

8.2.10 display mld routing-table

Function

The **display mld routing-table** command displays information about the MLD routing table.

Format

display mld routing-table [*ipv6-source-address* [*ipv6-source-mask-length*] | *ipv6-group-address* [*ipv6-group-mask-length*]] * [**static**] [**outgoing-interface-number** [*number*]]

Parameters

Parameter	Description	Value
ipv6-source-address	Specifies the IPv6 address of a multicast source.	The value is a 32-digit hexadecimal number in X:X:X:X:X:X:X:X format.
ipv6-source-mask-length	Specifies the mask length of the IPv6 address of a multicast source.	The value is an integer that ranges from 0 to 128.
ipv6-group-address	Specifies an IPv6 multicast group address.	The value is a 32-digit hexadecimal number in X:X:X:X:X:X:X:X format. The value ranges from FF00:: to FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF.
ipv6-group-mask-length	Specifies the mask length of the IPv6 multicast group address.	The value is an integer that ranges from 8 to 128.
static	Displays the MLD routing table of the static multicast group.	-
outgoing-interface-number	Displays the number of the outbound interfaces in MLD routing entries.	-

Parameter	Description	Value
number	Specifies the number of outbound interfaces. After this parameter is specified, the command displays information about the specified number of outbound interfaces.	The value is an integer that ranges from 1 to 2048.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

To view MLD routing entries, run the **display mld routing-table** command. You can specify parameters to view specified routing information, which facilitates fault location.

NOTE

This command provides output information only when PIM (IPv6) is not enabled on the MLD-capable interface.

Example

Display the MLD routing entry of the specified multicast group.

```
<HUAWEI> display mld routing-table
Routing table
 Total 2 entries

 00001. (FC00:0:0:1::3, FF44::)
      List of 1 downstream interface in include mode
       Vlanif100 (FE80::EE:53),
                 Protocol: STATIC

 00002. (*, FF55::)
      List of 1 downstream interface
       Vlanif100 (FE80::EE:53),
                 Protocol: MLD
```


Table 8-31 Description of the **display mld routing-table** command output

Item	Description
Routing table	MLD routing table.
Total 2 entries	Total number of MLD routing entries.
00001. (FC00:0:0:1::3, FF44::)	Entry 00001. (S, G) indicates that data is transmitted from S to G. (*, G) indicates that data is transmitted from any source to G.
List of 1 downstream interface in include mode	List of the downstream interfaces that join the multicast group in INCLUDE mode.
Vlanif100(FE80::EE:53)	Interface type and interface number (IPv6 link-local address).
Protocol	Protocol type. • SSM-MAP: Entries are generated using MLD SSM mapping. • MLD: Entries are generated using MLD. • STATIC: Entries are generated by the MLD static multicast group.
List of 1 downstream interface	Downstream interface list.

8.2.11 display mld ssm-mapping

Function

The **display mld ssm-mapping** command displays the configuration of MLD SSM mapping.

Format

display mld ssm-mapping { **group** [*ipv6-group-address*] | **interface** [*interface-type interface-number*] }

Parameters

Parameter	Description	Value
group *ipv6-group-address*	Specifies the source IPv6 address of a specified multicast group.	The value is a 32-digit hexadecimal number in X:X:X:X:X:X:X:X format. The value ranges from FF00:: to FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF.

Parameter	Description	Value
interface *interface-type interface-number*	Displays whether a specified interface is enabled with SSM mapping. If this parameter is not specified, the command displays information about all Up interfaces enabled with SSM mapping.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run this command to view multicast sources mapped to a multicast group. SSM mapping entries can be configured using the **ssm-mapping (MLD view)** command. The **display mld ssm-mapping** command also allows you to view the SSM mapping status on an interface, which can be configured using the **mld ssm-mapping enable** command.

Example

Display information about the interface configured with SSM mapping.

```
<HUAWEI> display mld ssm-mapping interface
Interface information
Vlanif100(FE80::1)
```

Table 8-32 Description of the **display mld ssm-mapping interface** command output

Item	Description
Vlanif100(FE80::1)	Interface type and interface number (IPv6 address).

Display information about SSM mapping of all multicast sources and groups.

```
<HUAWEI> display mld ssm-mapping group
MLD SSM-Mapping conversion table
 Group: FF3E::/64
  Number of Source(s): 3
    FC00:0:0:1::1
```



```
    FC00:0:0:1::2
    FC00:0:0:1::3
```

Table 8-33 Description of the **display mld ssm-mapping group** command output

Item	Description
MLD SSM-Mapping conversion table	MLD SSM mapping entries.
Group	Address of a multicast group.
Number of Source(s)	Number of multicast sources configured with SSM mapping.
FC00:0:0:1::1	Multicast source address.

Check whether MLD SSM mapping is enabled on VLANIF100.

```
<HUAWEI> display mld ssm-mapping interface Vlanif 100
MLD SSM-Mapping is enabled
```

Table 8-34 Description of the **display mld ssm-mapping interface Vlanif 100** command output

Item	Description
MLD SSM-Mapping is enabled	SSM mapping is enabled on the interface.

8.2.12 display mld ssm-mapping interface

Function

The **display mld ssm-mapping interface** command displays information about interfaces enabled with SSM mapping.

Format

display mld ssm-mapping interface [*interface-type interface-number* [**group** *ipv6-group-address*]]

Parameters

Parameter	Description	Value
interface-type interface-number	Specifies an interface.	-

Parameter	Description	Value
group *ipv6-group-address*	Displays the source address list associated with a specified group.	The value is a 32-digit hexadecimal number in X:X:X:X:X:X:X:X format. The value ranges from FF00:: to FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can use the **display mld ssm-mapping interface** command to view information about an interface enabled with SSM mapping.

Example

Display information about the interface configured with SSM mapping.

```
<HUAWEI> display mld ssm-mapping interface
Interface information
 Vlanif100(FE80::1)
```

Table 8-35 Description of the **display mld ssm-mapping interface** command output

Item	Description
Vlanif100(FE80::1)	Interface type and interface number (IPv6 link-local address).

8.2.13 lastlistener-queryinterval (MLD view)

Function

The **lastlistener-queryinterval** command globally sets the interval for sending Multicast Address Specific Query messages or Multicast Address and Source Specific Query messages after the MLD querier receives an MLD Done message from a host.

The **undo lastlistener-queryinterval** command restores the default value.

By default, the interval for sending Multicast Address Specific Query messages or Multicast Address and Source Specific Query messages is 1 second.

Format

lastlistener-queryinterval *interval*

undo lastlistener-queryinterval

Parameters

Parameter	Description	Value
interval	Specifies the interval for sending Multicast Address Specific Query messages or Multicast Address and Source Specific Query messages after the MLD querier receives a Multicast Listener Done message.	The value is an integer that ranges from 1 to 5, in seconds.

Views

MLD view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the MLD querier receives a Multicast Listener Done message of a multicast group, the querier sends Multicast Address Specific Query messages or Multicast Address and Source Specific Query messages continuously to check for other members in the multicast group. The **lastlistener-queryinterval** command sets the interval at which the querier sends Multicast Address Specific Query messages or Multicast Address and Source Specific Query messages. If the querier receives no Multicast Listener Report message for a specified period, the querier stops forwarding data to the multicast group. The period is calculated by multiplying *interval* by *robust-value*. To set *robust-value*, run the **mld robust-count** or **robust-count (MLD view)** command.

If the querier receives a Multicast Listener Report message from a host within the maximum response time, the querier maintains the membership of the multicast group. Otherwise, the querier considers that the last member has left the group and does not maintain the membership of the multicast group.

Prerequisites

Layer 3 IPv6 multicast has been enabled using the **multicast ipv6 routing-enable** command in the system view.

Precautions

The function of this command is the same as that of the **mld lastlistener-queryinterval** command used in the interface view. The configuration in the MLD view is globally valid, whereas the configuration in the interface view takes effect

only for the specified interface. The configuration in the interface view takes precedence over the configuration in the MLD view. The configuration in the MLD view is used only when no configuration is performed in the interface view.

Example

In the MLD view, set the interval for sending Multicast Address Specific Query messages or Multicast Address and Source Specific Query messages to 3 seconds.

```
<HUAWEI> system-view
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] mld
[HUAWEI-mld] lastlistener-queryinterval 3
```

8.2.14 limit (MLD view)

Function

The **limit** command sets the maximum number of MLD entries that can be created globally.

The **undo limit** command restores the maximum number of MLD entries that can be created globally to the default value.

The following lists the maximum number of MLD entries allowed on each model by default:

- S5720-LI, S5720S-LI: 496
- S5735S-H, S5736-S, S6720S-S: 512
- S5731-S, S5731S-S, S5720I-SI: 1024
- S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735S-S, S5735-S-I: 1500
- S5731-H, S5731S-H, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, S6730S-S: 4096

Format

limit *number*

undo limit

Parameters

Parameter	Description	Value
number	Specifies the maximum number of MLD entries that can be created globally.	The value is an integer that ranges from 1 to *The maximum number of MLD entries allowed by default*. **NOTE** The value range of S5731-H, S5731S-H, S5732-H, S6730S-H, and S6730-H are expanded after the high specification mode is configured for multicast forwarding using the **set multicast forwarding-table super-mode** command. The actual value range depends on the specification of the device.

Views

MLD view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

This command sets the maximum number of MLD entries globally.

When the number of MLD entries reaches the limit, the system no longer creates MLD entries. To enable the switch to allow new join requests, you can either delete useless entries or increase the limit. Alternatively, configure static multicast groups or source-group bindings on interfaces.

The number of MLD entries can be counted in the following methods:

- Each (*, G) entry is counted as one entry.
- Each (S, G) entry is counted as one entry.
- Each (*, G) entry for SSM mapping is counted as one entry.

Prerequisites

Layer 3 IPv6 multicast has been enabled using the **multicast ipv6 routing-enable** command in the system view.

Precautions

You can also run the **mld global limit** *number* command in the system view to set the maximum number of global MLD group memberships. If both the **limit** and **mld global limit** *number* commands are run, the smaller value takes effect.

Example

Set the maximum number of MLD entries to 1000 globally.


```
<HUAWEI> system-view
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] mld
[HUAWEI-mld] limit 1000
```

8.2.15 max-response-time (MLD view)

Function

The **max-response-time** command sets a global maximum response time for MLD General Query messages.

The **undo max-response-time** command restores the default global maximum response time for MLD General Query messages.

By default, the global maximum response time for MLD General Query messages is 10 seconds.

Format

max-response-time *interval*

undo max-response-time

Parameters

Parameter	Description	Value
interval	Specifies the maximum response time for MLD General Query messages.	The value is an integer that ranges from 1 to 25, in seconds.

Views

MLD view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If hosts send Multicast Listener Report messages immediately after receiving MLD General Query messages, the querier on the local network segment may receive a large number of Multicast Listener Report messages from the hosts at the same time. This may cause congestion on the network.

To avoid such situations, MLD messages specify the maximum response time for MLD General Query messages. When a host receives an MLD Query message, the host starts a timer for the multicast group that it joins. The timer length is a random value between 0 and the maximum response time. When the timer times out, the host sends a Multicast Listener Report message to the querier.

The maximum response time specifies the deadline for the host to send a Multicast Listener Report message. A proper maximum response time allows hosts to respond to MLD Query messages and prevents hosts from sending Report messages at the same time.

Prerequisites

Layer 3 IPv6 multicast has been enabled using the **multicast ipv6 routing-enable** command in the system view.

Precautions

- A shorter response time allows a multicast device to obtain multicast group member information more quickly, but consumes more bandwidth and system resources.
- The function of this command is the same as that of the **mld max-response-time** command used in the interface view. The configuration in the MLD view is globally valid, whereas the configuration in the interface view takes effect only for the specified interface. The configuration in the interface view takes precedence over the configuration in the MLD view. The configuration in the MLD view is used only when no configuration is performed in the interface view.

Example

In the MLD view, set the maximum response time for MLD General Query messages to 8 seconds.

```
<HUAWEI> system-view
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] mld
[HUAWEI-mld] max-response-time 8
```

8.2.16 mld

Function

The **mld** command displays the MLD view.

The **undo mld** command clears all configurations in the MLD view.

Format

mld

undo mld

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Global MLD parameters must be configured in the MLD view.

Prerequisites

Layer 3 IPv6 multicast has been enabled using the **multicast ipv6 routing-enable** command in the system view.

Precautions

In using the **undo mld** command, you need to enter Y or N to confirm the action. This command will clear global MLD configurations. So, use this command with caution.

Example

Enter the MLD view.

```
<HUAWEI> system-view
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] mld
[HUAWEI-mld]
```

8.2.17 mld enable

Function

The **mld enable** command enables MLD on an interface.

The **undo mld enable** command disables MLD on an interface.

By default, MLD is disabled on an interface.

Format

mld enable

undo mld enable

Parameters

None

Views

GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, VLANIF interface view, loopback interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On a shared IPv6 network segment, hosts and multicast devices must run MLD. A multicast device can process MLD messages sent from hosts only after MLD is enabled on the interfaces connected to user network segments.

Prerequisites

Layer 3 IPv6 multicast has been enabled using the **multicast ipv6 routing-enable** command in the system view.

Precautions

- If MLD parameters are configured on an interface, the parameter settings take effect only after MLD is enabled.
- If PIM (IPv6) and MLD need to be enabled on the same interface, enable PIM (IPv6) and MLD in sequence.
- Running the **mld enable** command failed on the VLANIF interface because Layer 2 multicast querier or report-suppress is enabled for this VLAN.
- When Layer 2 and Layer 3 multicast are both deployed, pay attention to the following points:
  - If both Layer 2 and Layer 3 multicast services are required in a VLAN, enable MLD on the corresponding VLANIF interface first, and then enable MLD snooping in the VLAN. If MLD snooping is enabled in the VLAN first, MLD cannot be enabled on the VLANIF interface.
  - If Layer 2 and Layer 3 multicast are both configured in a VLAN, you must delete the Layer 2 multicast configuration before you can modify or delete the Layer 3 multicast configuration. This means that you must disable MLD snooping in the VLAN first, then modify or disable the MLD and PIM (IPv6) configuration in the VLANIF interface view, and finally enable MLD snooping in the VLAN. Otherwise, the Layer 3 multicast configuration cannot be modified or deleted on the corresponding VLANIF interface.
  - If a VLANIF interface is shut down in the VLANIF interface view, Layer 2 multicast in the corresponding VLAN becomes ineffective accordingly. To make Layer 2 multicast effective, you must disable MLD snooping in the VLAN first, then disable MLD and PIM (IPv6) in the VLANIF interface view, and finally enable MLD snooping in the VLAN.
  - When both Layer 2 and Layer 3 multicast services are configured, traffic is forwarded based on Layer 3 multicast forwarding entries instead of Layer 2 multicast forwarding entries. This means that Layer 2 multicast provides physical outbound interfaces for Layer 3 multicast, implementing accurate forwarding of multicast data. In addition, the maximum number of Layer 3 multicast forwarding entries depends on the maximum number of Layer 2 multicast forwarding entries.
  - The default MLD version of the switch is MLDv2 (configured using the **mld version** *version* command); the default MLD snooping version of the

switch is MLDv1 (configured using the **mld-snooping version** *version* command). When Layer 2 and Layer 3 multicast services are both configured, MLD and MLD snooping must have the same version number.

Example

Enable MLD on VLANIF100 connected to a user network segment.

```
<HUAWEI> system-view
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] ipv6 enable
[HUAWEI-Vlanif100] mld enable
```

Enable MLD on GE0/0/1 connected to a user network segment.

```
<HUAWEI> system-view
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] ipv6 enable
[HUAWEI-GigabitEthernet0/0/1] mld enable
```

8.2.18 mld global limit

Function

The **mld global limit** command sets the maximum number of MLD entries that can be created on the entire switch.

The **undo mld global limit** command deletes the configured maximum number of MLD entries.

The following lists the maximum number of MLD entries allowed on each model by default:

- S5720-LI, S5720S-LI: 496
- S5735S-H, S5736-S, S6720S-S: 512
- S5731-S, S5731S-S, S5720I-SI: 1024
- S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735S-S, S5735-S-I: 1500
- S5731-H, S5731S-H, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, S6730S-S: 4096

Format

mld global limit *number*

undo mld global limit

Parameters

Parameter	Description	Value
number	Specifies the maximum number of MLD entries that can be created on the entire switch.	The value is an integer that ranges from 1 to *The maximum number of MLD entries allowed by default*. **NOTE** The value range of S5731-H, S5731S-H, S5732-H, S6730S-H, and S6730-H are expanded after the high specification mode is configured for multicast forwarding using the **set multicast forwarding-table super-mode** command. The actual value range depends on the specification of the device.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the number of MLD entries reaches the limit, the system no longer creates MLD entries. To enable the switch to allow new join requests, you can either delete useless entries or modify the limit. Alternatively, you can enable static addition on a multicast group or source group.

The number of MLD entries can be counted in the following methods:

- Each (*, G) entry is counted as one entry.
- Each (S, G) entry is counted as one entry.
- Each (*, G) entry for SSM mapping is counted as one entry.

Prerequisites

Layer 3 IPv6 multicast has been enabled using the **multicast ipv6 routing-enable** command in the system view.

Precautions

You can also run the **limit (MLD view)** command in the MLD view to set the maximum number of global MLD group entries. If both the **mld global limit** and **limit (MLD view)** commands are run, the smaller value takes effect.

Example

Set the maximum number of MLD entries that can be created on the switch to 500.


```
<HUAWEI> system-view
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] mld global limit 500
```

8.2.19 mld group-policy

Function

The **mld group-policy** command configures an MLD group policy on an interface to limit the range of multicast groups that the hosts can join.

The **undo mld group-policy** command deletes the MLD group policy.

By default, no MLD group policy is configured on an interface, and the hosts can join any multicast groups.

Format

mld group-policy *acl6-number* [**1** | **2**]

undo mld group-policy

Parameters

Parameter	Description	Value
acl6-number	Specifies the number of a basic or advanced IPv6 ACL6. This ACL6 defines the range of multicast groups.	The number of a basic ACL6 is an integer that ranges from 2000 to 2999. The number of an advanced ACL6 is an integer that ranges from 3000 to 3999.
1	Limits the range of multicast groups that MLDv1 hosts can join.	-
2	Limits the range of multicast groups that MLDv2 hosts can join.	-

Views

GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, VLANIF interface view, loopback interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To control the range of multicast groups that hosts on the network attached to an interface can join, specify an ACL6 in the **mld group-policy** command. This configuration improves security of the MLD application. You can also run this command to prevent the switch from receiving Multicast Listener Report messages for specified groups.

If the MLD version is not specified, ACL6 rule is applicable to the two versions by default.

Prerequisites

Layer 3 IPv6 multicast has been enabled using the **multicast ipv6 routing-enable** command in the system view.

Precautions

An ACL6 defining the range of multicast groups has been created.

The **mld group-policy** command is used with the **acl ipv6** command. To use a numbered ACL6 in the MLD group policy:

- In the basic ACL6 view, set **source** in the **rule (basic ACL6 view)** command to the range of multicast groups that an interface can join.
- In the advanced ACL6 view, set **source** in the **rule (advanced ACL6 view)** command to the source address that is allowed to send multicast data to the specified multicast groups, and set **destination** to the range of multicast groups that an interface can join.

The configurations of the Named ACL6 and the advanced ACL6 are the same, and can implement filtering of both source addresses and multicast group addresses. The Named ACL6 can also be configured with the **time-range** parameter.

After the **mld group-policy** command is executed on an interface:

- The interface filters the received Report messages based on the ACL6 and maintains memberships only for the multicast groups permitted by the ACL6.
- The interface discards the Report messages that are denied by the ACL6. If the entries of the multicast groups denied by the ACL6 exist on the switch, the switch deletes these entries when the aging time of the entries expires.

Example

Create ACL6 2005, and configure a rule that allows hosts to receive data of multicast group FF13::101. Configure an MLD group policy on VLANIF100 and reference ACL6 2005 to allow hosts connected to the interface to join only multicast group FF13::101.

```
<HUAWEI> system-view
[HUAWEI] acl ipv6 number 2005
[HUAWEI-acl6-basic-2005] rule permit source ff13::101 128
[HUAWEI-acl6-basic-2005] quit
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] ipv6 enable
[HUAWEI-Vlanif100] mld group-policy 2005
```

Create ACL6 2005, and configure a rule that allows hosts to receive data of multicast group FF13::101. Configure an MLD group policy on GE0/0/1 and reference ACL6 2005 to allow hosts connected to the interface to join only multicast group FF13::101.


```
<HUAWEI> system-view
[HUAWEI] acl ipv6 number 2005
[HUAWEI-acl6-basic-2005] rule permit source ff13::101 128
[HUAWEI-acl6-basic-2005] quit
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] ipv6 enable
[HUAWEI-GigabitEthernet0/0/1] mld group-policy 2005
```

8.2.20 mld ip-source-policy

Function

The **mld ip-source-policy** command enables filtering of Multicast Listener Report/Done messages based on source addresses.

The **undo mld ip-source-policy** command disables filtering of MLD messages based on source addresses.

By default, a multicast device does not filter MLD messages based on source addresses.

Format

mld ip-source-policy *basic-acl6-number*

undo mld ip-source-policy

Parameters

Parameter	Description	Value
basic-acl6-number	Specifies the number of a basic ACL6, which defines the range of source addresses.	The value is an integer that ranges from 2000 to 2999.

Views

GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, VLANIF interface view, loopback interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

MLD runs on receiver hosts and their directly connected multicast devices. A multicast device processes all received Multicast Listener Report/Done messages. For security purposes, you can configure the multicast device to filter Multicast Listener Report/Done messages received on an interface.

Prerequisites

Layer 3 IPv6 multicast has been enabled using the **multicast ipv6 routing-enable** command in the system view.

Precautions

For a numbered ACL, the **mld ip-source-policy** command works with the **acl ipv6** command. You can configure the source address of MLD messages by specifying the **source** parameter in the **rule** command in the basic ACL view.

Example

Configure VLANIF100 to accept only the Multicast Listener Report/Done messages with the source address FC00::1.

```
<HUAWEI> system-view
[HUAWEI] acl ipv6 number 2001
[HUAWEI-acl6-basic-2001] rule permit source fc00::1 128
[HUAWEI-acl6-basic-2001] quit
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] ipv6 enable
[HUAWEI-Vlanif100] mld ip-source-policy 2001
```

Configure GE0/0/1 to accept only the Multicast Listener Report/Done messages with the source address FC00::1.

```
<HUAWEI> system-view
[HUAWEI] acl ipv6 number 2001
[HUAWEI-acl6-basic-2001] rule permit source fc00::1 128
[HUAWEI-acl6-basic-2001] quit
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] ipv6 enable
[HUAWEI-GigabitEthernet0/0/1] mld ip-source-policy 2001
```

8.2.21 mld lastlistener-queryinterval

Function

The **mld lastlistener-queryinterval** command sets the interval at which the MLD querier sends Multicast Address Specific Query messages or Multicast Address and Source Specific Query messages after receiving Multicast Listener Done messages from a host.

The **undo mld lastlistener-queryinterval** command restores the default value.

By default, the interval for sending Multicast Address Specific Query messages or Multicast Address and Source Specific Query messages is 1 second.

Format

mld lastlistener-queryinterval *interval*

undo mld lastlistener-queryinterval

Parameters

Parameter	Description	Value
interval	Specifies the interval for sending Multicast Address Specific Query messages or Multicast Address and Source Specific Query messages.	The value is an integer that ranges from 1 to 5, in seconds.

Views

GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, VLANIF interface view, loopback interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the MLD querier receives a Multicast Listener Done message of a multicast group, the querier sends Multicast Address Specific Query messages or Multicast Address and Source Specific Query messages continuously to check for other members in the multicast group. The **mld lastlistener-queryinterval** command sets the interval at which the querier sends Multicast Address Specific Query messages or Multicast Address and Source Specific Query messages. If the querier receives no Multicast Listener Report message for a specified period, the querier stops forwarding data to the multicast group. The period is calculated by multiplying *interval* by *robust-value*. To set *robust-value*, run the **mld robust-count** or **robust-count (MLD view)** command.

If the querier receives a Multicast Listener Report message from a host within the maximum response time, the querier maintains the membership of the multicast group. Otherwise, the querier considers that the last member has left the group and does not maintain the membership of the multicast group.

Prerequisites

Layer 3 IPv6 multicast has been enabled using the **multicast ipv6 routing-enable** command in the system view.

Precautions

The function of the **mld lastlistener-queryinterval** command is the same as that of the **lastlistener-queryinterval** command used in the MLD view. The configuration in the MLD view is globally valid, whereas the configuration in the interface view takes effect only for the specified interface. The configuration in the interface view takes precedence over the configuration in the MLD view. The configuration in the MLD view is used only when no configuration is performed in the interface view.

Example

Set the interval for sending Multicast Address Specific Query messages or Multicast Address and Source Specific Query message to 3 seconds on VLANIF100.

```
<HUAWEI> system-view
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] ipv6 enable
[HUAWEI-Vlanif100] mld lastlistener-queryinterval 3
```

Set the interval for sending Multicast Address Specific Query messages or Multicast Address and Source Specific Query message to 3 seconds on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] ipv6 enable
[HUAWEI-GigabitEthernet0/0/1] mld lastlistener-queryinterval 3
```

8.2.22 mld limit

Function

The **mld limit** command sets the maximum number of MLD group memberships that the current interface can maintain.

The **undo mld limit** command restores the maximum number of MLD group memberships that the current interface can maintain to the default value.

The following lists the maximum number of MLD group memberships that can be maintained on the current interface of each model by default:

- S5720-LI, S5720S-LI: 496
- S5735S-H, S5736-S, S6720S-S 512
- S5731-S, S5731S-S, S5720I-SI: 1024
- S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735S-S, S5735-S-I: 1500
- S5731-H, S5731S-H, S5732-H, S6730-H, S6730S-H, S6730-S, S6730S-S: 2048
- S6720S-EI, S6735-S, S6720-EI: 4096

Format

mld limit *number* [**except** *acl6-number*]

undo mld limit

Parameters

Parameter	Description	Value
number	Specifies the maximum number of MLD group memberships that can be maintained on the current interface.	The value is an integer that ranges from 1 to *The maximum number of MLD group memberships that can be maintained on the current interface by default*. **NOTE** The value range of S5731-H, S5731S-H, S5732-H, S6730S-H, and S6730-H are expanded after the high specification mode is configured for multicast forwarding using the **set multicast forwarding-table super-mode** command. The actual value range depends on the specification of the device.
except	Specifies the range of multicast groups that are not limited by the specified maximum number.	-
acl6-number	Specifies the basic or advanced ACL6.	The value is an integer. The number of the basic ACL6 ranges from 2000 to 2999. The basic ACL6 filters group addresses only, without distinguishing (*, G) entries and (S, G) entries. The number of the advanced ACL6 ranges from 3000 to 3999. The advanced ACL6 filters (S, G) entries of the interface only.

Views

GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, VLANIF interface view, loopback interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the number of MLD entries reaches the limit, the system does not create any MLD entries. To allow more new join requests, delete unnecessary entries or increase the limit. Alternatively, configure static multicast groups or source-group bindings on interfaces.

The number of MLD entries can be counted in the following methods:

- Each (*, G) entry is counted as one entry.
- Each (S, G) entry is counted as one entry.
- Each (*, G) entry for SSM mapping is counted as one entry.

Prerequisites

Layer 3 IPv6 multicast has been enabled using the **multicast ipv6 routing-enable** command in the system view.

Precautions

If **except** is not set in the command, the maximum number of MLD entries corresponding to all the groups or source/groups is limited.

Before setting **except**, configure the associated ACL6. The interface then filters the received MLD Join messages according to the ACL6. The maximum number of entries corresponding to the multicast groups that match the ACL6 is not limited.

The **mld limit** command must be used with ACL6 configuration commands. When configuring ACL6 rules, note that:

- In the basic ACL6 view, specify the **source** parameter in the **rule (basic ACL6 view)** command for setting the range of multicast groups whose MLD entries do not need to be limited.
- In the advanced ACL6 view, specify the **source** parameter in the **rule (advanced ACL6 view)** command for setting the range of sources that are allowed to send multicast data to the multicast groups. Specify the **destination** parameter in the **rule (advanced ACL6 view)** command for setting the range of multicast groups whose MLD entries do not need to be limited.

The Named ACL and the advanced ACL can be configured based on the same rules, and can implement filtering of both source addresses and multicast group addresses. The **time-range** parameter takes effect in the **rule** command only for the Named ACL.

Example

Set the maximum number of MLD entries that can be created on the VLANIF100 to 500.

```
<HUAWEI> system-view
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] ipv6 enable
[HUAWEI-Vlanif100] mld limit 500
```

Create the advanced ACL6 with the number being 3100; set the maximum number of MLD entries that can be created on VLANIF100 to 500; allow the hosts to receive messages from the specific-source multicast group (FC00:0:0:2001::1, FF3E::1). That is, the specific-source multicast group (FC00:0:0:2001::1, FF3E::1) is not limited by the maximum number of MLD entries.

```
<HUAWEI> system-view
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] acl ipv6 3100
[HUAWEI-acl6-adv-3100] rule permit ipv6 source fc00:0:0:2001::1 64 destination ff3e::1 64
[HUAWEI-acl6-adv-3100] quit
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] ipv6 enable
[HUAWEI-Vlanif100] mld limit 500 except 3100
```


Set the maximum number of MLD entries that can be created on the GE0/0/1 to 500.

```
<HUAWEI> system-view
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] ipv6 enable
[HUAWEI-GigabitEthernet0/0/1] mld limit 500
```

8.2.23 mld max-response-time

Function

The **mld max-response-time** command sets the maximum response time for MLD General Query messages on an interface.

The **undo mld max-response-time** command restores the default maximum response time for General MLD Query messages.

By default, the maximum response time for MLD General Query messages is 10s on an interface.

Format

mld max-response-time *interval*

undo mld max-response-time

Parameters

Parameter	Description	Value
interval	Specifies the maximum response time for MLD General Query messages.	The value is an integer that ranges from 1 to 25, in seconds.

Views

GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, VLANIF interface view, loopback interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If hosts send Multicast Listener Report messages immediately after receiving MLD General Query messages, the querier on the local network segment may receive a large number of Multicast Listener Report messages from the hosts at the same time. This may cause congestion on the network.

To avoid such situations, MLD messages specify the maximum response time for MLD General Query messages. When a host receives an MLD Query message, the host starts a timer for the multicast group that it joins. The timer length is a random value between 0 and the maximum response time. When the timer times out, the host sends a Multicast Listener Report message to the querier.

The maximum response time specifies the deadline for the host to send a Multicast Listener Report message. A proper maximum response time allows hosts to respond to MLD Query messages and prevents hosts from sending Report messages at the same time.

Prerequisites

Layer 3 IPv6 multicast has been enabled using the **multicast ipv6 routing-enable** command in the system view.

Precautions

- A shorter response time allows a multicast device to obtain multicast group member information more quickly, but consumes more bandwidth and system resources.
- The function of the **mld max-response-time** command is the same as that of the **max-response-time (MLD view)** command used in the MLD view. The configuration in the MLD view takes effect for all interfaces, whereas the configuration in the interface view takes effect only for the specified interface. The configuration in the interface view takes precedence over the configuration in the MLD view. The configuration in the MLD view is used only when no configuration is performed in the interface view.

Example

Set the maximum response time for MLD General Query messages to 8 seconds on VLANIF100.

```
<HUAWEI> system-view
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] ipv6 enable
[HUAWEI-Vlanif100] mld max-response-time 8
```

Set the maximum response time for MLD General Query messages to 8 seconds on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] ipv6 enable
[HUAWEI-GigabitEthernet0/0/1] mld max-response-time 8
```

8.2.24 mld on-demand

Function

The **mld on-demand** command enables the MLD on-demand function. This function enables a querier to maintain group memberships according to requirements of group members, without sending Query messages. After MLD on-demand is enabled on an interface, dynamic MLD entries on the interface will never age out.

The **undo mld on-demand** command restores the default configuration.

By default, a querier does not maintain group memberships according to requirements of group members, and dynamic entries are aged out when the aging time expires.

Format

mld on-demand

undo mld on-demand

Parameters

None

Views

GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, VLANIF interface view, loopback interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In a standard MLD working process, a querier sends General Query messages periodically and collects group membership information based on received Multicast Listener Report and Done messages. Group members respond to every Query message they receive. The querier stops sending Query messages after MLD on-demand is configured, reducing MLD packets exchanged between the querier and receiver hosts.

The MLD on-demand function enables a querier to maintain group memberships based on Report messages sent from hosts, reducing traffic transmitted between the querier and receiver hosts.

Prerequisites

Layer 3 IPv6 multicast has been enabled using the **multicast ipv6 routing-enable** command in the system view.

Precautions

- The **mld on-demand** command can be used on the querier only.
- If dynamic MLD entries have been generated on the querier, run the **reset mld group** command to clear these dynamic MLD entries before running the **mld on-demand** command.
- After the **mld on-demand** command is executed on an interface:
  - The interface no longer sends MLD Query messages.

  - MLD group entries are generated after the interface receives Multicast Listener Report messages and will never age out.
  - When the interface receives a Multicast Listener Done message, it deletes the corresponding MLD group entry.
- The **mld on-demand** configuration of the VLANIF interface and the **mld-snooping enable** command in a VLAN are mutually exclusive.

Example

Enable the MLD on-demand function on VLANIF100.

```
<HUAWEI> system-view
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] ipv6 enable
[HUAWEI-Vlanif100] mld on-demand
```

Enable the MLD on-demand function on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] ipv6 enable
[HUAWEI-GigabitEthernet0/0/1] mld on-demand
```

8.2.25 mld prompt-leave

Function

The **mld prompt-leave** command enables the fast leave function on an interface. This function enables an MLD querier to delete MLD entries immediately after receiving Multicast Listener Done messages from group members, without sending Multicast Address Specific Query messages or Multicast Address and Source Specific Query messages.

The **undo mld prompt-leave** command disables fast leave on an interface.

By default, an MLD querier sends a Multicast Address Specific Query message or Multicast Address and Source Specific Query message after receiving a Multicast Listener Done message for a specific multicast group.

Format

mld prompt-leave [**group-policy** *acl6-number*]

undo mld prompt-leave

Parameters

Parameter	Description	Value
group-policy	Specifies an MLD multicast group policy. If this parameter is specified, the fast leave function takes effect only for multicast groups specified in the policy. When specifying this parameter, ensure that the referenced ACL6 has been configured. The interface filters Multicast Listener Done messages on the interface based on the ACL6. • If a host leaves a multicast group in the range permitted by the ACL6, the device immediately deletes the multicast group entry without sending Multicast Address Specific Query messages or Multicast Address and Source Specific Query messages. • If a host leaves a multicast group out of the range permitted by the ACL6, the device sends Multicast Address Specific Query messages or Multicast Address and Source Specific Query messages. If this parameter is not specified, the fast leave function takes effect for all multicast groups.	-
acl6-number	Specifies the number of a basic ACL6 or an advanced ACL6. This ACL6 defines the range of multicast groups.	The number of a basic ACL6 is an integer that ranges from 2000 to 2999. The number of an advanced ACL6 is an integer that ranges from 3000 to 3999.

Views

GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, VLANIF interface view, loopback interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In some scenarios, an interface on the MLD querier connects to only one receiver host. If the host frequently switches between multiple multicast groups, you can configure fast leave on the interface of the querier so that the interface can quickly respond to Multicast Listener Done messages sent from the host. After fast leave is configured, the querier does not send a Multicast Address Specific Query message or Multicast Address and Source Specific Query message after receiving a Multicast Listener Done message. Instead, the querier directly notifies the upstream multicast device that the host has left the multicast group. The fast leave function reduces delay in response to Multicast Listener Done messages and saves network bandwidth.

Prerequisites

Layer 3 IPv6 multicast has been enabled using the **multicast ipv6 routing-enable** command in the system view.

Precautions

- When an interface has more than one receiver connected, enabling fast leave interrupts multicast traffic of the other receivers in the multicast group. You are advised to enable this function on interfaces with only one receiver.
- When configuring an ACL6 to specify the range of multicast groups, pay attention to the following points:
  - When you run the **rule** command in the view of a basic ACL6, set **source** to the address range of multicast groups that hosts can fast leave.
  - When you run the **rule** command in the view of an advanced ACL6, set **source** to the multicast source address and **destination** to the range of multicast groups that hosts can fast leave.

Example

Configure fast leave on VLANIF100.

```
<HUAWEI> system-view
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] ipv6 enable
[HUAWEI-Vlanif100] mld prompt-leave
```

Configure fast leave on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] ipv6 enable
[HUAWEI-GigabitEthernet0/0/1] mld prompt-leave
```

8.2.26 mld query ip-source-policy

Function

The **mld query ip-source-policy** command configures MLD Query message filtering based on source addresses.

The **undo mld query ip-source-policy** command restores the default configuration.

By default, no source address-based MLD Query message filtering is configured.

Format

mld query ip-source-policy *basic-acl6-number*

undo mld query ip-source-policy

Parameters

Parameter	Description	Value
basic-acl6-number	Specifies the number of a basic ACL6, which defines the range of source addresses.	The value is an integer that ranges from 2000 to 2999.

Views

GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, VLANIF interface view, loopback interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If an attacker sends forged MLD Query messages with an IPv6 address smaller than the querier IPv6 address, the querier is replaced by the attacker. As a result, the real querier cannot respond to Multicast Listener Report messages from group members and bandwidth is wasted. Source address-based MLD Query message filtering can protect the querier from such attacks. With this function configured, the switch accepts only the MLD Query messages with source addresses permitted by the specified ACL6. This function controls querier election.

Prerequisites

Layer 3 IPv6 multicast has been enabled using the **multicast ipv6 routing-enable** command in the system view.

Precautions

- MLD Query messages are encapsulated into IPv6 messages. This command is used to filter the source addresses in IPv6 headers.
- After you configure source address-based MLD Query message filtering on an interface, the interface filters out the MLD Query messages whose source addresses do not match a specified ACL6 rule.

Example

Configure VLANIF100 to receive the MLD Query messages with the source address FC00::1.


```
<HUAWEI> system-view
[HUAWEI] acl ipv6 number 2001
[HUAWEI-acl6-basic-2001] rule permit source fc00::1 128
[HUAWEI-acl6-basic-2001] quit
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] ipv6 enable
[HUAWEI-Vlanif100] mld query ip-source-policy 2001
```

Configure GE0/0/1 to receive the MLD Query messages with the source address FC00::1.

```
<HUAWEI> system-view
[HUAWEI] acl ipv6 number 2001
[HUAWEI-acl6-basic-2001] rule permit source fc00::1 128
[HUAWEI-acl6-basic-2001] quit
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] ipv6 enable
[HUAWEI-GigabitEthernet0/0/1] mld query ip-source-policy 2001
```

8.2.27 mld require-router-alert

Function

The **mld require-router-alert** command configures an interface to discard MLD messages without the Router-Alert option.

The **undo mld require-router-alert** command disables an interface from checking for the Router-Alert option in MLD messages.

By default, all received MLD messages are processed, including the MLD messages without the Router-Alert option.

Format

mld require-router-alert

undo mld require-router-alert

Parameters

None

Views

GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, VLANIF interface view, loopback interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Generally, a network device sends a message to the routing protocol module for processing only when the destination address of the message is a local interface address. Destination addresses of MLD messages are multicast addresses but not addresses of interfaces on multicast devices. Therefore, multicast devices do not send MLD messages to the MLD module for processing, and the MLD module cannot maintain group memberships.

The Router-Alert option in the IPv6 header of an MLD message solves this problem. If an MLD message contains the Router-Alert option, the device sends the message to the MLD module.

You can configure the device to accept only MLD messages with the Router-Alert option to improve MLD security.

Prerequisites

Layer 3 IPv6 multicast has been enabled using the **multicast ipv6 routing-enable** command in the system view.

Precautions

The function of the **mld require-router-alert** command is the same as that of the **require-router-alert (MLD view)** command used in the MLD view. The configuration in the MLD view is globally valid, whereas the configuration in the interface view takes effect only for the specified interface. The system prefers the configuration in the interface view. The configuration in the MLD view is used only when no configuration is performed in the interface view.

Example

Configure VLANIF100 to discard MLD messages without the Router-Alert option.

```
<HUAWEI> system-view
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] ipv6 enable
[HUAWEI-Vlanif100] mld require-router-alert
```

Configure GE0/0/1 to discard MLD messages without the Router-Alert option.

```
<HUAWEI> system-view
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] ipv6 enable
[HUAWEI-GigabitEthernet0/0/1] mld require-router-alert
```

8.2.28 mld robust-count

Function

The **mld robust-count** command sets a robustness variable of an MLD querier on an interface.

The **undo mld robust-count** command restores the default robustness variable of an MLD querier.

By default, the robustness variable of an MLD querier is 2.

Format

mld robust-count *robust-value*

undo mld robust-count

Parameters

Parameter	Description	Value
robust-value	Specifies the robustness variable of an MLD querier.	The value is an integer that ranges from 2 to 5.

Views

GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, VLANIF interface view, loopback interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The MLD querier robustness variable specifies the retransmission count of MLD packets to minimize the impact of packet loss on the network.

On a shared network segment, a querier maintains MLD group memberships. The robustness variable affects the timeout period of group memberships. The timeout period of the group membership is calculated using the formula:

Timeout period of the group memberships = Interval for sending MLD General Query messages x Robustness variable + Maximum response time

The robustness variable determines the following values:

- Number of times the querier sends General Query messages when the querier starts

  When a querier starts, it sends General Query messages a certain number of times specified by the robustness variable to query the multicast groups that have members on the shared network segment. The interval for sending General Query messages is configured using the **mld timer query** or **timer query (MLD view)** command.

- Number of times the querier sends Multicast Address Specific Query messages or Multicast Address and Source Specific Query messages

  When receiving a Multicast Listener Done message of a multicast group, the querier sends Multicast Address Specific Query messages a certain number of times specified by the robustness variable to check whether the group has members. When the querier receives a Multicast Listener Report message indicating that source-group mapping changes, the querier sends Multicast

Address and Source Specific Query messages a certain number of times specified by the robustness variable. The interval for sending Multicast Address Specific Query messages or Multicast Address and Source Specific Query messages is set using the **mld lastlistener-queryinterval** or **lastlistener-queryinterval (MLD view)** command.

A larger robustness variable makes an MLD querier more robust but increases the timeout period of group memberships.

Prerequisites

Layer 3 IPv6 multicast has been enabled using the **multicast ipv6 routing-enable** command in the system view.

Precautions

The function of the **mld robust-count** command is the same as that of the **robust-count (MLD view)** command used in the MLD view. The configuration in the MLD view is globally valid, whereas the configuration in the interface view takes effect only for the specified interface. The configuration in the interface view takes precedence over the configuration in the MLD view. The configuration in the MLD view is used only when no configuration is performed in the interface view.

Example

Set the robustness variable of the querier on VLANIF100 to 3.

```
<HUAWEI> system-view
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] ipv6 enable
[HUAWEI-Vlanif100] mld robust-count 3
```

Set the robustness variable of the querier on GE0/0/1 to 3.

```
<HUAWEI> system-view
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] ipv6 enable
[HUAWEI-GigabitEthernet0/0/1] mld robust-count 3
```

8.2.29 mld send-router-alert

Function

The **mld send-router-alert** command configures an interface to send MLD messages containing the Router-Alert option in IPv6 headers.

The **undo mld send-router-alert** command disables an interface from sending MLD messages containing the Router-Alert option in IPv6 headers.

By default, the IPv6 headers of MLD messages sent by an interface contain the Router-Alert option.

Format

mld send-router-alert

undo mld send-router-alert

Parameters

None

Views

GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, VLANIF interface view, loopback interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

By default, the switch sends MLD messages that contain the Router-Alert option in IPv6 headers. If the switch needs to communicate with a device that does not support the Router-Alert option, run the **undo mld send-router-alert** command to configure the switch to send MLD messages without the Router-Alert option. The **mld send-router-alert** command is usually used together with the **mld require-router-alert** command.

Prerequisites

Layer 3 IPv6 multicast has been enabled using the **multicast ipv6 routing-enable** command in the system view.

Precautions

The function of the **mld send-router-alert** command is the same as that of the **send-router-alert (MLD view)** command used in the MLD view. The configuration in the MLD view is globally valid, whereas the configuration in the interface view takes effect only for the specified interface. The configuration in the interface view takes precedence over the configuration in the MLD view. The configuration in the MLD view is used only when no configuration is performed in the interface view.

Example

Configure VLANIF100 to send MLD messages with the Router-Alert option in their IPv6 headers.

```
<HUAWEI> system-view
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] ipv6 enable
[HUAWEI-Vlanif100] mld send-router-alert
```

Configure GE0/0/1 to send MLD messages with the Router-Alert option in their IPv6 headers.

```
<HUAWEI> system-view
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] ipv6 enable
[HUAWEI-GigabitEthernet0/0/1] mld send-router-alert
```


8.2.30 mld ssm-mapping enable

Function

The **mld ssm-mapping enable** command enables MLD SSM mapping on an interface.

The **undo mld ssm-mapping enable** command disables MLD SSM mapping on an interface.

By default, MLD SSM mapping is disabled on an interface.

Format

mld ssm-mapping enable

undo mld ssm-mapping enable

Parameters

None

Views

GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, VLANIF interface view, loopback interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The SSM model allows MLDv2 hosts to specify the multicast sources from which they want to receive data. However, some hosts can only run MLDv1. To allow these hosts to use SSM, configure MLD SSM mapping on the switch. MLD SSM mapping is implemented based on static SSM mapping entries on the switch. The switch converts (*, G) information in MLDv1 Multicast Listener Report messages to (S, G) information according to static SSM mapping entries to provide the SSM service for MLDv1 hosts.

The **mld ssm-mapping enable** command enables MLD SSM mapping on an interface. The mappings between SSM sources and multicast group addresses take effect only when MLD SSM mapping is enabled on an interface. SSM mapping entries are configured using the **ssm-mapping (MLD view)** command.

Prerequisites

Layer 3 IPv6 multicast has been enabled using the **multicast ipv6 routing-enable** command in the system view.

Precautions

SSM mapping enabled on an interface is irrelevant to the version number of MLD.

Example

Enable MLD SSM mapping on VLANIF100.

```
<HUAWEI> system-view
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] ipv6 enable
[HUAWEI-Vlanif100] mld ssm-mapping enable
```

Enable MLD SSM mapping on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] ipv6 enable
[HUAWEI-GigabitEthernet0/0/1] mld ssm-mapping enable
```

8.2.31 mld static-group

Function

The **mld static-group** command configures a static multicast group on an interface.

The **undo mld static-group** command deletes a static multicast group from an interface.

By default, no static multicast group is configured on an interface.

Format

mld static-group *ipv6-group-address* [**inc-step-mask** *ipv6-group-mask-length* **number** *group-number*] [**source** *ipv6-source-address*]

undo mld static-group { **all** | *ipv6-group-address* [**inc-step-mask** *ipv6-group-mask-length* **number** *group-number*] [**source** *ipv6-source-address*] }

Parameters

Parameter	Description	Value
ipv6-group-address	Specifies the IPv6 address of the multicast group that an interface statically joins. In batch configuration mode, this parameter specifies the initial address of the multicast group addresses.	The value is a 32-digit hexadecimal number in X:X:X:X:X:X:X:X format. The value ranges from FF00:: to FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF.

Parameter	Description	Value
inc-step-mask *ipv6-group-mask-length*	Specifies the incremental length of the step mask in batch configuration mode.	The value is an integer that ranges from 8 to 128.
number *group-number*	Specifies the number of group addresses in batch configuration mode.	The value is an integer that ranges from 2 to 512.
source *ipv6-source-address*	Specifies the IPv6 address of a multicast source.	The value is a 32-digit hexadecimal number in X:X:X:X:X:X:X:X format.
all	Specifies all the multicast groups that the interface statically joins.	-

Views

GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, VLANIF interface view, loopback interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The following are two scenarios in which you can configure static multicast groups on user-side interfaces of the switch:

- There are long-term group members on a shared network segment, and the switch needs to forward multicast data to these group members quickly and steadily.
- A network segment has no group member or hosts on the network segment cannot send Report messages, but multicast data needs to be sent to this network segment.

After a static multicast group is configured on an interface, the switch considers that the multicast group always has members on the network segment of the interface. Therefore, the switch always forwards multicast data of the multicast group.

The **mld static-group** command is used on an interface connected to user hosts. The command can configure a single group or source-group binding on an interface or configure multiple groups or source-group bindings in a batch.

Prerequisites

Layer 3 IPv6 multicast has been enabled using the **multicast ipv6 routing-enable** command in the system view.

Precautions

- After multicast groups are configured in batches for the first time, if you only modify the value of *group-number* but not the value of *ipv6-group-address* or *ipv6-group-mask-length* to configure multicast groups in batches again, the new configurations overwrite the corresponding original configurations.
- After you run the **mld static-group** command on an interface connected to user hosts, the entries matching the MLD groups that the interface statically joins never time out. The switch considers that this interface is always connected to group members, and keeps forwarding multicast packets of the specified multicast groups to the network segment where the interface resides.
- You can configure overlapping multicast group addresses in different batch configurations. When you configure multiple static multicast groups in a batch on an interface, do not delete any static group configuration before the system completes the batch static group configuration.
- If a user host no longer needs to receive multicast data of a static group, delete the static group configuration.
- When the interface that connects a multicast device to the user network segment joins a multicast group in both dynamic and static modes, the interface preferentially joins the multicast group in static mode if a conflict occurs.
- Running the **mld static-group** command failed on the VLANIF interface because Layer 2 multicast querier or report-suppress is enabled for this VLAN.

Example

Configure static multicast group FF13::101 on VLANIF100.

```
<HUAWEI> system-view
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] ipv6 enable
[HUAWEI-Vlanif100] mld static-group ff13::101
```

Configure the switch to forward multicast packets from multicast source FC00::101 to multicast group FF14::202 through VLANIF100.

```
<HUAWEI> system-view
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] ipv6 enable
[HUAWEI-Vlanif100] mld static-group ff14::202 source fc00::101
```

Add VLANIF100 statically to two multicast groups in a batch. Set the start multicast group address to FF25::1 and the step mask length to 24.

```
<HUAWEI> system-view
[HUAWEI] multicast ipv6 routing-enable
```



```
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] ipv6 enable
[HUAWEI-Vlanif100] mld static-group ff25::1 inc-step-mask 24 number 2
```

Add VLANIF100 statically to two multicast source/groups in a batch. Set the start multicast group address to FF33::1, the source address to FC00::101, and the step mask length to 24.

```
<HUAWEI> system-view
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] ipv6 enable
[HUAWEI-Vlanif100] mld static-group ff33::1 inc-step-mask 24 number 2 source fc00::101
```

Configure static multicast group FF13::101 on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] ipv6 enable
[HUAWEI-GigabitEthernet0/0/1] mld static-group ff13::101
```

8.2.32 mld timer other-querier-present

Function

The **mld timer other-querier-present** command sets the other querier present timer on an interface.

The **undo mld timer other-querier-present** command restores the default value of the other querier present timer on an interface.

By default, the Keepalive period of the other queriers is calculated as follows:

Other querier present timer = Robustness variable x Interval for sending MLD General Query messages + 1/2 x Maximum response time

If the default values of the robustness variable, interval for sending MLD General Query messages, and maximum response time are used, the other querier present timer value is 255 seconds.

Format

mld timer other-querier-present *interval*

undo mld timer other-querier-present

Parameters

Parameter	Description	Value
interval	Specifies the other querier present timer.	The value is an integer that ranges from 60 to 300, in seconds.

Views

GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, VLANIF interface view, loopback interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When a user network segment connects to multiple Layer 3 multicast devices, only one Layer 3 multicast device is elected as the MLD querier to send Query messages to hosts on the network segment. To create and maintain normal group memberships, non-queriers running MLD start the other querier present timer after they fail in the querier election. If the non-queriers do not receive Query messages from the querier before the timer times out, they consider the querier failed and start a new querier election.

Prerequisites

Layer 3 IPv6 multicast has been enabled using the **multicast ipv6 routing-enable** command in the system view.

Precautions

The function of the **mld timer other-querier-present** command is the same as that of the **timer other-querier-present (MLD view)** command used in the MLD view. The configuration in the MLD view is globally valid, whereas the configuration in the interface view takes effect only for the specified interface. The configuration in the interface view takes precedence over the configuration in the MLD view. The configuration in the MLD view is used only when no configuration is performed in the interface view.

NOTICE

If the other querier present timer is shorter than the interval for sending General Query messages, the querier election is triggered frequently.

Example

On VLANIF100, set the other querier present timer to 200 seconds.

```
<HUAWEI> system-view
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] ipv6 enable
[HUAWEI-Vlanif100] mld timer other-querier-present 200
```

On GE0/0/1, set the other querier present timer to 200 seconds.

```
<HUAWEI> system-view
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] interface gigabitethernet 0/0/1
```



```
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] ipv6 enable
[HUAWEI-GigabitEthernet0/0/1] mld timer other-querier-present 200
```

8.2.33 mld timer query

Function

The **mld timer query** command sets the interval at which an interface sends MLD General Query messages.

The **undo mld timer query** command restores the default interval at which an interface sends MLD General Query messages.

By default, an interface sends MLD General Query messages at an interval of 125s.

Format

mld timer query *interval*

undo mld timer query

Parameters

Parameter	Description	Value
interval	Specifies the interval at which an interface sends MLD General Query messages.	The value is an integer that ranges from 1 to 18000, in seconds.

Views

GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, VLANIF interface view, loopback interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

An MLD querier checks whether a local network segment has multicast group members by sending MLD General Query messages at an interval, known as the general query interval. You can set the general query interval based on needs of your network. The general query interval affects the following processes:

- When a querier starts, it sends General Query messages a certain number of times specified by the robustness variable to query the multicast groups that have members on the shared network segment. The message sending interval during this process is 1/4 of the interval for sending General Query messages.

The robustness variable can be set using the **mld robust-count** or **robust-count (MLD view)** command.

- After the startup process is complete, the querier sends General Query messages at intervals to maintain the group memberships on the interface.

Prerequisites

Layer 3 IPv6 multicast has been enabled using the **multicast ipv6 routing-enable** command in the system view.

Precautions

- The querier is more sensitive when it sends General Query messages at a smaller interval. However, more bandwidth and switch resources are consumed in this case.
- The function of the **MLD timer query** command is the same as that of the **timer query (MLD view)** command used in the MLD view. The configuration in the MLD view is globally valid, whereas the configuration in the interface view takes effect only for the specified interface. The system prefers the configuration in the interface view. The configuration in the MLD view is used only when no configuration is performed in the interface view.

Example

Set the interval at which VLANIF100 sends General Query messages to 200 seconds.

```
<HUAWEI> system-view
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] ipv6 enable
[HUAWEI-Vlanif100] mld timer query 200
```

Set the interval at which GE0/0/1 sends General Query messages to 200 seconds.

```
<HUAWEI> system-view
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] ipv6 enable
[HUAWEI-GigabitEthernet0/0/1] mld timer query 200
```

8.2.34 mld ttl-check

Function

The **mld ttl-check** command enables the device to check the TTL values in received MLD Report, Done, and Query messages on a specific interface.

The **undo mld ttl-check** command restores the default configuration.

By default, the device does not check the TTL values in received MLD Report, Done, and Query messages on an interface.

Format

mld ttl-check

undo mld ttl-check

Parameters

None

Views

GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, VLANIF interface view, loopback interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

This command enables TTL check for MLD Report, Leave, and Query messages on an interface. This function protects the system against attacking MLD messages by dropping the messages of which the TTL value is not 1. By default, TTL values of MLD messages are not checked on an interface.

You can also configure TTL check for MLD Report, Leave, and Query messages by using the **ttl-check** command in the MLD view. This command takes effect for all MLD-enabled interfaces.

Precautions

If both the **mld ttl-check** and **ttl-check** commands are run, the **mld ttl-check** configuration in the interface view takes precedence over the **ttl-check** configuration in the MLD view.

Example

Enable TTL check for MLD Report, Leave, and Query messages on a physical interface.

```
<HUAWEI> system-view
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] mld ttl-check
```

Enable TTL check for MLD Report, Leave, and Query messages on a VLANIF interface.

```
<HUAWEI> system-view
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] vlan 2
[HUAWEI-vlan2] quit
[HUAWEI] interface vlanif 2
[HUAWEI-Vlanif2] mld ttl-check
```


8.2.35 mld version

Function

The **mld version** command specifies an MLD version on an interface.

The **undo mld version** command restores the default MLD version on an interface.

By default, an interface runs MLDv2.

Format

mld version *version*

undo mld version

Parameters

Parameter	Description	Value
version	Specifies the MLD version running on the interface.	The value is integer that ranges from 1 to 2.

Views

GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, VLANIF interface view, loopback interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A multicast switch can only identify MLD messages of a version earlier than its own MLD version. To ensure normal MLD operation, set on the switch an MLD version the same as or later than that running on user hosts.

If many switches exist on a shared network segment, configure the same MLD version on all switch interfaces connected to hosts. If multicast devices run MLD of different versions, errors may occur in MLD operation because interfaces running different MLD versions send messages in different formats.

Prerequisites

Layer 3 IPv6 multicast has been enabled using the **multicast ipv6 routing-enable** command in the system view.

Example

Configure MLDv2 on VLANIF100.

```
<HUAWEI> system-view
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] ipv6 enable
[HUAWEI-Vlanif100] mld version 2
```

Configure MLDv2 on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] ipv6 enable
[HUAWEI-GigabitEthernet0/0/1] mld version 2
```

8.2.36 require-router-alert (MLD view)

Function

The **require-router-alert** command configures the switch to discard MLD messages without the Router-Alert option.

The **undo require-router-alert** command disables the switch from checking the Router-Alert option in MLD messages.

By default, the switch does not check whether the received MLD messages contain Router-Alert options in IPv6 headers, and it accepts all the received MLD messages.

Format

require-router-alert

undo require-router-alert

Parameters

None

Views

MLD view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Generally, a network device sends a message to the routing protocol module for processing only when the destination address of the message is a local interface address. Destination addresses of MLD messages are multicast addresses but not addresses of interfaces on multicast devices. Therefore, multicast devices do not

send MLD messages to the MLD module for processing, and the MLD module cannot maintain group memberships.

The Router-Alert option in the IPv6 header of an MLD message solves this problem. If an MLD message contains the Router-Alert option, the device sends the message to the MLD module.

You can configure the device to accept only MLD messages with the Router-Alert option to improve MLD security.

Prerequisites

Layer 3 IPv6 multicast has been enabled using the **multicast ipv6 routing-enable** command in the system view.

Precautions

The function of this command is the same as that of the **mld require-router-alert** command used in the interface view. The configuration in the MLD view is globally valid, whereas the configuration in the interface view takes effect only for the specified interface. The configuration in the interface view takes precedence over the configuration in the MLD view. The configuration in the MLD view is used only when no configuration is performed in the interface view.

Example

In the MLD view, configure the switch to discard the MLD messages that do not contain Router-Alert options in IPv6 headers.

```
<HUAWEI> system-view
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] mld
[HUAWEI-mld] require-router-alert
```

8.2.37 reset mld control-message counters

Function

The **reset mld control-message counters** command deletes statistics of MLD messages.

Format

reset mld control-message counters [**interface** *interface-type interface-number*] [**message-type** { **query** | **report** }]

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Clears MLD packet statistics on a specified interface. If this parameter is not specified, MLD packets on all interfaces are deleted.	-

Parameter	Description	Value
message-type	Clears statistics about MLD messages of a specified type. If this parameter is not specified, the command clears statistics about MLD messages of all types.	-
query	Clears the number of received Query messages.	-
report	Clears the number of received Multicast Listener Report messages.	-

Views

User view

Default Level

3: Management level

Usage Guidelines

After statistics about MLD messages are deleted, MLD still operates properly.

Example

Delete statistics about MLD messages from all interfaces.

```
<HUAWEI> reset mld control-message counters
```

Delete statistics about MLD messages from VLANIF100.

```
<HUAWEI> reset mld control-message counters interface vlanif 100
```

8.2.38 reset mld explicit-tracking

Function

The **reset mld explicit-tracking** command deletes hosts that dynamically join a multicast group using MLD from an interface.

Format

reset mld explicit-tracking { **all** | **interface** *interface-type interface-number* [**host** *ipv6-host-address* [**group** *ipv6-group-address* [**source** *ipv6-source-address*]]] }

Parameters

Parameter	Description	Value
all	Indicates information about all MLD hosts.	-
interface *interface-type interface-number*	Specifies the type and number of an interface. If this parameter is not specified, the command deletes hosts that dynamically join the host group using MLD from all interfaces.	-
host *ipv6-host-address*	Specifies the link-local address of a host.	The value is a 32-digit hexadecimal number in X:X:X:X:X:X:X:X format. The value ranges from FE80:: to FE80:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF.
group *ipv6-group-address*	Specifies an IPv6 multicast group address.	The value is a 32-digit hexadecimal number in X:X:X:X:X:X:X:X format. The value ranges from FF00:: to FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF.
source *ipv6-source-address*	Specifies the IPv6 address of a multicast source.	The value is a 32-digit hexadecimal number in X:X:X:X:X:X:X:X format.

Views

User view

Default Level

3: Management level

Usage Guidelines

You can use this command to delete hosts that dynamically join a multicast group using MLD from an interface. A host can rejoin the multicast group after being deleted from this group.

Example

Delete the host FE80::101 that joins multicast group FF23::101 through MLD on VLANIF100.

```
<HUAWEI> reset mld explicit-tracking interface vlanif 100 host fe80::101 group ff23::101
```

Delete the host FE80::101 that joins the (FC00:0:0:1::12, FF23::101) forwarding entry from VLANIF100.

```
<HUAWEI> reset mld explicit-tracking interface vlanif 100 host fe80::101 group ff23::101 source
fc00:0:0:1::12
```

8.2.39 reset mld group

Function

The **reset mld group** command deletes dynamic MLD entries on interfaces.

Format

reset mld group all

reset mld group interface *interface-type interface-number* { **all** | *ipv6-group-address* [*ipv6-group-mask-length*] [*ipv6-source-address* [*ipv6-source-mask-length*]] }

Parameters

Parameter	Description	Value
all	The first **all** deletes dynamic MLD entries on all interfaces. The second **all** deletes all MLD entries on a specified interface.	-
interface *interface-type interface-number*	Deletes dynamic MLD entries on a specified interface.	-
ipv6-group-address	Deletes dynamic MLD entries of a specified multicast group.	The value is a 32-digit hexadecimal number in X:X:X:X:X:X:X:X format. The value ranges from FF00:: to FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF.
ipv6-group-mask-length	Specifies the mask length of the multicast group address.	The value is an integer that ranges from 8 to 128.

Parameter	Description	Value
ipv6-source-address	Specifies the IPv6 address of a multicast source.	The value is a 32-digit hexadecimal number in X:X:X:X:X:X:X:X format.
ipv6-source-mask-length	Specifies the mask length of the multicast source address.	The value is an integer that ranges from 0 to 128.

Views

User view

Default Level

3: Management level

Usage Guidelines

This command deletes all the dynamic MLD group memberships on an interface, including common group memberships and group memberships established with SSM mapping. This command cannot delete statically configured MLD group memberships.

A host can rejoin the multicast group after being deleted from this group.

NOTICE

After dynamic MLD entries on an interface are deleted, the interface cannot receive multicast data. Exercise caution before running this command.

Example

Delete dynamic MLD entries within the range of FF03::101:0 to FF03::101:FFFF on VLANIF100.

```
<HUAWEI> reset mld group interface vlanif 100 ff03::101:0 112
```

8.2.40 reset mld group ssm-mapping

Function

The **reset mld group ssm-mapping** command deletes multicast group entries established with MLD SSM mapping.

Format

reset mld group ssm-mapping all

reset mld group ssm-mapping interface *interface-type interface-number* { **all** | *ipv6-group-address* [*ipv6-group-mask-length*] }

Parameters

Parameter	Description	Value
all	The first **all** deletes multicast group entries established with MLD SSM mapping on all interfaces. The second **all** deletes all multicast group entries established with MLD SSM mapping on a specified interface.	-
interface *interface-type interface-number*	Deletes the multicast group entries established with MLD SSM mapping on a specified interface.	-
ipv6-group-address	Specifies an IPv6 multicast group address.	The value consists of 128 octets, which are classified into 8 groups. Each group contains 4 hexadecimal numbers in the format X:X:X:X:X:X:X:X. The value ranges from FF00:: to FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF.
ipv6-group-mask-length	Specifies the mask length of the multicast group address.	The value is an integer that ranges from 8 to 128.

Views

User view

Default Level

3: Management level

Usage Guidelines

This command is valid only on the multicast groups that an interface has dynamically joined, and deletes only the MLDv1 multicast group entries within the range of SSM group addresses.

SSM mapping can be re-configured after being deleted.

NOTICE

After the multicast group entries established with MLD SSM mapping on an interface are deleted, the interface cannot receive multicast data. Exercise caution before running this command.

Example

Delete multicast group entries established with MLD SSM mapping within the range of FF13::101:0 to FF13::101:FFFF on VLANIF100.

```
<HUAWEI> reset mld group ssm-mapping interface vlanif 100 ff13::101:0 112
```

8.2.41 robust-count (MLD view)

Function

The **robust-count** command sets a global robustness variable for an MLD querier.

The **undo robust-count** command restores the default robustness variable.

By default, the robustness variable of an MLD querier is 2.

Format

robust-count *robust-value*

undo robust-count

Parameters

Parameter	Description	Value
robust-value	Specifies the robustness variable of an MLD querier.	The value is an integer that ranges from 2 to 5.

Views

MLD view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The MLD querier robustness variable specifies the retransmission count of MLD packets to minimize the impact of packet loss on the network.

On a shared network segment, a querier maintains MLD group memberships. The robustness variable affects the timeout period of group memberships. The timeout period of the group membership is calculated using the formula:

Timeout period of the group memberships = Interval for sending MLD General Query messages x Robustness variable + Maximum response time

The robustness variable determines the following values:

- Number of times the querier sends General Query messages when the querier starts

  When a querier starts, it sends General Query messages a certain number of times specified by the robustness variable to query the multicast groups that have members on the shared network segment. The interval for sending General Query messages is configured using the **mld timer query** or **timer query (MLD view)** command.
- Number of times the querier sends Multicast Address Specific Query messages or Multicast Address and Source Specific Query messages

  When receiving a Multicast Listener Done message of a multicast group, the querier sends Multicast Address Specific Query messages a certain number of times specified by the robustness variable to check whether the group has members. When the querier receives a Multicast Listener Report message indicating that source-group mapping changes, the querier sends Multicast Address and Source Specific Query messages a certain number of times specified by the robustness variable. The interval for sending Multicast Address Specific Query messages or Multicast Address and Source Specific Query messages is set using the **mld lastlistener-queryinterval** or **lastlistener-queryinterval (MLD view)** command.

A larger robustness variable makes an MLD querier more robust but increases the timeout period of group memberships.

Prerequisites

Layer 3 IPv6 multicast has been enabled using the **multicast ipv6 routing-enable** command in the system view.

Precautions

The function of this command is the same as that of the **mld robust-count** command used in the interface view. The configuration in the MLD view is globally valid, whereas the configuration in the interface view takes effect only for the current interface. The configuration in the interface view takes precedence over the configuration in the MLD view. The configuration in the MLD view is used only when no configuration is performed in the interface view.

Example

Set the robustness variable of an MLD querier to 3 in the MLD view.

```
<HUAWEI> system-view
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] mld
[HUAWEI-mld] robust-count 3
```

8.2.42 send-router-alert (MLD view)

Function

The **send-router-alert** command configures the switch to send MLD messages containing the Router-Alert option in IPv6 headers.

The **undo send-router-alert** command disables the switch from sending MLD messages containing the Router-Alert option in IPv6 headers.

By default, the MLD messages sent by the switch contain the Router-Alert option.

Format

send-router-alert

undo send-router-alert

Parameters

None

Views

MLD view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

By default, the MLD messages sent by the switch contain the Router-Alert option in their IPv6 headers. If the switch needs to communicate with a device that does not support the Router-Alert option, run the **undo send-router-alert** command to configure the switch to send MLD messages without the Router-Alert option. The **send-router-alert** command is usually used together with the **require-router-alert (MLD view)** command.

Prerequisites

Layer 3 IPv6 multicast has been enabled using the **multicast ipv6 routing-enable** command in the system view.

Precautions

The function of this command is the same as that of the **mld send-router-alert** command used in the interface view. The configuration in the MLD view is globally valid, whereas the configuration in the interface view takes effect only for the specified interface. The configuration in the interface view takes precedence over the configuration in the MLD view. The configuration in the MLD view is used only when no configuration is performed in the interface view.

Example

In the MLD view, configure the switch to send MLD packets with the Router-Alert option in IPv6 headers.

```
<HUAWEI> system-view
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] mld
[HUAWEI-mld] send-router-alert
```


8.2.43 ssm-mapping (MLD view)

Function

The **ssm-mapping** command configures an SSM mapping entry to map a multicast source to a group address.

The **undo ssm-mapping** command deletes an SSM mapping entry.

By default, no SSM mapping entry is configured.

Format

ssm-mapping *ipv6-group-address ipv6-group-mask-length ipv6-source-address*

undo ssm-mapping { **all** | *ipv6-group-address ipv6-group-mask-length* [*ipv6-source-address*] }

Parameters

Parameter	Description	Value
ipv6-group-address	Specifies the IPv6 address of a multicast group configured with SSM mapping.	The value is a 32-digit hexadecimal number in X:X:X:X:X:X:X:X format. The value ranges from FF00:: to FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF.
ipv6-group-mask-length	Specifies the mask length of the IPv6 multicast group address.	The value is an integer, which can be 16, 32, 64, or 128.
ipv6-source-address	Specifies the IPv6 address of a multicast source.	The value is a 32-digit hexadecimal number in X:X:X:X:X:X:X:X format.
all	Deletes all the configured static SSM mapping entries.	-

Views

MLD view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Hosts that support only MLDv1 cannot join SSM groups. To enable multicast devices to provide the SSM service for these hosts, configure SSM mapping on the

multicast devices. An SSM mapping entry maps a multicast source to a multicast group. After SSM mapping entries are configured on a multicast device, the device can convert (*, G) information in Report messages of MLDv1 to (S, G) information.

Prerequisites

Layer 3 IPv6 multicast has been enabled using the **multicast ipv6 routing-enable** command in the system view.

Precautions

- You can configure multiple static SSM mapping entries by running the **ssm-mapping** command several times.
- To delete an SSM mapping entry, run the **undo ssm-mapping** *ipv6-group-address ipv6-group-mask-length* [*ipv6-source-address*] command. The **undo ssm-mapping all** command deletes all the SSM mapping entries. Exercise caution before running this command.

Example

Configure an SSM mapping entry mapping the source address FC00::1 to group address FF35::1/128.

```
<HUAWEI> system-view
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] mld
[HUAWEI-mld] ssm-mapping ff35::1 128 fc00::1
```

8.2.44 timer other-querier-present (MLD view)

Function

The **timer other-querier-present** command sets a global other querier present timer.

The **undo timer other-querier-present** command restores the default value of the other querier present timer.

By default, the Keepalive period of the other queriers is calculated as follows:

Other querier present timer = Robustness variable x Interval for sending MLD General Query messages + 1/2 x Maximum response time

If the default values of the robustness variable, interval for sending MLD General Query messages, and maximum response time are used, the other querier present timer value is 255 seconds.

Format

timer other-querier-present *interval*

undo timer other-querier-present

Parameters

Parameter	Description	Value
interval	Specifies the other querier present timer.	The value is an integer that ranges from 60 to 300, in seconds.

Views

MLD view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When a user network segment connects to multiple Layer 3 multicast devices, only one Layer 3 multicast device is elected as the MLD querier to send Query messages to hosts on the network segment. To create and maintain normal group memberships, non-queriers running MLD start the other querier present timer after they fail in the querier election. If the non-queriers do not receive Query messages from the querier before the timer times out, they consider the querier failed and start a new querier election.

Prerequisites

Layer 3 IPv6 multicast has been enabled using the **multicast ipv6 routing-enable** command in the system view.

Precautions

The function of this command is the same as that of the **mld timer other-querier-present** command used in the interface view. The configuration in the MLD view is globally valid, whereas the configuration in the interface view takes effect only for the specified interface. The configuration in the interface view takes precedence over the configuration in the MLD view. The configuration in the MLD view is used only when no configuration is performed in the interface view.

NOTICE

If the other querier present timer is shorter than the interval for sending General Query messages, the querier election is triggered frequently.

Example

Set the other querier present timer to 200 seconds.

```
<HUAWEI> system-view
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] mld
[HUAWEI-mld] timer other-querier-present 200
```


8.2.45 timer query (MLD view)

Function

The **timer query** command sets a global interval for sending MLD General Query messages.

The **undo timer query** command restores the default interval for sending MLD General Query messages.

By default, the interval for sending MLD General Query messages is 125 seconds.

Format

timer query *interval*

undo timer query

Parameters

Parameter	Description	Value
interval	Interval for sending MLD General Query messages	The value is an integer that ranges from 1 to 18000, in seconds.

Views

MLD view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

An MLD querier checks whether a local network segment has multicast group members by sending MLD General Query messages at an interval, known as the general query interval. You can set the general query interval based on needs of your network. The general query interval affects the following processes:

- When a querier starts, it sends General Query messages a certain number of times specified by the robustness variable to query the multicast groups that have members on the shared network segment. The message sending interval during this process is 1/4 of the interval for sending General Query messages. The robustness variable can be set using the **mld robust-count** or **robust-count (MLD view)** command.
- After the startup process is complete, the querier sends General Query messages at intervals to maintain the group memberships on the interface.

Prerequisites

Layer 3 IPv6 multicast has been enabled using the **multicast ipv6 routing-enable** command in the system view.

Precautions

- The querier is more sensitive when it sends General Query messages at a smaller interval. However, more bandwidth and switch resources are consumed in this case.
- The function of this command is the same as that of the **mld timer query** command used in the interface view. The configuration in the MLD view is globally valid, whereas the configuration in the interface view takes effect only for the specified interface. The configuration in the interface view takes precedence over the configuration in the MLD view. The configuration in the MLD view is used only when no configuration is performed in the interface view.

Example

In the MLD view, set the interval for sending MLD General Query messages to 200 seconds.

```
<HUAWEI> system-view
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] mld
[HUAWEI-mld] timer query 200
```

8.2.46 ttl-check (MLD view)

Function

The **ttl-check** command enables the device to check the TTL values in received MLD Report, Done, and Query messages on all interfaces.

The **undo ttl-check** command restores the default configuration.

By default, the device does not check the TTL values in received MLD Report, Done, and Query messages.

Format

ttl-check

undo ttl-check

Parameters

None

Views

MLD view

Default Level

2: Configuration level

Usage Guidelines

To protect a device against MLD message attacks, run the **ttl-check** command to enable the device to check the TTL values in received MLD Report, Done, and Query messages on all interfaces and discard such a message if its TTL value is not 1.

Example

Enable the device to check the TTL values in received MLD Report, Done, and Query messages on all interfaces.

```
<HUAWEI> system-view
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] mld
[HUAWEI-mld] ttl-check
```

8.3 IPv4 PIM Configuration Commands

8.3.1 Command Support

Product	Support
S1700	Not supported.
S300	Supported.
S500	Supported.
S2700	Supported.
S5700	Supported except S5731-L and S5731S-L.
S6700	Supported.

NOTE

Only S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support the PIM multi-instance feature.

8.3.2 bsm semantic fragmentation (IPv4)

Function

The **bsm semantic fragmentation** command enables BSR message fragmentation.

The **undo bsm semantic fragmentation** command disables BSR message fragmentation.

By default, BSR message fragmentation is not enabled.

Format

bsm semantic fragmentation

undo bsm semantic fragmentation

Parameters

None

Views

PIM view of public network instance or PIM view of VPN instance

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A BSR message carries information about all C-RPs on the network. Therefore, if there is a large number of C-RPs on the network, the length of a BSR message exceeds the MTU of the outgoing interface. As a result, the BSR message cannot be processed and RP election fails. Consequently, multicast services cannot be transmitted normally. In this case, you can enable BSR message fragmentation to ensure that the devices on the network can learn consistent RP information and MDTs can be successfully established.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command.

Configuration Impact

You can also configure IP fragmentation to solve the preceding problem. The difference between IP fragmentation and BSR message fragmentation is as follows:

- If IP fragmentation is enabled, the protocol layer transmits the entire BSR message up to the IP layer regardless of the length of the BSR message. The BSR message is then fragmented at the IP layer. During the transmission of BSR message fragments to the destination, if one fragment is lost, the destination cannot parse the entire BSR message. As a result, the destination cannot learn RP information and MDTs cannot be established, which causes a multicast data forwarding failure.
- If BSR message fragmentation is enabled, the protocol layer directly fragments a long BSR message. During the transmission of BSR message fragments to the destination, if one fragment is lost, only the information carried in this fragment is lost. As a result, only MDTs corresponding to the information carried in the lost fragments cannot be established. Since the other BSR message fragments can still reach the destination, the corresponding MDTs can be correctly established.

BSR message fragmentation is recommended because IP fragmentation causes all fragments to become unavailable when fragment information is lost.

Precautions

Enable BSR message fragmentation on all devices on the network. If BSR message fragmentation is not enabled on some devices, RP information on these devices is inconsistent with that on other devices and MDTs cannot be established on these devices.

Example

Enable BSR message fragmentation in the public network instance PIM view.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] pim
[HUAWEI-pim] bsm semantic fragmentation
```

8.3.3 bsr-policy (IPv4)

Function

The **bsr-policy** command specifies the range of valid bootstrap router (BSR) addresses. Then the switch drops the BSR messages sent from the addresses out of this range to defend against BSR spoofing.

The **undo bsr-policy** command restores the default configuration.

By default, the range of BSR addresses is not limited, and all BSR packets are considered valid.

Format

bsr-policy *basic-acl-number*

undo bsr-policy

Parameters

Parameter	Description	Value
basic-acl-number	Specifies the basic ACL number. The ACL defines the filtering policy for the range of source addresses of BSR packets. This parameter corresponds to *basic-acl-number* in the **acl** command.	The value is an integer that ranges from 2000 to 2999.

Views

PIM view of public network instance or PIM view of VPN instance

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On a PIM-SM network that applies the BSR mechanism, you can configure any switch as a C-BSR to take part in BSR election. Once a switch is elected as the BSR, the switch is responsible for advertising RP information in the network. To prevent the valid BSR from being maliciously replaced, take the following measures:

- Certain hosts try changing the RP mapping to spoof the switch by forging BSR packets.

  Solution: The attack often occurs on edge switches because the BSR packet is a multicast packet with the TTL value of 1. As the BSR is inside the network and hosts are outside the network, the switches can perform neighbor checks and RPF checks on the received BSR packets to prevent the attack.
- Certain attackers control the switch on the network, or the switch accesses the network. The attackers configure the switch as a C-BSR, and help the switch win the BSR election. The attackers obtain the right of advertising RP information in the network.

  Solution: After the switch is configured as a C-BSR, the switch spreads multicast BSR packets in the network. The BSR packets have a TTL value of 1 and are forwarded hop by hop. As long as the neighboring switch cannot receive the packets, the packets are not spread in the entire network. The solution is to use the **bsr-policy** command on every switch in the network to limit the valid BSR range. For example, only switches 10.1.1.1/32 and 10.1.1.2/32 are elected as BSRs; therefore, the switches do not receive or forward other BSR packets.

The two countermeasures mentioned above can partially protect BSRs in the network. However, if attackers control a valid BSR, problems can still be caused on the network.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command.

Configuration Impact

After the **bsr-policy** command is run, the switch accepts only BSR messages matching the configured policy.

Precautions

The **bsr-policy** command and the **acl** command are used together. In the ACL view, you can set the source address range for BSR packets by specifying the **source** parameter in the **rule** command.

Example

In the public network instance PIM view, configure address 10.1.1.0/24 as the valid BSR address range.

```
<HUAWEI> system-view
[HUAWEI] acl number 2001
[HUAWEI-acl-basic-2001] rule permit source 10.1.1.0 0.0.0.255
[HUAWEI-acl-basic-2001] quit
```



```
[HUAWEI] pim
[HUAWEI-pim] bsr-policy 2001
```

8.3.4 c-bsr (IPv4)

Function

The **c-bsr** command configures a C-BSR.

The **undo c-bsr** command restores the default configuration.

By default, the C-BSR is not configured.

Format

c-bsr *interface-type interface-number* [*hash-length* [*priority*]]

undo c-bsr

Parameters

Parameter	Description	Value
interface-type interface-number	Specifies the type and the number of an interface. C-BSR is configured on this interface. PIM-SM must be enabled on this interface to make the configuration effective. **NOTE** To avoid frequent protocol changes caused by interface flapping, using loopback interfaces is recommended.	-
hash-length	Specifies the hash mask length of the C-BSR. The mask is used in a hash function to calculate the RP.	The value is an integer that ranges from 0 to 32. By default, the value is 30.
priority	Specifies a priority of the C-BSR. The greater the value, the higher the priority of the C-BSR.	The value is an integer ranging from 0 to 255. By default, the value is 0.

Views

PIM view of public network instance or PIM view of VPN instance

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

One or more C-BSRs need to be configured in a PIM-SM domain. A BSR is elected from C-BSRs and is responsible for collecting C-RP information and summarizing C-RP information into an RP-set. The RP-set is then encapsulated in a BootStrap message and advertised to all the devices in the PIM domain.

The process of BSR election is as follows:

1. Each C-BSR considers itself as the BSR of the local PIM-SM domain and uses IP address of this interface as the address of the BSR to send Bootstrap messages.
2. When a C-BSR receives a Bootstrap message from other devices, it compares the BSR in the received Bootstrap message with the current BSR. The BSR with the highest priority is preferred. If BSRs have the same priority, the BSR with a larger IP address is preferred. If the BSR carried in the received Bootstrap message is superior to the current BSR, the C-BSR replaces its BSR address with the address of the BSR carried in the received Bootstrap message.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command.

Before configuring an interface as a C-BSR, enable PIM-SM on the interface.

For the multicast BSR messages learned through the GRE tunnel, you need to configure a static multicast route to ensure that the next hop to the BSR is a GRE interface. You need to configure static multicast routes properly to avoid routing loops.

Example

In the PIM view of public network instance, configure a C-BSR on VLANIF100.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] pim sm
[HUAWEI-Vlanif100] quit
[HUAWEI] pim
[HUAWEI-pim] c-bsr vlanif 100
```

In the PIM view, configure a C-BSR on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] pim sm
[HUAWEI-GigabitEthernet0/0/1] quit
[HUAWEI] pim
[HUAWEI-pim] c-bsr gigabitethernet 0/0/1
```

8.3.5 c-bsr admin-scope

Function

The **c-bsr admin-scope** command configures a BSR administrative scope in a PIM-SM domain.

The **undo c-bsr admin-scope** command restores the default configuration.

By default, no BSR administrative scope is configured.

Format

c-bsr admin-scope

undo c-bsr admin-scope

Parameters

None

Views

PIM view of public network instance or PIM view of VPN instance

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

By default, each PIM-SM domain has only one BSR that serves all the devices in the entire PIM-SM domain. To achieve more effective management, you can divide a PIM-SM domain into multiple BSR administrative domains and a global domain. This can reduce the workload of a single BSR and designate a private-network group address for users in a specific domain.

Each BSR administrative domain maintains one BSR that serves multicast groups on network segment 239.0.0.0/8. Multicast packets for groups on this network segment cannot pass through the border of the BSR administrative domain. Multicast groups that do not belong to any BSR administrative domain belong to a global domain. The global domain maintains a BSR that serves all the remaining multicast groups, namely, multicast groups beyond the range 239.0.0.0/8.

A BSR administrative domain is similar to a VPN in unicast, and multicast address segment 239.0.0.0/8 is equivalent to unicast address segment 10.0.0.0/8. Other multicast group addresses can be used on the public network and address conflicts need be avoided. If a PIM-SM domain is divided into different BSR administrative domains, each BSR administrative domain is equivalent to a VPN, serving the multicast groups on the network segment 239.0.0.0/8. You can use the same multicast group address in different BSR administration domains. If you configure the BSR in a BSR administration domain to serve multicast groups beyond 239.0.0.0/8, a message indicating a configuration error will be displayed.

The **c-bsr admin-scope** command configures a BSR administrative scope on the switch.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command.

Configuration Impact

After the **undo pim** command or the **undo multicast routing-enable** command is run in the system view, the BSR administrative domain is automatically disabled.

Precautions

The **c-bsr admin-scope** command needs to be run on all the devices in a PIM-SM domain.

Example

In the public network instance PIM view, configure a BSR administrative scope in a PIM-SM domain.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] pim
[HUAWEI-pim] c-bsr admin-scope
```

8.3.6 c-bsr global

Function

The **c-bsr global** command configures the switch as a C-BSR in the global domain.

The **undo c-bsr global** command restores the default configuration.

By default, no C-BSR is configured in the global domain.

Format

c-bsr global [**hash-length** *hash-length* | **priority** *priority*] *

undo c-bsr global

Parameters

Parameter	Description	Value
hash-length *hash-length*	Specifies the hash mask length of a C-BSR in the global domain.	The value is an integer that ranging from 0 to 32. By default, the value is 30.
priority *priority*	Specifies the priority of the C-BSR in the global domain. The greater the value, the higher the priority of the C-BSR.	The value is an integer ranging from 0 to 255. By default, it is 0.

Views

PIM view of public network instance or PIM view of VPN instance

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

By default, each PIM-SM domain has only one BootStrap router (BSR) and the BSR serves all the devices in the entire PIM-SM domain. To achieve more effective management, you can divide a PIM-SM domain into multiple BSR administrative domains and a global domain.

Each BSR administrative domain maintains one BSR that serves the multicast groups in a specific group address range. Multicast packets for groups in the range cannot pass through the border of the BSR administrative domain. Addresses of multicast groups that BSRs in different BSR administrative domains serve can overlap. Overlapped multicast groups, however, similar to private group addresses, take effect only in local BSR administrative domains. Multicast groups that do not belong to any BSR administrative domain belong to a global domain. A global domain maintains a BSR that serves all the remained multicast groups.

The **c-bsr global** command configures the switch as a C-BSR in the global domain. The BSR in the global domain is generated through election.

C-BSRs compare the priorities and IP addresses to elect the BSR in the global area. The conditions for the election are as follows:

- The C-BSR with the highest priority is elected as the BSR.
- In the case of the same priority, the C-BSR with the largest IP address is elected as the BSR.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command.

Configuration Impact

If the **c-bsr global** command is run several times, the latest configuration overrides the previous one.

After the **undo pim** command or the **undo multicast routing-enable** command is run in the system view, the C-BSRs in the global domain are automatically disabled.

Precautions

The **c-bsr global** command takes effect only in a BSR administrative domain and can enable a device in a BSR administrative domain to receive multicast data of groups beyond 239.0.0.0/8.

The **c-bsr global** command needs to be used together with the **c-bsr admin-scope** command.

Example

In the public network instance PIM view, configure the switch as a C-BSR in the global domain, and then set the priority of the C-BSR to 1.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] pim
[HUAWEI-pim] c-bsr global priority 1
```

8.3.7 c-bsr group

Function

The **c-bsr group** command specifies the range of multicast groups that an administrative domain can serve on a C-BSR.

The **undo c-bsr group** command restores the default configuration.

By default, range of multicast groups that an administrative domain can serve is not configured.

Format

c-bsr group *group-address* { *mask* | *mask-length* } [**hash-length** *hash-length* | **priority** *priority*] *

undo c-bsr group *group-address*

Parameters

Parameter	Description	Value
group-address	Specifies a multicast group address.	The address is in dotted decimal notation. The value ranges from 239.0.0.0 to 239.255.255.255.
mask	Specifies the mask of a multicast group address.	The address is in dotted decimal notation.
mask-length	Indicates the mask length of a multicast address.	The value is an integer ranging from 8 to 32.
hash-length *hash-length*	Specifies the hash mask length for the C-BSR in a BSR administrative domain.	The value is an integer ranging from 0 to 32. By default, it is 30.
priority *priority*	Specifies the priority of the C-BSR in the BSR administrative domain. A larger value indicates a higher priority.	The value is an integer ranging from 0 to 255. By default, it is 0.

Views

PIM view of public network instance or PIM view of VPN instance

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After a PIM-SM domain is divided into different BSR administrative domains, configure a multicast group address for each BSR administrative domain on the C-BSR. The group addresses must be in the range of 239.0.0.0/8. The group address ranges served by different BSR administrative domains can overlap. The address of a multicast group that a BSR administrative domain serves is used as a private group address.

By running this command on the C-BSR of each administrative domain, you can specify the group address of the administrative domain served by each C-BSR and the priority of each C-BSR.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command in the public network instance or VPN instance.

Configuration Impact

If the **c-bsr group** command is run several times, the latest configuration overrides the previous one.

After the **undo pim** command or the **undo multicast routing-enable** command is run in the system view or the VPN instance view, the C-BSRs in the BSR administrative domain are automatically disabled.

Example

In the public network instance PIM view, configure a C-BSR in the BSR administrative domain to serve groups 239.0.0.0/8, and set the priority of the C-BSR to 10.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] pim
[HUAWEI-pim] c-bsr group 239.0.0.0 255.0.0.0 priority 10
```

8.3.8 c-bsr hash-length (IPv4)

Function

The **c-bsr hash-length** command configures the global hash mask length of a C-BSR.

The **undo c-bsr hash-length** command restores the default configuration.

By default, the global hash mask length of a C-BSR is 30.

Format

c-bsr hash-length *hash-length*

undo c-bsr hash-length

Parameters

Parameter	Description	Value
hash-length	Specifies the global hash mask length of a C-BSR.	The value is an integer that ranges from 0 to 32.

Views

PIM view of public network instance or PIM view of VPN instance

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

During dynamic RP election, if C-RPs have the same interface address mask and priority for a specified multicast group, a hash function needs to be executed to select the RP for the multicast group. The switch performs hash calculation for the group address of G, C-RP address, and hash mask length of the C-RPs with the same priority and compares the hash values. The C-RP with the greatest hash value acts as the RP for G.

The hash mask length is used to adjust the hash calculation result.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command.

Precautions

You can run the **c-bsr** *interface-type interface-number hash-length* command in the PIM view to configure the C-BSR interface and specify the hash mask length. The **c-bsr hash-length** *hash-length* command specifies the global hash mask length. If both **c-bsr** *interface-type interface-number hash-length* and **c-bsr hash-length** *hash-length* are used, the **c-bsr** *interface-type interface-number hash-length* command takes effect.

Example

In the public network instance PIM view, set the global hash mask length of a C-BSR to 16.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] pim
[HUAWEI-pim] c-bsr hash-length 16
```


8.3.9 c-bsr holdtime (IPv4)

Function

The **c-bsr holdtime** command configures the timeout period during which the C-BSR waits to receive Bootstrap messages sent by the BSR.

The **undo c-bsr holdtime** command restores the default configuration.

By default, the timeout period during which the C-BSR waits to receive Bootstrap messages sent by the BSR is 130s.

Format

c-bsr holdtime *interval*

undo c-bsr holdtime

Parameters

Parameter	Description	Value
interval	Specifies the timeout time during which C-BSR waits for the Bootstrap message to be sent by BSR.	The value is an integer that ranges from 1 to 214748364, in seconds.

Views

PIM view of public network instance or PIM view of VPN instance

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After a C-BSR is elected as the BSR, it periodically sends Bootstrap messages carrying its own IP address and the RP-set information. The interval for sending Bootstrap messages is BS_interval, which can be configured using the **c-bsr interval** command.

Other C-BSRs that fail in the election are suppressed from sending Bootstrap messages and start the timer to monitor the elected BSR. The timeout period of a timer is holdtime, which can be configured using the **c-bsr holdtime** command.

- If the C-BSR receives the Bootstrap messages sent by the BSR, the C-BSR refreshes the timer. The C-BSRs that fail in the election also refresh the timeout period of the BSR according to the holdtime. After the BSR times out, the C-BSRs receive new BSR messages.
- If the timer times out, the elected BSR is considered faulty. The C-BSRs that failed in the election triggers a new BSR election, preventing service interruption.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command.

Precautions

In actual applications, all C-BSRs in the same PIM domain must use the same BS_interval and holdtime; otherwise, the BSR will become unstable. This may result in multicast faults. Note the following points:

- If BS_interval and holdtime are configured at the same time, ensure that BS_interval is less than holdtime.
- If BS_interval or holdtime is configured, use the following formula to calculate the other one: holdtime = 2 x BS_interval + 10. The following determines which value is used:
  - If holdtime is configured and the calculated BS_interval is less than the minimum value of BS_interval, the minimum value is used.
  - If BS_interval is configured and the calculated holdtime is more than the maximum value of holdtime, the maximum value is used.
- If neither BS_interval nor holdtime is configured, the default values are used. The default BS_interval is 60s and the default holdtime is 130s.

Example

In the PIM view of public network instance, set the timeout interval during which the C-BSR waits for the Bootstrap message to be sent by BSR to 150 seconds.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] pim
[HUAWEI-pim] c-bsr holdtime 150
```

8.3.10 c-bsr interval (IPv4)

Function

The **c-bsr interval** command configures the interval for the BSR to continuously send Bootstrap messages.

The **undo c-bsr interval** command restores the default configuration.

By default, the interval for the BSR to continuously send Bootstrap messages is 60s.

Format

c-bsr interval *interval*

undo c-bsr interval

Parameters

Parameter	Description	Value
interval	Specifies the interval for the BSR to continuously send the Bootstrap messages.	The value is an integer that ranges from 1 to 107374177, in seconds.

Views

PIM view of public network instance or PIM view of VPN instance

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After a C-BSR is elected as the BSR, it periodically sends Bootstrap messages carrying its own IP address and the RP-set information to the network.

Other C-BSRs that fail in the election are suppressed from sending Bootstrap messages and start the timer to monitor the BSR. The timeout period of a timer is holdtime, which can be configured using the **c-bsr holdtime** command. The following applies to the timer:

- If the C-BSR receives the Bootstrap messages sent by the BSR, the C-BSR refreshes the timer.
- If the timer times out, the BSR is considered to be faulty. The C-BSRs that failed in the election triggers a new BSR election, preventing service interruption.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command.

Precautions

In actual applications, all C-BSRs in the same PIM domain must use the same BS_interval and holdtime values; otherwise, the BSR will become unstable. This may result in a multicast fault. Note the following points:

- If BS_interval and holdtime are configured at the same time, ensure that BS_interval is less than holdtime.
- If only one of the BS_interval and holdtime is configured, use the following formula to calculate the other parameter: holdtime = 2 x BS_interval + 10. The following determines which value is used:
  - If holdtime is configured and the calculated BS_interval is less than the minimum value of BS_interval, the minimum value is used.
  - If BS_interval is configured and the calculated holdtime is more than the maximum value of holdtime, the maximum value is used.

- If neither the BS_interval nor the holdtime is configured, default values are used. The default value of BS_interval is 60s, and the default value of holdtime is 130s.

Example

In the PIM view of public network instance, set the interval for the C-BSR to continuously send Bootstrap messages to 30 seconds.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] pim
[HUAWEI-pim] c-bsr interval 30
```

8.3.11 c-bsr priority (IPv4)

Function

The **c-bsr priority** command configures the global priority for a C-BSR.

The **undo c-bsr priority** command restores the default configuration.

By default, the global priority of the C-BSR is 0.

Format

c-bsr priority *priority*

undo c-bsr priority

Parameters

Parameter	Description	Value
priority	Specifies the global priority of the C-BSR. The greater the value, the higher the priority of the C-BSR.	The value is an integer that ranges from 0 to 255.

Views

PIM view of public network instance or PIM view of VPN instance

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When multiple C-BSRs take part in the BSR election in the PIM-SM domain, the following situations occur:

- The switch with the highest priority wins in the BSR election.

- If they have the same priority, the switch with the largest IP address wins in the BSR election.

To enable a C-BSR to function as the BSR, you can run the **c-bsr priority** command to increase the priority value of the C-BSR.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command.

Precautions

You can run the **c-bsr** *interface-type interface-number priority* command in the PIM view to configure the C-BSR interface and specify the C-BSR priority. The **c-bsr priority** *priority* command specifies the global C-BSR priority. If both **c-bsr** *interface-type interface-number priority* and **c-bsr priority** *priority* are used, the **c-bsr** *interface-type interface-number priority* command takes effect.

Example

In the PIM view of public network instance, configure the global priority of the C-BSR to 5.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] pim
[HUAWEI-pim] c-bsr priority 5
```

8.3.12 c-rp (IPv4)

Function

The **c-rp** command configures the switch to advertise itself as a C-RP to the BSR.

The **undo c-rp** command restores the default configuration.

By default, no C-RP is configured.

Format

c-rp *interface-type interface-number* [**group-policy** *basic-acl-number* | **priority** *priority* | **holdtime** *hold-interval* | **advertisement-interval** *adv-interval*] *

undo c-rp *interface-type interface-number*

Parameters

Parameter	Description	Value
interface-type interface-number	Specifies the type and the number of an interface. The IP address of the specified interface is advertised as a C-RP address. **NOTE** To avoid frequent protocol changes caused by interface flapping, using loopback interfaces is recommended.	-
group-policy *basic-acl-number*	Specifies the range of the multicast groups served by a C-RP. The range is restricted to the multicast group range permitted by the specified ACL. The *basic-acl-number* parameter specifies the number of the basic ACL to identify the service range of the advertised RP.	The value is an integer ranging from 2000 to 2999.
priority *priority*	Specifies the priority of a C-RP. The greater the value, the lower the priority.	The value is an integer ranging from 0 to 255. The default value is 0.
holdtime *hold-interval*	Specifies the timeout period during which the BSR waits to receive an Advertisement message from a C-RP.	The value is an integer ranging from 1 to 65535, in seconds. The default value is 150.
advertisement-interval *adv-interval*	Specifies the interval for a C-RP to send Advertisement messages.	The value is an integer ranging from 1 to 65535, in seconds. The default value is 60.

Views

PIM view of public network instance or PIM view of VPN instance

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

An RP is the core of a PIM-SM domain, and therefore a C-RP must be able to communicate with the other devices in the PIM-SM domain. You are advised to

configure a C-RP on the core switch and reserve enough bandwidth between the switch and each of the other devices in the PIM-SM domain.

An RP is elected from multiple C-RPs following these rules, in descending order of precedence:

1. The C-RP with the longest mask length of the served group address range matching the multicast group that users have joined wins.
2. The C-RP with highest priority wins.
3. The C-RP with the largest hash value wins.
4. The C-RP with the largest address wins.

Prerequisites

- IP multicast routing has been enabled using the **multicast routing-enable** command.
- PIM-SM has been enabled on the interface that acts as the C-RP.

Configuration Impact

An interface is specified in the command; therefore, the settings of **group-policy** *basic-acl-number*, **priority** *priority*, **holdtime** *hold-interval* and **advertisement-interval** *adv-interval* configured using this command override the global parameter settings that the interface obtains from the PIM view. If you run this command multiple times and specify the same interface, only the latest configuration takes effect.

NOTE

If IP address unnumbered is configured, it is not recommended to configure C-RP on the interfaces that use the same addresses. If the interfaces have different priorities, the BSR considers that the C-RP configuration has been repeatedly modified.

Precautions

- *basic-acl-number* specifies a group range. All permitted group ranges will be advertised as the ranges of groups that the RP serves. If no group range is specified, the C-RP serves all multicast groups.
- To enable a C-RP to serve multiple PIM-SM domains, configure multiple **rule**s in the ACL to specify multicast group ranges for the domains.
- The **c-rp** command needs to be used together with the **acl** command. In the ACL view, **source** can be specified in the **rule** command to specify the range of groups that a C-RP serves.

Example

In the PIM view of public network instance, use basic ACL 2069 to specify Loopback 0 as the C-RP for PIM-SM domains 225.1.0.0/16 and 226.2.0.0/16, and set the C-RP priority to 10.

```
<HUAWEI> system-view
[HUAWEI] acl number 2069
[HUAWEI-acl-basic-2069] rule permit source 225.1.0.0 0.0.255.255
[HUAWEI-acl-basic-2069] rule permit source 226.2.0.0 0.0.255.255
[HUAWEI-acl-basic-2069] quit
[HUAWEI] multicast routing-enable
[HUAWEI] interface loopback 0
```



```
[HUAWEI-LoopBack0] pim sm
[HUAWEI-LoopBack0] quit
[HUAWEI] pim
[HUAWEI-pim] c-rp loopback 0 group-policy 2069 priority 10
```

8.3.13 c-rp advertisement-interval (IPv4)

Function

The **c-rp advertisement-interval** command sets the interval at which a C-RP sends Advertisement messages.

The **undo c-rp advertisement-interval** command restores the default interval.

By default, a C-RP sends Advertisement messages at an interval of 60 seconds.

Format

c-rp advertisement-interval *interval*

undo c-rp advertisement-interval

Parameters

Parameter	Description	Value
interval	Specifies the interval at which a C-RP sends Advertisement messages.	The value ranges from 1 to 65535, in seconds.

Views

PIM view of public network instance or PIM view of VPN instance

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

All C-RPs in a PIM-SM domain periodically send Advertisement messages to the same BSR. The BSR can collect the integrated RP-Set.

The **c-rp advertisement-interval** command sets the interval at which a C-RP sends Advertisement messages to the BSR.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command.

Precautions

You can also set the advertisement interval when you run the **c-rp** *interface-type interface-number* **advertisement-interval** *adv-interval* command in the PIM view

to configure the C-RP interface. The **c-rp advertisement-interval** *interval* command specifies the global advertisement interval. If both the commands are configured, the interval configured by the **c-rp** *interface-type interface-number* **advertisement-interval** *adv-interval* command takes effect.

Example

In the PIM view of public network instance, set the interval at which a C-RP sends Advertisement messages to 30s.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] pim
[HUAWEI-pim] c-rp advertisement-interval 30
```

8.3.14 c-rp holdtime (IPv4)

Function

The **c-rp holdtime** command configures the holdtime for a received Advertisement message on a BSR.

The **undo c-rp holdtime** command restores the default holdtime.

By default, the holdtime for a received Advertisement message is 150 seconds.

Format

c-rp holdtime *interval*

undo c-rp holdtime

Parameters

Parameter	Description	Value
interval	Specifies the timeout period for a BSR to wait the Advertisement message from a C-RP.	The value ranges from 1 to 65535, in seconds.

Views

PIM view of public network instance or PIM view of VPN instance

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When *interval* is set on a C-RP, the C-RP encapsulates *interval* in an Advertisement message and sends it to the BSR. The BSR obtains this *interval* from the message and starts the timer. If the BSR receives no Advertisement message from the C-RP within the timeout period, the BSR regards the C-RP invalid or unreachable.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command.

Precautions

You can also set the holdtime for a received Advertisement message when you run the **c-rp** *interface-type interface-number* **holdtime** *hold-interval* in the PIM view to configure a C-PR interface. The **c-rp holdtime** *hold-interval* configures the global holdtime for Advertisement messages. If both the two commands are configured, the holdtime configured by the **c-rp** *interface-type interface-number* **holdtime** *hold-interval* command takes effect.

Example

In the PIM view of public network instance, set the holdtime for a received Advertisement message to 100s.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] pim
[HUAWEI-pim] c-rp holdtime 100
```

8.3.15 c-rp priority (IPv4)

Function

The **c-rp priority** command configures the global priority of a C-RP.

The **undo c-rp priority** command restores the default configuration.

By default, the global priority of a C-RP is 0.

Format

c-rp priority *priority*

undo c-rp priority

Parameters

Parameter	Description	Value
priority	Specifies the global priority of a C-RP. The greater the value, the lower the priority.	The value is an integer that ranges from 0 to 255.

Views

PIM view of public network instance or PIM view of VPN instance

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The following rules are used to elect an RP from multiple C-RPs, in descending order of precedence:

- The C-RP with the interface address that has the longest mask wins.
- The C-RP with highest priority wins.
- The C-RP with the largest hash value wins.
- The C-RP with the largest address wins.

To enable a C-RP to function as an RP, you can run the **c-rp priority** command to increase the priority of the C-RP.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command.

Precautions

You can run the **c-rp** *interface-type interface-number* **priority** *priority* command in the PIM view to configure the C-RP interface and specify the C-RP priority. The **c-rp priority** *priority* command specifies the global C-RP priority. If both **c-rp** *interface-type interface-number* **priority** *priority* and **c-rp priority** *priority* are used, the **c-rp** *interface-type interface-number* **priority** *priority* command takes effect.

Example

In the PIM view of public network instance, set the global priority of a C-RP to 5.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] pim
[HUAWEI-pim] c-rp priority 5
```

8.3.16 crp-policy (IPv4)

Function

The **crp-policy** limits the range of valid C-RP addresses and the range of the multicast addresses served by a C-RP. The BSR drops the C-RP messages with addresses out of the specified range to protect valid C-RPs.

The **undo crp-policy** command restores the default configuration.

By default, the BSR does not limit the range of valid C-RP addresses and the range of the multicast groups served by a C-RP. The BSR considers all the received C-RP messages valid.

Format

crp-policy *advanced-acl-number*

undo crp-policy

Parameters

Parameter	Description	Value
advanced-acl-number	Specifies the number of an advanced ACL. The ACL defines the range of the C-RP addresses and the range of the group addresses served by a C-RP.	The value is an integer that ranges from 3000 to 3999.

Views

PIM view of public network instance or PIM view of VPN instance

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On a PIM SM network that uses the BSR mechanism, any switch can be configured as a C-RP to serve the multicast groups in a specified range. Each C-RP sends its information to the BSR in unicast mode. The BSR summarizes all received C-RP information into am RP-set and floods it on the entire network using BSR messages. The local switch then works out the RP serving a specific multicast group address range according to the RP-set.

To protect valid C-RPs from spoofing, configure **crp-policy** on BSR switches to limit the range of valid C-RP addresses and the range of multicast group addresses served by a C-RP. Configure the same filtering rule on each C-BSR because any C-BSR can become the BSR.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command.

Configuration Impact

If an ACL rule is specified but no C-RP address range is set, all C-RP messages are denied.

Precautions

The **crp-policy** command and the **acl** command are used together. In the ACL view, you can set the valid source address range for the C-RP by specifying the **source** parameter in the **rule** command. You can set the address range of multicast groups that are served by specifying the **destination** parameter in the **rule** command.

A received C-RP message matches the configured filtering policy only when the C-RP address carried by the message matches **source** and the group address range carried by the message is a subset of the group address range defined in the ACL.

Example

Configure a C-RP policy on the C-BSR, which allows only the C-RP with the address 10.1.1.1/32 and allows the C-RP to serve only the multicast groups 225.1.0.0/16.

```
<HUAWEI> system-view
[HUAWEI] acl number 3100
[HUAWEI-acl-adv-3100] rule permit ip source 10.1.1.1 0 destination 225.1.0.0 0.0.255.255
[HUAWEI-acl-adv-3100] quit
[HUAWEI] multicast routing-enable
[HUAWEI] pim
[HUAWEI-pim] crp-policy 3100
```

8.3.17 display default-parameter pim-dm

Function

The **display default-parameter pim-dm** command displays default configurations about PIM-DM.

Format

display default-parameter pim-dm

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The **display default-parameter pim-dm** command displays default configurations about PIM-DM. Even if PIM-DM parameters are modified, the **display default-parameter pim-dm** command still displays default parameter settings. Therefore, you can use this command to check which parameters on the device have been modified.

Example

Display default configurations about PIM-DM.

```
<HUAWEI> display default-parameter pim-dm
 PIM View Default Configurations:
 --------------------------------
 Hello-option dr-priority: 1
 Hello-option holdtime: 105 s
 Hello-option lan-delay: 500 ms
 Hello-option neighbor-tracking: disabled
 Hello-option override-interval: 2500 ms
```



```
Holdtime assert: 180 s
Holdtime join-prune: 210 s
Source-lifetime: 210 s
State-refresh-interval: 60 s
State-refresh-rate-limit: 30 s
State-refresh-ttl: 255
Hello periodic interval: 30 s
Join-prune periodic interval: 60 s

Interface View Default Configurations:
--------------------------------------
Pim bfd: disabled
Pim hello-option dr-priority: 1
Pim hello-option holdtime: 105 s
Pim hello-option lan-delay: 500 ms
Pim hello-option neighbor-tracking: disabled
Pim hello-option override-interval: 2500 ms
Pim holdtime assert: 180 s
Pim holdtime join-prune: 210 s
Pim require-genid: disabled
Pim silent: disabled
Pim state-refresh-capable: enabled
Pim timer dr-switch-delay: disabled
Pim timer graft-retry: 3 s
Pim hello periodic interval: 30 s
Pim join-prune periodic interval: 60 s
Pim triggered-hello-delay: 5 s
Pim version: 2
Pim ipsec sa: disabled
Pim neighbor-policy: disabled
```

Table 8-36 Description of the **display default-parameter pim-dm** command output

Item	Description
PIM View Default Configurations	Default configurations in the PIM view.
Hello-option dr-priority	Priority for DR election. This parameter is configured by the **hello-option dr-priority (IPv4)** command.
Hello-option holdtime	Time period for the neighbor to hold the reachable state. This parameter is configured by the **hello-option holdtime (IPv4)** command.
Hello-option lan-delay	Delay in transmitting Prune messages at a shared network segment. This parameter is configured by the **hello-option lan-delay (IPv4)** command.
Hello-option neighbor-tracking	Whether neighbor tracking is enabled. ● enabled: Neighbor tracking is enabled. ● disabled: Neighbor tracking is disabled This function is configured using the **hello-option neighbor-tracking (IPv4)** command.

Item	Description
Hello-option override-interval	Interval for sending Prune Override messages. This parameter is configured by the **hello-option override-interval (IPv4)** command.
Holdtime assert	Time period for holding the Assert state. This parameter is configured by the **holdtime assert (IPv4)** command.
Holdtime join-prune	Time period for holding the Join or Prune state. This parameter is configured by the **holdtime join-prune (IPv4)** command.
Source-lifetime	Timeout period of an (S, G) entry. This parameter is configured by the **source-lifetime (IPv4)** command.
State-refresh-interval	Interval for sending State-Refresh messages. This parameter is configured by the **state-refresh-interval (IPv4)** command.
State-refresh-rate-limit	Minimum interval from when the last State-Refresh message is received to when the next State-Refresh message is received. This parameter is configured by the **state-refresh-rate-limit (IPv4)** command.
State-refresh-ttl	TTL value of the State-Refresh message. This parameter is configured by the **state-refresh-ttl (IPv4)** command.
Hello periodic interval	Interval for sending Hello messages. This parameter is configured by the **timer hello (IPv4)** command.
Join-prune periodic interval	Interval for sending Join/Prune messages. This parameter is configured by the **timer join-prune (IPv4)** command.
Interface View Default Configurations	Default configurations in the interface view.
Pim bfd	Whether PIM BFD is enabled on the interface. This parameter is configured by the **pim bfd enable** command.
Pim hello-option dr-priority	Priority for DR election on the interface. This parameter is configured by the **pim hello-option dr-priority** command.

Item	Description
Pim hello-option holdtime	Time period for the neighbor on the interface to hold the reachable state. This parameter is configured by the **pim hello-option holdtime** command.
Pim hello-option lan-delay	Delay in transmitting Prune messages at the shared network segment where the interface resides. This parameter is configured by the **pim hello-option lan-delay** command.
Pim hello-option neighbor-tracking	Whether neighbor tracking is enabled on the interface. ● enabled: Neighbor tracking is enabled. ● disabled: Neighbor tracking is disabled This function is configured using the **pim hello-option neighbor-tracking** command.
Pim hello-option override-interval	Interval for the interface to send Prune Override messages. This parameter is configured by the **pim hello-option override-interval** command.
Pim holdtime assert	Time period for the interface to hold the Assert state. This parameter is configured by the **pim holdtime assert** command.
Pim holdtime join-prune	Time period for the interface to hold the Join or Prune state. This parameter is configured by the **pim holdtime join-prune** command.
Pim require-genid	Whether the received Hello message is required to carry the Generation ID. ● enabled: The received Hello message is required to carry the Generation ID. ● disabled: The received Hello message is not required to carry the Generation ID. This parameter is configured using the **pim require-genid** command.

Item	Description
Pim silent	Whether the interface is set to PIM silent state. ● enabled: The interface is in PIM silent state. ● disabled: The interface is not in PIM silent state. This function is configured using the **pim silent** command.
Pim state-refresh-capable	Whether State-Refresh is enabled on the interface. ● enabled: State-Refresh is enabled on the interface. ● disabled: State-Refresh is disabled on the interface. This function is configured using the **pim state-refresh-capable** command.
Pim timer dr-switch-delay	Whether the DR switch delay is set on the interface. ● enabled: The DR switch delay is set on the interface. ● disabled: The DR switch delay is not set on the interface. This parameter is configured by the **pim timer dr-switch-delay** command.
Pim timer graft-retry	Interval for the interface to retransmit Graft messages. This parameter is configured by the **pim timer graft-retry** command.
Pim hello periodic interval	Interval for the interface to send Hello messages. This parameter is configured by the **pim timer hello** command.
Pim join-prune periodic interval	Interval for the interface to send Join/Prune messages. This parameter is configured by the **pim timer join-prune** command.
Pim triggered-hello-delay	Maximum delay for the interface to send Hello messages. This parameter is configured by the **pim triggered-hello-delay** command.
Pim version	Version of PIM enabled on the interface.

Item	Description
Pim ipsec sa	Whether PIM IPSec is enabled on the interface. This parameter is configured by the **pim ipsec sa** command.
Pim neighbor-policy	Whether a neighbor policy is configured on the interface. • enabled: A neighbor policy is configured on the interface. • disabled: No neighbor policy is configured on the interface. This parameter is configured by the **pim neighbor-policy** command.

8.3.18 display default-parameter pim-sm

Function

The **display default-parameter pim-sm** command displays default configurations about PIM-SM.

Format

display default-parameter pim-sm

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The **display default-parameter pim-sm** command displays default configurations about PIM-SM. Even if PIM-SM parameters are modified, the **display default-parameter pim-sm** command still displays default parameter settings. Therefore, you can use this command to check which parameters on the device have been modified.

Example

Display default configurations about PIM-SM.


```
<HUAWEI> display default-parameter pim-sm
 PIM View Default Configurations:
 --------------------------------
 Auto-rp listening enable: disabled
 Bsr-policy: disabled
 C-bsr admin-scope: disabled
 C-bsr global: disabled
 C-bsr group: none
 C-bsr hash-length: 30
 C-bsr holdtime: 130 s
 C-bsr interval: 60 s
 C-bsr priority: 0
 C-rp advertisement-interval: 60 s
 C-rp holdtime: 150 s
 C-rp priority: 0
 Crp-policy: disabled
 Bsm semantic fragmentation: disabled
 Hello-option dr-priority: 1
 Hello-option holdtime: 105 s
 Hello-option lan-delay: 500 ms
 Hello-option neighbor-tracking: disabled
 Hello-option override-interval: 2500 ms
 Holdtime assert: 180 s
 Holdtime join-prune: 210 s
 Probe-interval: 5 s
 Register-header-checksum: disabled
 Register-policy: disabled
 Register-suppression-timeout: 60 s
 Source-lifetime: 210 s
 Source-policy: disabled
 Spt-switch-threshold: disabled
 Ssm-policy: disabled
 Static-rp:  disabled
 Hello periodic interval: 30 s
 Join-prune periodic interval: 60 s
 Timer spt-switch: 15 s

 Interface View Default Configurations:
 --------------------------------------
 Pim bfd: disabled
 Pim bsr-boundary: disabled
 Pim hello-option dr-priority: 1
 Pim hello-option holdtime: 105 s
 Pim hello-option lan-delay: 500 ms
 Pim hello-option neighbor-tracking: disabled
 Pim hello-option override-interval: 2500 ms
 Pim holdtime assert: 180 s
 Pim holdtime join-prune: 210 s
 Pim require-genid: disabled
 Pim silent: disabled
 Pim timer dr-switch-delay: disabled
 Pim hello periodic interval: 30 s
 Pim join-prune periodic interval: 60 s
 Pim triggered-hello-delay: 5 s
 Pim version: 2
 Pim ipsec sa: disabled
 Pim join-policy: disabled
 Pim neighbor-policy: disabled
```

Table 8-37 Description of the **display default-parameter pim-sm** command output

Item	Description
PIM View Default Configurations	Default configurations in the PIM view.

Item	Description
Auto-rp listening enable	Whether the auto-RP listening function is enabled. The switch does not support this function.
Bsr-policy	Whether the valid address range of the BSR is set. This parameter is configured by the **bsr-policy (IPv4)** command.
C-bsr admin-scope	Whether the BSR administrative domain is configured. This parameter is configured by the **c-bsr admin-scope** command.
C-bsr global	Whether the C-BSR in the global domain is configured. This parameter is configured by the **c-bsr global** command.
C-bsr group	Whether the C-BSR in the BSR administrative domain is configured. This parameter is configured by the **c-bsr group** command.
C-bsr hash-length	Global hash mask length of the C-BSR. This parameter is configured by the **c-bsr hash-length (IPv4)** command.
C-bsr holdtime	Waiting time for the BSR to receive the Bootstrap message. This parameter is configured by the **c-bsr holdtime (IPv4)** command.
C-bsr interval	Interval for the BSR to send Bootstrap messages. This parameter is configured by the **c-bsr interval (IPv4)** command.
C-bsr priority	Global priority of the C-BSR. This parameter is configured by the **c-bsr priority (IPv4)** command.
C-rp advertisement-interval	Interval for the C-RP to send Advertisement messages. This parameter is configured by the **c-rp advertisement-interval (IPv4)** command.
C-rp holdtime	Waiting time for the BSR to receive the Advertisement message. This parameter is configured by the **c-rp holdtime (IPv4)** command.
C-rp priority	Global priority of the C-RP. This parameter is configured by the **c-rp priority (IPv4)** command.

Item	Description
Crp-policy	Whether the valid address range of the C-RP and the range of multicast groups that the C-RP serves are set. This parameter is configured by the **crp-policy (IPv4)** command.
Bsm semantic fragmentation	Whether the BSR fragmentation is enabled. This parameter is configured by the **bsm semantic fragmentation (IPv4)** command.
Hello-option dr-priority	Priority for DR election. This parameter is configured by the **hello-option dr-priority (IPv4)** command.
Hello-option holdtime	Time period for the neighbor to hold the reachable state, in seconds. This parameter is configured by the **hello-option holdtime (IPv4)** command.
Hello-option lan-delay	Delay in transmitting Prune messages at a shared network segment, in milliseconds. This parameter is configured by the **hello-option lan-delay (IPv4)** command.
Hello-option neighbor-tracking	Whether neighbor tracking is enabled. This parameter is configured by the **hello-option neighbor-tracking (IPv4)** command.
Hello-option override-interval	Interval for sending Prune Override messages, in milliseconds. This parameter is configured by the **hello-option override-interval (IPv4)** command.
Holdtime assert	Time period for holding the Assert state, in seconds. This parameter is configured by the **holdtime assert (IPv4)** command.
Holdtime join-prune	Time period for holding the Join or Prune state, in seconds. This parameter is configured by the **holdtime join-prune (IPv4)** command.
Probe-interval	Interval for sending Probe messages (empty Register messages) to the RP, in seconds. This parameter is configured by the **probe-interval (IPv4)** command.
Register-header-checksum	Whether calculating the checksum based on information in Register message header is required. This parameter is configured by the **register-header-checksum** command.

Item	Description
Register-policy	Whether the rule for filtering Register messages is configured. This parameter is configured by the **register-policy (IPv4)** command.
Register-suppression-timeout	Time period for holding the register-suppression state, in seconds. This parameter is configured by the **register-suppression-timeout (IPv4)** command.
Source-lifetime	Timeout period of an (S, G) entry, in seconds. This parameter is configured by the **source-lifetime (IPv4)** command.
Source-policy	Whether the rule for filtering multicast sources is configured. This parameter is configured by the **source-policy (IPv4)** command.
Spt-switch-threshold	Whether the threshold of the multicast packet rate that triggers the switch from the RPT to the SPT is configured. This parameter is configured by the **spt-switch-threshold (IPv4)** command.
Ssm-policy	Whether the SSM group address range is set. This parameter is configured by the **ssm-policy (IPv4)** command.
Static-rp	Whether the static RP is configured. This parameter is configured by the **static-rp (IPv4)** command.
Hello periodic interval	Interval for sending Hello messages, in seconds. This parameter is configured by the **timer hello (IPv4)** command.
Join-prune periodic interval	Interval for sending Join/Prune messages, in seconds. This parameter is configured by the **timer join-prune (IPv4)** command.
Timer spt-switch	Whether the interval for checking whether the multicast packet rate exceeds the threshold before the switchover from RPT to SPT is configured, in seconds. This parameter is configured by the **timer spt-switch (IPv4)** command.
Interface View Default Configurations	Default configurations in the interface view.
Pim bfd	Whether PIM BFD is enabled on the interface. This parameter is configured by the **pim bfd enable** command.

Item	Description
Pim bsr-boundary	Whether the PIM boundary is configured on the interface. This parameter is configured by the **pim bsr-boundary** command.
Pim hello-option dr-priority	Priority for DR election on the interface. This parameter is configured by the **pim hello-option dr-priority** command.
Pim hello-option holdtime	Time period for the neighbor on the interface to hold the reachable state, in seconds. This parameter is configured by the **pim hello-option holdtime** command.
Pim hello-option lan-delay	Delay in transmitting Prune messages at a shared network segment on the interface, in milliseconds. This parameter is configured by the **pim hello-option lan-delay** command.
Pim hello-option neighbor-tracking	Whether neighbor tracking is enabled on the interface. This parameter is configured by the **pim hello-option neighbor-tracking** command.
Pim hello-option override-interval	Interval for the interface to send Prune Override messages, in milliseconds. This parameter is configured by the **pim hello-option override-interval** command.
Pim holdtime assert	Time period for the interface to hold the Assert state, in seconds. This parameter is configured by the **pim holdtime assert** command.
Pim holdtime join-prune	Time period for the interface to hold the Join or Prune state, in seconds. This parameter is configured by the **pim holdtime join-prune** command.
Pim require-genid	Whether the received Hello message is required to carry the Generation ID. This parameter is configured by the **pim require-genid** command.
Pim silent	Whether PIM Silent is enabled on the interface. This parameter is configured by the **pim silent** command.
Pim timer dr-switch-delay	Whether the DR switch delay is set on the interface. This parameter is configured by the **pim timer dr-switch-delay** command.

Item	Description
Pim hello periodic interval	Interval for the interface to send Hello messages, in seconds. This parameter is configured by the **pim timer hello** command.
Pim join-prune periodic interval	Interval for the interface to send Join/Prune messages, in seconds. This parameter is configured by the **pim timer join-prune** command.
Pim triggered-hello-delay	Maximum delay for the interface to send Hello messages, in seconds. This parameter is configured by the **pim triggered-hello-delay** command.
Pim version	Version of PIM enabled on the interface.
Pim ipsec sa	Whether PIM IPSec is enabled on the interface. This parameter is configured by the **pim ipsec sa** command.
Pim join-policy	Whether the join-policy is configured on the interface. This parameter is configured by the **pim join-policy** command.
Pim neighbor-policy	Whether the neighbor-policy is configured on the interface. This parameter is configured by the **pim neighbor-policy** command.

8.3.19 display default-parameter pim-ssm

Function

The **display default-parameter pim-ssm** command displays default configurations of PIM-SM for SSM.

Format

display default-parameter pim-ssm

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The **display default-parameter pim-ssm** command displays default configuration of PIM-SM for SSM. Even if the configuration of PIM-SM for SSM is modified, the **display default-parameter pim-ssm** command still displays default parameter settings. Therefore, you can use this command to check which parameters on the device have been modified.

Example

Display default configuration of PIM-SM for SSM.

```
<HUAWEI> display default-parameter pim-ssm
 PIM View Default Configurations:
 --------------------------------
 Hello-option dr-priority: 1
 Hello-option holdtime: 105 s
 Hello-option lan-delay: 500 ms
 Hello-option neighbor-tracking: disabled
 Hello-option override-interval: 2500 ms
 Holdtime assert: 180 s
 Holdtime join-prune: 210 s
 Probe-interval: 5 s
 Register-header-checksum: disabled
 Register-policy: disabled
 Register-suppression-timeout: 60 s
 Source-lifetime: 210 s
 Source-policy: disabled
 Ssm-policy: disabled
 Hello periodic interval: 30 s
 Join-prune periodic interval: 60 s

 Interface View Default Configurations:
 --------------------------------------
 Pim bfd: disabled
 Pim hello-option dr-priority: 1
 Pim hello-option holdtime: 105 s
 Pim hello-option lan-delay: 500 ms
 Pim hello-option neighbor-tracking: disabled
 Pim hello-option override-interval: 2500 ms
 Pim holdtime assert: 180 s
 Pim holdtime join-prune: 210 s
 Pim require-genid: disabled
 Pim silent: disabled
 Pim timer dr-switch-delay: disabled
 Pim hello periodic interval: 30 s
 Pim join-prune periodic interval: 60 s
 Pim triggered-hello-delay: 5 s
 Pim version: 2
 Pim ipsec sa: disabled
 Pim join-policy: disabled
 Pim neighbor-policy: disabled
```

Table 8-38 Description of the **display default-parameter pim-ssm** command output

Item	Description
PIM View Default Configurations	Default configurations in the PIM view.

Item	Description
Hello-option dr-priority	Priority for DR election. This parameter is configured by the **hello-option dr-priority (IPv4)** command.
Hello-option holdtime	Time period for the neighbor to hold the reachable state, in seconds. This parameter is configured by the **hello-option holdtime (IPv4)** command.
Hello-option lan-delay	Delay in transmitting Prune messages at a shared network segment, in milliseconds. This parameter is configured by the **hello-option lan-delay (IPv4)** command.
Hello-option neighbor-tracking	Whether neighbor tracking is enabled. This parameter is configured by the **hello-option neighbor-tracking (IPv4)** command.
Hello-option override-interval	Interval for sending Prune Override messages, in milliseconds. This parameter is configured by the **hello-option override-interval (IPv4)** command.
Holdtime assert	Time period for holding the Assert state, in seconds. This parameter is configured by the **holdtime assert (IPv4)** command.
Holdtime join-prune	Time period for holding the Join or Prune state, in seconds. This parameter is configured by the **holdtime join-prune (IPv4)** command.
Probe-interval	Interval for sending Probe messages (empty Register messages) to the RP, in seconds. This parameter is configured by the **probe-interval (IPv4)** command.
Register-header-checksum	Whether calculating the checksum based on information in Register message header is required. This parameter is configured by the **register-header-checksum** command.
Register-policy	Whether the rule for filtering Register messages is configured. This parameter is configured by the **register-policy (IPv4)** command.
Register-suppression-timeout	Time period for holding the register-suppression state, in seconds. This parameter is configured by the **register-suppression-timeout (IPv4)** command.

Item	Description
Source-lifetime	Timeout period of an (S, G) entry, in seconds. This parameter is configured by the **source-lifetime (IPv4)** command.
Source-policy	Whether the rule for filtering multicast sources is configured. This parameter is configured by the **source-policy (IPv4)** command.
Ssm-policy	Whether the SSM group address range is set. This parameter is configured by the **ssm-policy (IPv4)** command.
Hello periodic interval	Interval for sending Hello messages, in seconds. This parameter is configured by the **timer hello (IPv4)** command.
Join-prune periodic interval	Interval for sending Join/Prune messages, in seconds. This parameter is configured by the **timer join-prune (IPv4)** command.
Interface View Default Configurations	Default configurations in the interface view.
Pim bfd	Whether PIM BFD is enabled on the interface. This parameter is configured by the **pim bfd enable** command.
Pim hello-option dr-priority	Priority for DR election on the interface. This parameter is configured by the **pim hello-option dr-priority** command.
Pim hello-option holdtime	Time period for the neighbor on the interface to hold the reachable state, in seconds. This parameter is configured by the **pim hello-option holdtime** command.
Pim hello-option lan-delay	Delay in transmitting Prune messages at a shared network segment on the interface, in milliseconds. This parameter is configured by the **pim hello-option lan-delay** command.
Pim hello-option neighbor-tracking	Whether neighbor tracking is enabled on the interface. This parameter is configured by the **pim hello-option neighbor-tracking** command.
Pim hello-option override-interval	Interval for the interface to send Prune Override messages, in milliseconds. This parameter is configured by the **pim hello-option override-interval** command.

Item	Description
Pim holdtime assert	Time period for the interface to hold the Assert state, in seconds. This parameter is configured by the **pim holdtime assert** command.
Pim holdtime join-prune	Time period for the interface to hold the Join or Prune state, in seconds. This parameter is configured by the **pim holdtime join-prune** command.
Pim require-genid	Whether the received Hello message is required to carry the Generation ID. This parameter is configured by the **pim require-genid** command.
Pim silent	Whether PIM Silent is enabled on the interface. This parameter is configured by the **pim silent** command.
Pim timer dr-switch-delay	Whether the DR switch delay is set on the interface. This parameter is configured by the **pim timer dr-switch-delay** command.
Pim hello periodic interval	Interval for the interface to send Hello messages, in seconds. This parameter is configured by the **pim timer hello** command.
Pim join-prune periodic interval	Interval for the interface to send Join/Prune messages, in seconds. This parameter is configured by the **pim timer join-prune** command.
Pim triggered-hello-delay	Maximum delay for the interface to send Hello messages, in seconds. This parameter is configured by the **pim triggered-hello-delay** command.
Pim version	Version of PIM enabled on the interface.
Pim ipsec sa	Whether PIM IPSec is enabled on the interface. This parameter is configured by the **pim ipsec sa** command.
Pim join-policy	Whether the join-policy is configured on the interface. This parameter is configured by the **pim join-policy** command.
Pim neighbor-policy	Whether the neighbor-policy is configured on the interface. This parameter is configured by the **pim neighbor-policy** command.

8.3.20 display pim bfd session

Function

The **display pim bfd session** command displays the information about PIM BFD sessions.

NOTE

Only the S5720I-SI, S5735-S, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6720S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Format

display pim [**vpn-instance** *vpn-instance-name* | **all-instance**] **bfd session statistics**

display pim [**vpn-instance** *vpn-instance-name* | **all-instance**] **bfd session** [**interface** *interface-type interface-number* | **neighbor** *neighbor-address*] *

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Specifies a VPN instance. The *vpn-instance-name* specifies the name of the VPN instance.	The value must be an existing VPN instance name.
all-instance	Indicates all the instances.	-
statistics	Displays PIM BFD statistics.	-
interface *interface-type interface-number*	Specifies an interface to be displayed. *interface-type interface-number* specifies the type and number of the interface.	-
neighbor *neighbor-address*	Specifies the IP address of a PIM neighbor to be displayed.	The address is in dotted decimal notation.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The **display pim bfd session** command output helps you locate communication faults between neighbors.

Example

Display PIM BFD sessions on VLANIF 10.

```
<HUAWEI> display pim bfd session interface vlanif 10
 VPN-Instance: public net

 Vlanif10 (10.1.2.2): Total 2 BFD sessions Created

 Neighbor     ActTx(ms)     ActRx(ms)     ActMulti     Local/Remote     State
 10.1.2.3     20            20            5            8756/8652        Up
 10.1.2.4     30            10            3            8754/8423        Up
```

Display PIM BFD sessions on VLANIF 10 when the switch is not enabled with global BFD.

```
<HUAWEI> display pim bfd session interface vlanif 10
 VPN-Instance: public net

 Vlanif10 (10.1.2.2): Total 1 BFD session Created

 Neighbor    ActTx(ms)    ActRx(ms)    ActMulti    Local/Remote          State
 10.1.2.1    --           --           --          0/0                   BFD global disable
```

Display the statistics of a PIM BFD session.

```
<HUAWEI> display pim bfd session statistics
 VPN-Instance: public net
  Total 1 PIM BFD session in this instance.

   Total 1 PIM BFD session up.
   Total 0 PIM BFD session down.
```

Display information about PIM BFD sessions of the neighbor 10.1.2.3.

```
<HUAWEI> display pim bfd session neighbor 10.1.2.3
VPN-Instance: public net
  Vlanif10 (10.1.2.2)
 Neighbor     ActTx(ms)     ActRx(ms)     ActMulti     Local/Remote     State
 10.1.2.3     20            20            5            8756/8652        Up
```

Table 8-39 Description of the **display pim bfd session** command output

Item	Description
Vlanif10 (10.1.2.2)	PIM interface name (the IP address).
Neighbor	IP address of a PIM neighbor.
ActTx (ms)	Actual minimum transmission interval, in milliseconds.
ActRx (ms)	Actual minimum receiving interval, in milliseconds.
ActMulti	Actual local detection multiple.
Local/Remote	Local and remote discriminators.

Item	Description
State	Status of the PIM BFD session. • Up: indicates that the BFD session is set up successfully and detection packets are periodically exchanged. • Init: indicates that the local end can communicate with the remote end and wants the session status to be Up. • BFD global disable: indicates that BFD is globally disabled. • Detect down: indicates that no BFD packets are not received when the detection time expires. • Neighbour down: indicates that the packets with the State field being Down are received from neighbors.
Total 1 PIM BFD session in this instance	Total number of PIM BFD sessions in a public network instance or a VPN instance.
Total 1 PIM BFD session up	Number of PIM BFD sessions in the Up state in a public network instance or a VPN instance.
Total 0 PIM BFD session down	Number of PIM BFD sessions in the Down state in a public network instance or a VPN instance, that is, all PIM BFD sessions except the PIM BFD sessions in the Up state.

8.3.21 display pim bsr-info

Function

The **display pim bsr-info** command displays the BSRs in a PIM-SM domain.

Format

display pim [**vpn-instance** *vpn-instance-name* | **all-instance**] **bsr-info**

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Specifies a VPN instance. *vpn-instance-name* specifies the name of the VPN instance.	The value must be an existing VPN instance name.
all-instance	Indicates all the instances.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

This command applies to the PIM-SM domain where the RP is dynamically elected among BSRs. You can run this command on any switch in the domain to view the BSR information.

- If the current switch is configured with the C-BSR, the command output includes information about the elected BSR and locally configured C-BSR.
- If the current switch is not configured with the C-BSR, the command output includes information about the elected BSR only.

Precautions

When the **display pim bsr-info** command is used, only information about the public network instance is displayed if the **vpn-instance** or **all-instance** is not specified.

This command has output only after C-BSRs have been configured in a PIM-SM domain.

Example

Display information about the BSR in the PIM-SM domain. If the switch is not configured with C-BSR, only information about the elected BSR is displayed.

```
<HUAWEI> display pim bsr-info
 VPN-Instance: public net
 Elected AdminScoped BSR Count: 0
 Elected BSR Address: 10.1.2.2
     Priority: 0
     Hash mask length: 30
     State: Accept Preferred
     Scope: Not scoped
     Uptime: 00:01:46
     Expires: 00:02:02
     C-RP Count: 1
```

Display information about BSR in the current PIM-SM.

If the switch is configured with C-BSR, information about the elected BSR and C-BSR is displayed.

```
<HUAWEI> display pim bsr-info
 VPN-Instance: public net
 Elected AdminScoped BSR Count: 0
 Elected BSR Address: 10.1.2.2
     Priority: 0
     Hash mask length: 30
     State: Elected
     Scope: Not scoped
     Uptime: 00:10:42
     Next BSR message scheduled at: 00:00:31
     C-RP Count: 1
 Candidate AdminScoped BSR Count: 0
 Candidate BSR Address: 10.1.2.2
     Priority: 0
```



```
Hash mask length: 30
State: Elected
Scope: Not scoped
Wait to be BSR: 0
```

Table 8-40 Description of the **display pim bsr-info** command output

Item	Description
Elected AdminScoped BSR Count	Number of elected AdminScoped BSRs.
Elected BSR Address	Address of the elected BSR.
Priority	Priority of the BSR. By default, the value is 0.
Hash mask length	Mask length in the RP hash calculation.
State	Status of the BSR.
Scope	Range of multicast addresses in the administrative scope when the BSR is an AdminScoped BSR. Not scoped indicates that the BSR is not an AdminScoped BSR.
Uptime	Period during which the BSR exists. The time format is as follows: • If the time is shorter than or equal to 24 hours, the format is hours:minutes:seconds. • If the time is longer than 24 hours but shorter than or equal to one week, the format is days:hours. • If the time is longer than one week, the format is weeks:days.
Expires	Remaining time of the BSR. The time format is as follows: • If the time is shorter than or equal to 24 hours, the format is hours:minutes:seconds. • If the time is longer than 24 hours but shorter than or equal to one week, the format is days:hours. • If the time is longer than one week, the format is weeks:days.
C-RP Count	Number of RPs learned through the BSR.
Next BSR message scheduled at	Period after which the next BSR message is sent. BSR messages are sent only when the timer maintained by the elected BSR times out.

Item	Description
Candidate AdminScoped BSR Count	Number of AdminScoped C-BSRs.
Candidate BSR Address	Address of the C-BSR.
Wait to be BSR	Whether the current C-BSR is valid. The values are as follows: • 0: indicates that the current C-BSR is valid. The current C-BSR takes part in the BSR election. • 1: indicates that the current C-BSR is invalid. The current C-BSR does not take part in the BSR election. When the number of C-BSRs configured on the switch exceeds the threshold, the value is 1.

8.3.22 display pim claimed-route

Function

The **display pim claimed-route** command displays the unicast routing information used by PIM.

Format

display pim [**vpn-instance** *vpn-instance-name* | **all-instance**] **claimed-route** [*source-address*]

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Specifies a VPN instance. *vpn-instance-name* specifies the name of the VPN instance.	The value must be an existing VPN instance name.
all-instance	Indicates all the instances.	-
source-address	Specifies the multicast source address.	The address is in decimal notation.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

The **display pim claimed-route** command is used to view information about unicast routes used by PIM, including RPF neighbors, interfaces, route types, and route selection policies.

Configuration Impact

Differences between the **display pim claimed-route** and **display multicast rpf-info** commands are as follows:

- The **display multicast rpf-info** command is used to check information about RPF neighbors, RPF interfaces, or whether there is a route to a specified source address.
- The **display pim claimed-route** command is used to check information about unicast routes used by multicast routing and entries of these routes.

Example

Display the unicast routing information used by PIM.

```
<HUAWEI> display pim claimed-route
 VPN-Instance: public net
 multicast load-splitting rule: source-group
 RPF information about: 10.1.0.0 in PIM-SM routing table
     RPF interface: Vlanif10, RPF neighbor: 10.1.2.2
     Referenced route/mask: 10.1.0.0/24
     Referenced route type: igp
     RPF-route selecting rule: preference-preferred
     The (S, G) or (*, G) list dependent on this route entry
     (10.1.0.1, 225.0.0.1)
```

Table 8-41 Description of the **display pim claimed-route** command output

Item	Description
multicast load-splitting rule	How multi-cast loads are split. The following policies apply: • group: multicast group-based load splitting • source: multicast source-based load splitting • source-group: multicast source and group-based load splitting • stable-preferred: stable-preferred load splitting • balance-preferred: balance-preferred load splitting This parameter is configured by the **multicast load-splitting** command.

Item	Description
RPF information about: 10.1.0.0 in PIM-SM routing table	RPF routing information with the source address of 10.1.0.0 in the PIM-SM routing table
RPF interface	RPF interface on the switch.
RPF neighbor	RPF neighbor of the switch.
Referenced route/mask	Destination address/mask of the referenced route.
Referenced route type	Type of the route.
RPF-route selecting rule	Preferred rule for selecting the RPF-route.
The (S,G) or (*,G) list dependent on this route entry	List of multicast entries based on RPF routes.

8.3.23 display pim control-message counters

Function

The **display pim control-message counters** command displays the number of sent, received, and invalid PIM control messages.

Format

display pim [**vpn-instance** *vpn-instance-name* | **all-instance**] **control-message counters message-type** { **probe** | **register** | **register-stop** | **crp** }

display pim [**vpn-instance** *vpn-instance-name* | **all-instance**] **control-message counters** [**message-type** { **assert** | **graft** | **graft-ack** | **hello** | **join-prune** | **state-refresh** | **bsr** } | **interface** *interface-type interface-number*] *

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Specifies the name of a VPN instance.	The value must be an existing VPN instance name.
all-instance	Indicates all the instances.	-
message-type	Indicates a PIM control message type.	-
probe	Indicates the Probe message.	-
register	Indicates the Register message.	-

Parameter	Description	Value
register-stop	Indicates the Register-stop message.	-
crp	Indicates the C-RP message.	-
assert	Indicates the Assert message.	-
graft	Indicates the Graft message.	-
graft-ack	Indicates the Graft-ack message.	-
hello	Indicates the Hello message.	-
join-prune	Indicates the Join/Prune message.	-
state-refresh	Indicates the State-Refresh message.	-
bsr	Indicates the BSR message.	-
interface *interface-type interface-number*	Indicates the type and number of an interface.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

When multicast data messages cannot be forwarded on a PIM network, run the **display pim control-message counters** command to view statistics on protocol messages. The command output helps you locate faults.

When you run the **display pim control-message counters** command:

- If you specify **interface** *interface-type interface-number*, you can view the number of various PIM control messages that were sent and received on the specified interface only.
- If you specify **message-type**, you can view the number of PIM control messages of this type sent and received on all interfaces of the switch.

Example

Display the statistics about sent, received, and invalid PIM control messages on the device.

```
<HUAWEI> display pim control-message counters
 VPN-Instance: public net
 PIM global control-message counters:
 Message Type     Received        Sent          Invalid         Filtered
 Register         51              0             0               0
 Register-Stop    0               48            0               0
 Probe            44              0             0               0
 C-RP             0               0             0               0

 PIM control-message counters for interface: Vlanif10
```



```
Message Type     Received        Sent            Invalid         Filtered
Assert           0               6               0               0
Graft            0               0               0               0
Graft-Ack        0               0               0               0
Hello            34496           34495           0               0
Join-prune       26171           90              0               0
State-Refresh    0               0               0               0
BSR              0               0               0               0

PIM control-message counters for interface: Vlanif20
Message Type     Received        Sent            Invalid         Filtered
Assert           0               0               0               0
Graft            0               0               0               0
Graft-Ack        0               0               0               0
Hello            34491           34495           0               0
Join-prune       0               41              0               0
State-Refresh    0               0               0               0
BSR              0               0               0               0
```

Display the statistics about sent, received, invalid PIM control messages on VLANIF 10.

```
<HUAWEI> display pim control-message counters interface Vlanif 10
 VPN-Instance: public net
 PIM control-message counters for interface: Vlanif 10
 Message Type     Received        Sent            Invalid     Filtered
 Assert           0               0               0           0
 Graft            0               0               0           0
 Graft-Ack        0               0               0           0
 Hello            328             331             0           0
 Join-prune       2               0               0           0
 State-Refresh    0               0               0           0
 BSR              0               0               0           0
```

Table 8-42 Description of the **display pim control-message counters** command output

Item	Description
PIM global control-message counters	Number of PIM control messages in the public network.
PIM control-message counters for interface	Name of the interface where statistics about PIM control messages are collected.
Message Type	Type of the control messages.
Received	Number of control messages received by the interface.
Sent	Number of control messages sent by the interface.
Invalid	Number of invalid control messages.
Filtered	Number of control messages filtered out by the interface.
Register	Number of Register messages.
Register-Stop	Number of Register-Stop messages.
Probe	Number of Probe messages.

Item	Description
C-RP	Number of CRP messages.
Assert	Number of Assert messages.
Graft	Number of Graft messages.
Graft-Ack	Number of Graft-Ack messages.
Hello	Number of Hello messages.
Join-prune	Number of Join/Prune messages.
State-Refresh	Number of State-Refresh messages.
BSR	Number of Bootstrap messages.

8.3.24 display pim grafts

Function

The **display pim grafts** command displays the information about unacknowledged PIM-DM Graft messages.

Format

display pim [**vpn-instance** *vpn-instance-name* | **all-instance**] **grafts**

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Specifies a VPN instance. *vpn-instance-name* specifies the name of the VPN instance.	The value must be an existing VPN instance name.
all-instance	Specifies all the instances.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

In PIM-DM, after sending the Graft message, the switch needs to wait to receive the Graft-Ack message from the upstream device. You can run the **display pim grafts** command to view the information about the PIM-DM Graft messages sent but unacknowledged.

Example

Display the unacknowledged PIM-DM graft messages on the switch.

```
<HUAWEI> display pim grafts
VPN-Instance: public net
Source                Group               Expire    RetransmitIn
10.0.5.200            226.3.3.3           00:02:52  00:00:02
```

Table 8-43 Description of the **display pim grafts** command output

Item	Description
Source	Multicast source address.
Group	Multicast group address.
Expire	Timeout period of an (S, G) entry.
RetransmitIn	Amount of time before the next retransmission of the Graft message.

8.3.25 display pim interface

Function

The **display pim interface** command displays PIM information on an interface.

Format

display pim [**vpn-instance** *vpn-instance-name* | **all-instance**] **interface** [*interface-type interface-number* | **up** | **down**] [**verbose**]

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Specifies the name of a VPN instance.	The value must be an existing VPN instance name.
all-instance	Specifies all the instances.	-
interface-type interface-number	Specifies the type and number of an interface.	-
up	Displays PIM information on interfaces in Up state.	-
down	Displays PIM information on interfaces in Down state.	-

Parameter	Description	Value
verbose	Displays detailed information about a PIM interface.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

An interface with PIM enabled is called a PIM interface. The **display pim interface** command is used to display information about PIM interfaces, including the PIM state, number of PIM neighbors, interval at which Hello messages are sent, DR priority, and DR address.

When the **display pim interface** command is used:

- If *interface-type interface-number* is specified, the command displays various PIM state parameters on the specified interface.
- If *interface-type interface-number* is not specified, the command displays state parameters of all the PIM interfaces.
- If **up** is specified in the command, the command displays parameters of the PIM interfaces in the Up stated.
- If **down** is specified in the command, the command displays parameters of the PIM interfaces in the Down state.

Example

Display information about all the PIM interfaces.

```
<HUAWEI> display pim interface
 VPN-Instance: public net
 Interface      State  NbrCnt  HelloInt  DR-Pri     DR-Address
 Loop0          up     0       30        1          10.1.0.2    (local)
 Vlanif10       up     1       30        1          10.1.1.2
 Vlanif20       up     0       30        1          10.1.2.2    (local)
 Vlanif30       up     1       30        1          10.1.3.2
```

Table 8-44 Description of the **display pim interface** command output

Item	Description
Interface	Name of the PIM interface.
State	Status of the PIM interface, Up or Down.
NbrCnt	Number of PIM neighbors on the interface.

Item	Description
HelloInt	Interval for sending Hello messages, in seconds.
DR-Pri	DR priority.
DR-Address	DR address.

Display detailed information about PIM on VLANIF10.

```
<HUAWEI> display pim interface vlanif 10 verbose
 VPN-Instance: public net
 Interface: Vlanif10, 10.1.1.1
    PIM version: 2
    PIM mode: Sparse
    PIM state: up
    PIM DR: 10.1.1.2
    PIM DR Priority (configured): 1
    PIM neighbor count: 1
    PIM hello interval: 30 s
    PIM LAN delay (negotiated): 500 ms
    PIM LAN delay (configured): 500 ms
    PIM hello override interval (negotiated): 2500 ms
    PIM hello override interval (configured): 2500 ms
    PIM Silent: disabled
    PIM neighbor tracking (negotiated): disabled
    PIM neighbor tracking (configured): disabled
    PIM generation ID: 0XF5712241
    PIM require-GenID: disabled
    PIM hello hold interval: 105 s
    PIM assert hold interval: 180 s
    PIM triggered hello delay: 5 s
    PIM J/P interval: 60 s
    PIM J/P hold interval: 210 s
    PIM BSR domain border: disabled
    PIM BFD: enabled
    PIM dr-switch-delay timer : 20 s
    Number of routers on link not using DR priority: 0
    Number of routers on link not using LAN delay: 0
    Number of routers on link not using neighbor tracking: 2
    ACL of PIM neighbor policy: myacl
    ACL of PIM ASM join policy: 2000
    ACL of PIM SSM join policy: -
    ACL of PIM join policy: -
    PIM ipsec: disabled
```

Table 8-45 Description of the **display pim interface verbose** command output

Item	Description
Interface	Name and IP address of the PIM interface.
PIM version	PIM version enabled on the interface.
PIM mode	PIM mode used on the interface.
PIM state	Status of the PIM interface, Up or Down.
PIM DR	DR address on the interface.

Item	Description
PIM DR Priority (configured)	DR priority configured on the interface.
PIM neighbor count	Number of PIM neighbors on the interface.
PIM hello interval	Interval for sending PIM Hello messages, in seconds.
PIM LAN delay (negotiated)	Negotiated delay for transmitting packets on the interface, in milliseconds.
PIM LAN delay (configured)	Configured delay for transmitting packets on the interface, in milliseconds.
PIM hello override interval (negotiated)	Negotiated override interval on the interface, in milliseconds.
PIM hello override interval (configured)	Configured override interval on the interface, in milliseconds.
PIM Silent	Whether the interface is set to PIM silent state. • enabled: The interface is in the PIM silent state. • disabled: The interface is not in the PIM silent state. This function is configured using the **pim silent** command.
PIM neighbor tracking (negotiated)	Whether PIM neighbor tracking is enabled on the interface after negotiation. • enabled: PIM neighbor tracking is enabled on the interface. • disabled: PIM neighbor tracking is disabled on the interface.
PIM neighbor tracking (configured)	Whether PIM neighbor tracking is configured on the interface. • enabled: PIM neighbor tracking is configured on the interface. • disabled: PIM neighbor tracking is not configured on the interface. This function is configured using the **pim hello-option neighbor-tracking** command.
PIM generation ID	Generation ID option on the interface.

Item	Description
PIM require-GenID	Whether the switch is enabled to reject Hello messages not carrying the Generation ID. • enabled: The switch is enabled to reject Hello messages not carrying the Generation ID. • disabled: The switch is disabled from rejecting Hello messages not carrying the Generation ID. This function is configured using the **pim require-genid** command.
PIM hello hold interval	Interval during which the receiver of the Hello message to keep its neighbor reachable, in seconds.
PIM assert hold interval	Interval for sending Assert messages, in seconds.
PIM triggered hello delay	Maximum random delay for triggering Hello messages, in seconds.
PIM J/P interval	Interval at which the interface sends Join/Prune messages, in seconds.
PIM J/P hold interval	Period for holding the Join/Prune status on the interface, in seconds.
PIM BSR domain border	Whether the BSR boundary is configured on the interface. • enabled: The BSR boundary is configured on the interface. • disabled: The BSR boundary is not configured on the interface. This function is configured using the **multicast boundary** command.
PIM BFD	Whether PIM BFD is enabled. • enabled: PIM BFD is enabled. • disabled: PIM BFD is disabled. This function is configured using the **pim bfd enable** command.
PIM BFD min-tx-interval	Minimum interval for sending PIM BFD packets. This parameter is configured using the **pim bfd min-tx-interval** *tx-value* command.

Item	Description
PIM BFD min-rx-interval	Minimum interval for receiving PIM BFD packets. This parameter is configured using the **pim bfd min-rx-interval** *rx-value* command.
PIM BFD detect-multiplier	PIM BFD detection multiplier. This parameter is configured using the **pim bfd detect-multiplier** *multiplier-value* command.
PIM dr-switch-delay timer	DR switching delay.
Number of routers on link not using DR priority	Number of switches that do not use DR priority in all the network segments connected to the interface.
Number of routers on link not using LAN delay	Number of switches that do not use LAN delay in all the network segments connected to the interface.
Number of routers on link not using neighbor tracking	Indicates the number of switches that are not enabled with the neighbor tracing function in the network segment where the interface resides.
ACL of PIM neighbor policy	Neighbor filtering policy configured on the interface.
ACL of PIM ASM join policy	ASM Join information filtering policy configured on the interface.
ACL of PIM SSM join policy	SSM Join information filtering policy configured on the interface.
ACL of PIM join policy	Join information filtering policy configured on the interface.

Item	Description
PIM ipsec	Whether PIM IPSec is configured in the PIM view or interface view, and the SA policy name if PIM IPSec is configured. The value can be: • PIM ipsec: enabled(sa-name: sa1) Security association sa1 has been configured to authenticate all PIM protocol packets using the **ipsec sa (IPv4)** command in the PIM view or the **pim ipsec sa** command in the interface view. If the SA is configured in the interface view, the configuration on the interface is displayed. Otherwise, the configuration in the PIM view is displayed. • PIM hello ipsec: enabled(sa-name: sa1) Security association sa1 has been configured to authenticate only PIM Hello packets using the **hello ipsec sa (IPv4)** command in the PIM view or the **pim hello ipsec sa** command in the interface view. If the SA is configured in the interface view, the configuration on the interface is displayed. Otherwise, the configuration in the PIM view is displayed. • PIM ipsec: disabled PIM IPSec is not configured in the PIM view or interface view.

8.3.26 display pim invalid-packet

Function

The **display pim invalid-packet** command displays statistics about invalid PIM messages received by a device and details of these messages.

Format

display pim [**vpn-instance** *vpn-instance-name* | **all-instance**] **invalid-packet** [**interface** *interface-type interface-number* | **message-type** { **assert** | **bsr** | **hello** | **join-prune** | **graft** | **graft-ack** | **state-refresh** }] *

display pim [**vpn-instance** *vpn-instance-name* | **all-instance**] **invalid-packet message-type** { **crp** | **register** | **register-stop** }

display pim invalid-packet [*packet-number*] **verbose**

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Displays statistics about invalid PIM messages received in a specified VPN instance. The *vpn-instance-name* parameter specifies the VPN instance name.	The value must be an existing VPN instance name.
all-instance	Displays statistics about invalid PIM messages received in all VPN instances.	-
interface *interface-type interface-number*	Specifies the type and number of an interface on the switch.	-
message-type	Displays statistics about invalid PIM messages of a specific type.	-
assert	Displays statistics about invalid Assert messages.	-
bsr	Displays statistics about invalid BSR messages.	-
hello	Displays statistics about invalid Hello messages.	-
join-prune	Displays statistics about invalid Join/Prune messages.	-
graft	Displays statistics about invalid Graft messages.	-
graft-ack	Displays statistics about invalid Graft-Ack messages.	-
state-refresh	Displays statistics about invalid State-Refresh messages.	-
crp	Displays statistics about invalid C-RP messages.	-
register	Displays statistics about invalid Register messages.	-

Parameter	Description	Value
register-stop	Displays statistics about invalid Register-Stop messages.	-
packet-number	Displays details about a specified number of invalid PIM messages recently received.	The value is an integer that ranges from 1 to 100. By default, details of all the invalid PIM messages currently stored are displayed.
verbose	Displays details of invalid PIM messages.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

If a switch fails to create PIM entries, you can run the **display pim invalid-packet** command first to check whether the switch has received invalid PIM messages. If the command output displays counters of invalid PIM messages, run the **display pim invalid-packet** [*packet-number*] **verbose** command to view details of invalid PIM messages for fault location.

You can run the following commands to view information about specific invalid PIM messages:

- Run the **display pim** [**vpn-instance** *vpn-instance-name* | **all-instance**] **invalid-packet** command to view statistics about invalid PIM messages received in a specified VPN instance or in all VPN instances.
- Run the **display pim invalid-packet interface** *interface-type interface-number* command to view statistics about invalid PIM messages received by a specified interface.
- Run the **display pim invalid-packet** *packet-number* **verbose** command to view details of invalid PIM messages recently received. Currently, details of a maximum of 100 invalid PIM messages can be displayed.

Example

Display statistics about invalid PIM messages received on the switch.

```
<HUAWEI> display pim invalid-packet

        Statistics of invalid packets for public net:
```



```
------------------------------------------------------------------------------
PIM General invalid packet:
Invalid PIM Version     : 0          Invalid PIM Type        : 0
Fault Length            : 0          Bad Checksum            : 0

PIM Register invalid packet:
Invalid Multicast Source: 0          Invalid Multicast Group : 0
Invalid Dest Addr       : 0

PIM Register-Stop invalid packet:
Invalid Multicast Source: 0          Invalid Multicast Group : 0
Invalid Dest Addr       : 0          IP Source not RP        : 0

PIM CRP invalid packet:
Invalid Dest Addr       : 0          Invalid CRP Addr        : 0
Fault Length            : 0          CRP Adv Fault Length    : 0
Invalid Multicast Group : 0

PIM Assert invalid packet:
Invalid Dest Addr       : 0          Invalid IP Source Addr  : 0
Invalid Multicast Source: 0          Invalid Multicast Group : 0

PIM BSR invalid packet:
Bad Payload             : 0          Fault Length            : 0
Bad Scope Mask          : 0          Invalid Multicast Group : 0
Not CBSR But BSR        : 0          Invalid BSR Addr        : 0
Fault Hash Length       : 0          Invalid IP Source Addr  : 0

PIM Hello invalid packet:
Invalid Addr List       : 0          Fault Length            : 0
Bad Holdtime Length     : 0          Bad LanPruneDelay Length: 0
Bad DrPriority Length   : 0          Bad GenID Length        : 0
Invalid Dest Addr       : 0          Invalid IP Source Addr  : 0

PIM Join/Prune invalid packet:
Invalid Multicast Source: 0          Invalid Multicast Group : 0
Invalid Up Neighbor     : 0          Invalid IP Source Addr  : 0
Invalid Dest Addr       : 0          Fault Length            : 0

PIM Graft invalid packet:
Invalid Multicast Source: 0          Invalid Multicast Group : 0
Invalid Up Neighbor     : 0          Invalid IP Source Addr  : 0
Fault Length            : 0

PIM Graft-Ack invalid packet:
Invalid Multicast Source: 0          Invalid Multicast Group : 0
Invalid Up Neighbor     : 0          Invalid IP Source Addr  : 0
Fault Length            : 0

PIM State Refresh invalid packet:
Invalid Multicast Source: 0          Invalid Multicast Group : 0
Invalid Originator Addr : 0          Fault Length            : 0
------------------------------------------------------------------------------
```

Table 8-46 Description of the **display pim invalid-packet** command output

Item	Description
PIM General invalid packet	General invalid PIM messages.
Invalid PIM Version	Number of messages with invalid PIM versions.
Invalid PIM Type	Number of messages with invalid PIM message types.

Item	Description
Fault Length	Number of messages of invalid lengths.
Bad Checksum	Number of messages with invalid checksum.
PIM Register invalid packet	Number of invalid PIM Register messages.
Invalid Multicast Source	Number of messages with invalid multicast source addresses.
Invalid Multicast Group	Number of messages with invalid multicast group addresses.
Invalid Dest Addr	Number of messages with invalid destination addresses.
PIM Register-Stop invalid packet	Number of invalid PIM Register-Stop messages.
IP Source not RP	Number of messages whose source addresses are not the RP address.
PIM CRP invalid packet	Number of invalid PIM C-RP messages.
Invalid CRP Addr	Number of messages with invalid C-RP addresses.
CRP Adv Fault Length	Number of messages whose CRP Adv fields are of invalid lengths.
PIM Assert invalid packet	Number of invalid PIM Assert messages.
Invalid IP Source Addr	Number of messages with invalid multicast source addresses.
PIM BSR invalid packet	Number of invalid PIM BSR messages.
Bad Payload	Number of messages with invalid payloads.
Bad Scope Mask	Number of messages with invalid scope masks.
Not CBSR But BSR	Number of BSR messages received on interfaces that do not act as a C-BSR.
Invalid BSR Addr	Number of messages with invalid BSR addresses.
Fault Hash Length	Number of messages with hash mask fields of invalid lengths.
PIM Hello invalid packet	Number of invalid PIM Hello messages.
Invalid Addr List	Number of messages with invalid address lists.
Bad Holdtime Length	Number of messages with Holdtime fields of invalid lengths.

Item	Description
Bad LanPruneDelay Length	Number of messages with LanPruneDelay fields of invalid lengths.
Bad DrPriority Length	Number of messages with DrPriority fields of invalid lengths.
Bad GenID Length	Number of messages with Generation ID fields of invalid lengths.
PIM Join/Prune invalid packet	Number of invalid PIM Join/Prune messages.
Invalid Up Neighbor	Number of messages with invalid upstream neighbors.
PIM Graft invalid packet	Number of invalid PIM Graft messages.
PIM Graft-Ack invalid packet	Number of invalid PIM Graft-Ack messages.
PIM State Refresh invalid packet	Number of invalid PIM State-Refresh messages.
Invalid Originator Addr	Number of messages with invalid Originator address.

Display details of one invalid PIM message recently received on the switch.

```
<HUAWEI> display pim invalid-packet 1 verbose
      Detailed information of invalid packets
-------------------------------------------------------
Packet information (Index 1):
-------------------------------------------------------
Interface          :  Vlanif10
Time               :  2010-6-1 20:04:35 UTC-08:00
Message Length     :  26
Invalid Type       :  Invalid Multicast Source
0000: 25 00 96 77 01 00 00 20 e1 01 01 01 01 00 e0 00
0010: 00 00 80 00 00 64 00 00 00 00
-------------------------------------------------------
```

Table 8-47 Description of the **display pim invalid-packet 1 verbose** command output

Item	Description
Detailed information of invalid packets	Details of an invalid PIM message.
Packet information (Index 1)	Sequence number of the invalid PIM message (numbered in the opposite order the message is received. For example, the index of the last received message is 1, the index of the penultimate message is 2, and so on).
Interface	Interface that received the invalid PIM message.

Item	Description
Time	Time when the invalid SPT switch message was received, in any of the following formats: ● YYYY-MM-DD HH:MM:SS ● YYYY-MM-DD HH:MM:SS UTC±HH:MM DST ● YYYY-MM-DD HH:MM:SS UTC±HH:MM ● YYYY-MM-DD HH:MM:SS DST The format UTC±HH:MM indicates that a time zone has been configured using the **clock timezone** command; DST indicates that the daylight saving time has been configured using **clock daylight-saving-time** command.
Message Length	Length of the invalid PIM message.
Invalid Type	Type of the invalid PIM message.
0000: 25 00 96 77 01 00 00 20 e1 01 01 01 01 00 e0 00 0010: 00 00 80 00 00 64 00 00 00 00	Contents of the invalid PIM message.

8.3.27 display pim neighbor

Function

The **display pim neighbor** command displays information about PIM neighbors.

Format

display pim [**vpn-instance** *vpn-instance-name* | **all-instance**] **neighbor** [*neighbor-address* | **interface** *interface-type interface-number* | **verbose**] *

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Specifies the name of a VPN instance.	The value must be an existing VPN instance name.
all-instance	Specifies all the instances.	-
interface *interface-type interface-number*	Specifies the type and number of an interface.	-

Parameter	Description	Value
neighbor-address	Specifies the IP address of a PIM neighbor.	The address is in dotted decimal notation.
verbose	Displays detailed information about PIM neighbors.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The **display pim neighbor** command displays information about PIM neighbors, including the number of neighbors, DR priority, and BFD session status. You can adjust PIM neighbor relationships based on the command output.

When you run the **display pim neighbor** command:

- If you specify **interface** *interface-type interface-number*, the command displays information about PIM neighbors connected to the specified interface.
- If you do not specify **interface** *interface-type interface-number*, the command displays information about all PIM neighbors attached to the switch.

Example

Display information about all PIM neighbors.

```
<HUAWEI> display pim neighbor
 VPN-Instance: public net
 Total Number of Neighbors = 2

 Neighbor        Interface     Uptime      Expires     Dr-Priority  BFD-Session
 10.1.1.2        Vlanif10      02:50:49    00:01:31    1            Y
 10.1.2.2        Vlanif20      02:49:39    00:01:42    1            Y
```

Table 8-48 Description of the **display pim neighbor** command output

Item	Description
Total Number of Neighbors	Total number of PIM neighbors on an interface.
Neighbor	IP Address of a PIM neighbor.
Interface	Interface connected to a PIM neighbor.
Uptime	Time elapsed since a PIM neighbor relationship is set up.

Item	Description
Expires	Amount of time left before a PIM relationship times out.
Dr-Priority	DR priority of a PIM neighbor.
BFD-Session	Whether the BFD session has been set up with a neighbor. ● Y: The BFD session has been set up. ● N: The BFD session has not been set up.

Display detailed information about the PIM neighbor with IP address 10.1.1.2 in the public network instance.

```
<HUAWEI> display pim neighbor 10.1.1.2 verbose
 VPN-Instance: public net
 Neighbor: 10.1.1.2
    Interface: Vlanif 10
    Uptime: 02:53:50
    Expiry time: 00:01:30
    DR Priority: 1
    Generation ID: 0X90B0360B
    Holdtime: 105 s
    LAN delay: 500 ms
    Override interval: 2500 ms
    Neighbor tracking: Disabled
    PIM BFD-Session: Y
    PIM BFD-Session min-tx-interval: 1000 ms
    PIM BFD-Session min-rx-interval: 1000 ms
    PIM BFD-Session detect-multiplier: 3
```

Table 8-49 Description of the **display pim neighbor verbose** command output

Item	Description
Expiry time	Amount of time left before a PIM relationship times out.
Generation ID	PIM neighbor status random value.
Holdtime	Keepalive period of the PIM neighbor.
LAN delay	Delay in transmitting Prune messages.
Override interval	Override interval for a prune action.
State refresh interval	Interval at which State-Refresh messages are sent.
Neighbor tracking	Whether the neighbor tracking function is enabled. ● enabled: Neighbor tracking is enabled. ● disabled: Neighbor tracking is disabled.

Item	Description
PIM BFD-Session	Whether the BFD session is set up. • Y: The BFD session has been set up. • N: The BFD session has not been set up.
PIM BFD-Session min-tx-interval	Minimum interval at which PIM BFD packets are sent.
PIM BFD-Session min-rx-interval	Minimum interval at which PIM BFD packets are received.
PIM BFD-Session detect-multiplier	PIM BFD detection multiplier.

8.3.28 display pim routing-table

Function

The **display pim routing-table** command displays the PIM routing table.

Format

display pim [**vpn-instance** *vpn-instance-name* | **all-instance**] **routing-table brief** [*group-address* [**mask** { *group-mask-length* | *group-mask* }] | *source-address* [**mask** { *source-mask-length* | *source-mask* }] | **incoming-interface** { *interface-type interface-number* | **register** }] *

display pim [**vpn-instance** *vpn-instance-name* | **all-instance**] **routing-table** [*group-address* [**mask** { *group-mask-length* | *group-mask* }] | *source-address* [**mask** { *source-mask-length* | *source-mask* }] | **incoming-interface** { *interface-type interface-number* | **register** } | **outgoing-interface** { **include** | **exclude** | **match** } { *interface-type interface-number* | **register** | **none** } | **mode** { **dm** | **sm** | **ssm** } | **flags** *flag-value* | **fsm**] * [**outgoing-interface-number** [*number*]]

display pim routing-table [*group-address* [**mask** { *group-mask-length* | *group-mask* }] | *source-address* [**mask** { *source-mask-length* | *source-mask* }] | **incoming-interface** { *interface-type interface-number* | **register** } | **outgoing-interface** { **include** | **exclude** | **match** } { *interface-type interface-number* | **vpn-instance** *vpn-instance-name* | **register** | **none** } | **mode** { **dm** | **sm** | **ssm** } | **flags** *flag-value* | **fsm**] * [**outgoing-interface-number** [*number*]]

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Displays PIM routing entries in a specified VPN instance. *vpn-instance-name* specifies the name of the VPN instance.	The value must be an existing VPN instance name.

Parameter	Description	Value
all-instance	Displays PIM routing entries in all the instances.	-
group-address	Displays the PIM routing entry of a specified group.	The address is in dotted decimal notation. The value ranges from 224.0.1.0 to 239.255.255.255.
mask	Specifies the mask of a multicast source address or group address.	-
group-mask	Specifies the group address mask.	The address is in dotted decimal notation.
group-mask-length	Specifies the length of the group address mask.	The value is an integer that ranges from 4 to 32.
source-address	Displays the PIM routing entry of a specified multicast source.	The source address is in dotted decimal notation.
source-mask	Specifies the multicast source IP address mask.	The address mask is in dotted decimal notation.
source-mask-length	Specifies the length of the source address mask.	The value is an integer that ranges from 0 to 32.
incoming-interface	Displays the PIM routing entries with a specified interface as the upstream interface.	-
interface-type interface-number	Specifies the type and number of an interface.	-
register	Indicates the register interface.	-
outgoing-interface	Displays the PIM routing entries with a specified interface as the downstream interface.	-
include	Displays the PIM routing entries with the downstream interface list containing a specified interface.	-

Parameter	Description	Value
exclude	Displays the PIM routing entries with the downstream interface list not containing a specified interface.	-
match	Displays the PIM routing entries with the downstream interface list containing only the specified interface.	-
none	Displays the PIM routing entries with an empty downstream interface list.	-
mode	Specifies the PIM operation mode.	-
dm	Displays PIM-DM routing entries.	-
sm	Displays PIM-SM routing entries.	-
ssm	Displays PIM-SSM routing entries.	-
flags *flag-value*	Displays PIM-SSM routing entries with the specified flag. The *flag-value* parameter is the type flag of entries.	-
fsm	Displays the details of FSM states.	-
outgoing-interface-number	Displays the number of downstream interfaces of PIM routing entries.	-
number	Specifies the number of the downstream interfaces to be displayed.	The value is an integer that ranges from 0 to 2048.
brief	Displays only the upstream interface names and the number of downstream interfaces in PIM routing entries.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can use this command to:

- Check whether PIM has been configured successfully on the network.
- Check the inbound interfaces, outbound interfaces, flags, and other information in the routing entries to identify failure points when forwarding errors occur on the PIM network.

The PIM routing table includes both (*, G) and (S, G) entries. (*, G) entries are used to set up a rendezvous point tree (RPT), and (S, G) entries are used to set up a shortest path tree (SPT).

Table 8-50 lists the values of the **flags** *flag-value* parameter.

Table 8-50 Values of the flag-value parameter

Item	Description
2msdp	The RP received a Register message recently and learned the (S, G) entry. The RP will notify MSDP of the (S, G) entry in the next SA message.
act	Multicast routing entries that have matched received data.
del	Multicast routing entries to be deleted.
exprune	Multicast routing entries pruned from the RPT, with no receiver interested in the data from the source.
ext	Multicast routing entries that contain downstream interfaces provided by other multicast routing protocols.
loc	Multicast routing entries on the switch directly connected to the network segment of the multicast source.
msdp	Multicast routing entries learned from recently received MSDP SA messages.
niif	Multicast routing entries with unknown upstream interfaces.
nonbr	Multicast routing entries in which the upstream neighbor address (link-local address) towards the RP or the source is not found.
none	Multicast routing entries without any flag.
rpt	Multicast routing entries that are on the RPT but do not use the RPT data.
sg_rcvr	The switch has receivers of the source specified in the (S, G) entry, and PIM is the owner of the downstream interfaces.
sgjoin	The switch has receivers of the source specified in the (S, G) entry, but PIM is not the owner of the downstream interfaces.

Item	Description
spt	Multicast routing entries on the shortest path tree (SPT).
swt	Multicast routing entries during the SPT switchover.
upchg	A route change has occurred. The current entry is using the original upstream interface to forward data and is waiting for data received from a new interface.
wc	(*, G) entry.

Example

Display the PIM routing table of the switch.

```
<HUAWEI> display pim routing-table
 VPN-Instance: public net
 Total 0 (*, G) entry; 1 (S, G) entry

 (172.16.0.12, 227.0.0.1)
    RP: 10.2.2.2
    Protocol: pim-sm, Flag: SPT LOC ACT
    UpTime: 02:54:43
    Upstream interface: Vlanif10
        Upstream neighbor: NULL
        RPF prime neighbor: NULL
    Downstream interface(s) information:
    Total number of downstreams: 1
        1: Vlanif20
            Protocol: pim-sm, UpTime: 02:54:43, Expires: 00:02:47
```

Table 8-51 Description of the **display pim routing-table** command output

Item	Description
Total 0 (*, G) entry; 1 (S, G) entry	Total number of (S, G) and (*, G) entries in the PIM routing table.
(172.16.0.12, 227.0.0.1)	(S, G) entry in the PIM routing table.
RP	RP address.
Protocol	PIM protocol type, which can be PIM-DM, PIM-SM or PIM-SSM.
Flag	Flag of PIM (S, G) or (*, G) entry. Refer to the table of *Values of the flag-value parameter*.
UpTime	Amount of time an interface has been Up.
Upstream interface	Upstream interface in an (S, G) entry or (*, G) entry.
Upstream neighbor	Upstream neighbor of an (S, G) or (*, G) entry.

Item	Description
RPF prime neighbor	RPF neighbor of an (S, G) or (*, G) entry. • For a (*, G) entry, when the local device is an RP, the RPF neighbor in the (*, G) entry is null. • For an (S, G) entry, when the local device is directly connected to the source, the RPF neighbor in the (S, G) entry is null.
Downstream interface(s) information	Information about the downstream interface, including the following: • Total number of downstream interfaces • Name of each downstream interface • PIM protocol type configured for the downstream interface • Keepalive period and timeout period of the downstream interface
Total number of downstreams	Number of downstream interfaces.
Expires	Timeout period of an interface.

Display the number of the downstream interfaces of PIM routing entries on the switch.

```
<HUAWEI> display pim routing-table outgoing-interface-number
 VPN-Instance: public net
 Total 2 (*, G) entries; 0 (S, G) entry

 (*, 226.1.1.1)
     RP: 10.2.2.2 (local)
     Protocol: pim-sm, Flag: WC EXT
     UpTime: 21:37:28
     Upstream interface: Register
         Upstream neighbor: NULL
         RPF prime neighbor: NULL
     Downstream interface(s) information:
     Total number of downstreams: 50

 (*, 226.1.2.1)
     RP: 10.2.2.2 (local)
     Protocol: pim-sm, Flag: WC EXT
     UpTime: 21:37:28
     Upstream interface: Register
         Upstream neighbor: NULL
         RPF prime neighbor: NULL
     Downstream interface(s) information:
     Total number of downstreams: 50
```


Table 8-52 Description of the **display pim routing-table outgoing-interface-number** command output

Item	Description
Total 2 (*, G) entries; 0 (S, G) entry	Total number of the (S, G) entries and (*, G) entries in the PIM routing table.
Total number of downstreams	Total number of the downstream interfaces of the (*, G) entries or (S, G) entries.

8.3.29 display pim rp-info

Function

The **display pim rp-info** command displays information about the RP for a multicast group.

Format

display pim [**vpn-instance** *vpn-instance-name* | **all-instance**] **rp-info** [*group-address*]

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Specifies the name of a VPN instance.	The value must be an existing VPN instance name.
all-instance	Specifies all the instances.	-
group-address	Displays the information about the RP for a specified multicast group.	The address is in dotted decimal notation. The value ranges from 224.0.1.0 to 239.255.255.255.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

You can use this command to view information about the RP for a multicast group.

Configuration Impact

The command output includes information about the RP discovered through the BSR mechanism and static RP.

If *group-address* is not specified, the command displays RP information for all the multicast groups.

Example

Display RP information for all the multicast groups in the public network instance.

```
<HUAWEI> display pim rp-info
 VPN-Instance: public net
 PIM-SM BSR RP Number:1
 Group/MaskLen: 224.0.0.0/4
     RP: 10.2.2.2 (local)
     Priority: 0
     Uptime: 03:01:36
     Expires: 00:02:29
 PIM SM static RP Number:1
     Static RP: 10.1.1.1
```

Table 8-53 Description of the **display pim rp-info** command output

Item	Description
PIM-SM BSR RP Number	Number of PIM-SM RPs elected dynamically using the BSR mechanism.
Group/MaskLen	Multicast group address and mask length.
RP	RP address.
Priority	Priority of the RP.
Uptime	Time elapsed since presence of the RP.
Expires	Amount of time left before the RP times out.
PIM SM static RP Number	Number of static RPs.
Static RP	IP address of a static RP.

8.3.30 graceful-restart (IPv4)

Function

The **graceful-restart** command enables PIM GR.

The **undo graceful-restart** command disables PIM GR.

By default, PIM GR is not enabled.

Format

graceful-restart

undo graceful-restart

Parameters

None

Views

PIM view of public network instance or PIM view of VPN instance

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If a stack is used on the PIM-SM network, after an active/standby switchover occurs in the stack system, multicast data transmission is interrupted because the new master device does not have PIM forwarding entries.

PIM GR enables the system to back up join and prune information in PIM routing entries to the new master device when an active/standby switchover is performed in the system. This ensures normal multicast data forwarding during restoration of the multicast distribution tree. For details about stack configuration, see Stack Configuration in the *S300, S500, S2700, S5700, and S6700 V200R023C00 Configuration Guide - Device Management*.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command.

Precautions

At least one switch interface must have PIM-SM enabled for the **graceful-restart** command to take effect.

Example

Enable PIM GR in the PIM view of public network instance.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] pim
[HUAWEI-pim] graceful-restart
```

8.3.31 graceful-restart period (IPv4)

Function

The **graceful-restart period** command configures the minimum PIM GR period.

The **undo graceful-restart period** command restores the default minimum PIM GR period.

By default, the minimum PIM GR period is 120 seconds.

Format

graceful-restart period *period*

undo graceful-restart period

Parameters

Parameter	Description	Value
period	Specifies the minimum PIM GR period.	The value is an integer that ranges from 90 to 3600 in seconds.

Views

PIM view of public network instance or PIM view of VPN instance

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **graceful-restart period** command ensures the minimum time for maintaining forwarding entries.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command.

Configuration Impact

If you run the **graceful-restart period** command multiple times, only the latest configuration takes effect.

Precautions

Unicast protocol GR form the basis of PIM GR; therefore, the minimum PIM GR period must be longer than the unicast protocol GR period.

The PIM GR period also depends on the complexity of the network topology and increases with the expansion of unicast route capacity and multicast route capacity.

Example

Set the minimum PIM GR period in the PIM view of public network instance to 150 seconds.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] pim
```



```
[HUAWEI-pim] graceful-restart
[HUAWEI-pim] graceful-restart period 150
```

8.3.32 hello ipsec sa (IPv4)

Function

The **hello ipsec sa** command specifies an IPSec SA globally used for encrypting and authenticating PIM Hello (IPv4) messages sent and received by the device.

The **undo hello ipsec sa** command deletes the IPSec SA globally used for encrypting and authenticating PIM Hello (IPv4) messages sent and received by the device.

By default, no IPSec SA is specified for encrypting and authenticating PIM Hello (IPv4) messages.

Format

hello ipsec sa *sa-name*

undo hello ipsec sa

Parameters

Parameter	Description	Value
sa-name	Specifies the name of the globally used SA.	The value is an existing SA name.

Views

PIM view of public network instance or PIM view of VPN instance

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When a Huawei device connects to a non-Huawei device that can only encrypt and authenticate PIM Hello messages, run this command to configure the Huawei device to encrypt and authenticate only PIM Hello messages, so that the devices can interwork.

Prerequisites

- IP multicast routing has been enabled using the **multicast routing-enable** command.
- Basic IPSec functions have been configured.

Precautions

If you run both this command and the **ipsec sa (IPv4)** command in the PIM view, the last configured one takes effect.

This command has the same function as the **pim hello ipsec sa** command used in the interface view except for the effective scope. The configuration in the interface view takes precedence over the configuration in the PIM view. If SAs are specified in both the interface view and PIM view, the specified interface uses the SA configured in the interface view. If no SA is specified on an interface, the interface uses the SA specified in the PIM view.

Example

Configure the device to encrypt and authenticate PIM Hello messages using the PIM IPSec SA named **sa1**. (This SA has been created.)

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] pim
[HUAWEI-pim] hello ipsec sa sa1
```

8.3.33 hello-option dr-priority (IPv4)

Function

The **hello-option dr-priority** command configures the priority of the switch that candidates for the Designated Router (DR).

The **undo hello-option dr-priority** command restores the default priority.

By default, the priority of the switch that candidates for the DR is 1.

Format

hello-option dr-priority *priority*

undo hello-option dr-priority

Parameters

Parameter	Description	Value
priority	Specifies the priority of the switch that candidates for the DR. The greater the value, the higher the priority.	The value is an integer ranging from 0 to 4294967295.

Views

PIM view of public network instance or PIM view of VPN instance

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On a PIM network, switches on a shared network segment are candidates for the DR. The DR is responsible for registration of local multicast sources and the joining of receivers.

The DR is elected based on the priority and the IP address. Candidates send Hello messages with their priorities, and the switch with the highest priority becomes the DR. If multiple switches have the same priority, the switch with the largest IP address becomes the DR.

If at least one switch in the network does not support Hello packets that contain the priority, the switch with the largest IP address becomes the DR.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command.

Precautions

The **hello-option dr-priority** command has the same function as the **pim hello-option dr-priority** command in the interface view. By default, if the **pim hello-option dr-priority** command is not used, the value configured in the PIM view is used; otherwise, the value configured in the interface view is used.

Example

In the PIM view of public network instance, configure the DR priority of a switch to 3.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] pim
[HUAWEI-pim] hello-option dr-priority 3
```

8.3.34 hello-option holdtime (IPv4)

Function

The **hello-option holdtime** command sets the timeout period for a switch to wait to receive Hello messages from its PIM neighbor.

The **undo hello-option holdtime** command restores the default configuration.

By default, the timeout period for a switch to wait to receive Hello messages from its PIM neighbor is 105 seconds.

Format

hello-option holdtime *interval*

undo hello-option holdtime

Parameters

Parameter	Description	Value
interval	Specifies the timeout time during which a switch waits to receive a Hello message from its PIM neighbor.	The value is an integer ranging from 1 to 65535, in seconds.

Views

PIM view of public network instance or PIM view of VPN instance

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On a PIM network, after the switch receives a Hello message from its PIM neighbor, it starts a timer. The timer length is the value of Holdtime in the Hello message. If the switch does not receive any Hello message from its PIM neighbor when the timer expires, it considers the neighbor invalid or unreachable.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command.

Precautions

- The **hello-option holdtime** command is valid for PIM-SM and PIM-DM.
- The timeout period must be greater than the interval for sending Hello messages. You can run the **timer hello** command to set the interval for sending Hello messages.
- The **hello-option holdtime** command has the same function as the **pim hello-option holdtime** command in the interface view. By default, if the **pim hello-option holdtime** command is not used, the value configured in the PIM view is used; otherwise, the value configured in the interface view is used.

Example

In the PIM view of public network instance, set the timeout interval to 120 seconds. The timeout interval is the period during which a switch waits to receive the Hello message from its PIM neighbor.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] pim
[HUAWEI-pim] hello-option holdtime 120
```


8.3.35 hello-option lan-delay (IPv4)

Function

The **hello-option lan-delay** command sets the delay in transmitting Prune message on the shared network segment.

The **undo hello-option lan-delay** command restores the default delay.

By default, the delay in transmitting Prune message on the shared network segment is 500 milliseconds.

Format

hello-option lan-delay *interval*

undo hello-option lan-delay

Parameters

Parameter	Description	Value
interval	Specifies the delay in transmitting Prune message on the shared network segment.	The value is an integer that ranges from 1 to 32767, in milliseconds (ms).

Views

PIM view of public network instance or PIM view of VPN instance

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Hello messages sent from switches carry **lan-delay** and **override-interval** values. The **lan-delay** parameter indicates the delay in transmitting messages in the LAN. If switches on the same link have different **lan-delay** values, the maximum value is used.

When a switch sends a Prune message to the upstream device in the same network segment, other switches that still request multicast data need to send a Join message to the upstream device within the override-interval period.

The value of the Prune-Pending Timer (PPT) is the sum of the **lan-delay** and **override-interval** values, and refers to the delay from the switch receiving a Prune message from the downstream interface to performing the prune action. If the switch receives a Join message from the downstream interface in PPT, the switch cancels the prune action.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command.

Precautions

This command is valid for PIM-SM and PIM-DM.

If the delay in transmitting Prune message is too short, the upstream switch will stop forwarding multicast packets before the downstream switch determines whether to override the Prune action or not. Exercise caution when you run the **hello-option lan-delay** command.

The **hello-option lan-delay** command has the same function as the **pim hello-option lan-delay** command in the interface view. By default, if the **pim hello-option lan-delay** command is not used, the value configured in the PIM view is used; otherwise, the value configured in the interface view is used.

Example

Set the delay in transmitting Prune message on the shared network segment to 200 ms in PIM view of public network instance.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] pim
[HUAWEI-pim] hello-option lan-delay 200
```

8.3.36 hello-option neighbor-tracking (IPv4)

Function

The **hello-option neighbor-tracking** command enables the neighbor tracking function.

The **undo hello-option neighbor-tracking** command restores the default configuration.

By default, the neighbor tracking function is not enabled.

Format

hello-option neighbor-tracking

undo hello-option neighbor-tracking

Parameters

None

Views

PIM view of public network instance or PIM view of VPN instance

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When sending a Hello message, the switch generates a Generation ID and encapsulates it into the message. The Generation ID changes only when the status of the switch changes. In this case, the neighboring device detects the Generation ID change after receiving the Hello message and immediately sends a Join message to the switch to update the neighbor relationship. If multiple devices on the shared network segment prepare to send Join messages to the same upstream PIM neighbor, only one device is allowed to send the Join message. After other devices detect the Join message, they do not send Join messages to the upstream neighbor. This means that the upstream neighbor cannot update neighbor relationships with downstream devices after a Generation ID change.

After the neighbor tracking function is enabled, when the device detects Join messages from other devices, the device still sends the Join messages to the same upstream PIM neighbor.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command.

Precautions

This command is valid for only PIM-SM.

Neighbor tracking can be implemented only when this function is enabled on all devices on the shared network segment.

The **hello-option neighbor-tracking** command has the same function as the **pim hello-option neighbor-tracking** command in the interface view. By default, if neighbor tracking is not used on an interface, the neighbor tracking configuration in the PIM view takes effect.

Example

In the PIM view of public network instance, enable the downstream neighbor tracking function.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] pim
[HUAWEI-pim] hello-option neighbor-tracking
```

8.3.37 hello-option override-interval (IPv4)

Function

The **hello-option override-interval** command sets the interval for overriding the prune action in a Hello message.

The **undo hello-option override-interval** command restores the default interval.

By default, the interval for overriding the prune action in a Hello message is 2500 ms.

Format

hello-option override-interval *interval*

undo hello-option override-interval

Parameters

Parameter	Description	Value
interval	Specifies the interval for overriding the prune action in a Hello message.	The value is an integer that ranges from 1 to 65535, in milliseconds.

Views

PIM view of public network instance or PIM view of VPN instance

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Hello messages sent from switches carry **lan-delay** and **override-interval** parameters. The **override-interval** parameter indicates the period during which a downstream switch can override the prune action.

When a switch sends a Prune message to the upstream device in the same network segment, other switches that still request multicast data need to send a Join message to the upstream device within the override-interval period.

When a device has only one PIM neighbor on a link and receives a Prune message from the neighbor, the device immediately deletes the downstream interface of the multicast routing entry. If a device has two or more PIM neighbors on a link and the **override-interval** values in the messages sent from the two neighbors are different, the largest **override-interval** value takes effect.

The value of Prune-Pending Timer (PPT) is the sum of **lan-delay** and **override-interval** values. When receiving a Prune message from a downstream interface, the switch does not perform the prune action until the PPT times out. If the switch receives a Join message from the downstream interface in PPT, the interface cancels the Prune action.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command.

Precautions

This command is valid for PIM-SM and PIM-DM.

The **hello-option override-interval** command has the same function as the **pim hello-option override-interval** command in the interface view. By default, if the **pim hello-option override-interval** command is not used, the value configured in the PIM view is used; otherwise, the value configured in the interface view is used.

Example

In the PIM view of public network instance, set the interval for denying the prune action in a Hello message to 2000 ms.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] pim
[HUAWEI-pim] hello-option override-interval 2000
```

8.3.38 holdtime assert (IPv4)

Function

The **holdtime assert** command sets the timeout period for all PIM interfaces to keep the Assert state on the local switch.

The **undo holdtime assert** command restores the default timeout.

By default, the timeout period for all PIM interfaces to keep the Assert state on the local switch is 180 seconds.

Format

holdtime assert *interval*

undo holdtime assert

Parameters

Parameter	Description	Value
interval	Specifies the time during which the PIM interface keeps the Assert state.	The value is an integer that ranges from 7 to 65535, in seconds.

Views

PIM view of public network instance or PIM view of VPN instance

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On the shared network segment connected to multiple PIM devices, if the same multicast packets reach these PIM devices and pass the RPF check, multiple copies

of the same multicast packets are forwarded to this network segment. In this situation, these PIM devices need to initiate the assert mechanism. The device that wins assert election is responsible for multicast forwarding on the shared network segment. Other devices suppress multicast data forwarding and retain the Assert state for a period of time. After the timer for a PIM interface in the Assert state expires, the device that fails to be elected triggers a new round of election.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command.

Precautions

The **holdtime assert** command is valid for PIM-SM and PIM-DM.

The **holdtime assert** command has the same function as the **pim holdtime assert** command in the interface view. By default, if the timeout period is not used on an interface, the timeout period configured in the PIM view is used.

Example

In the PIM view of public network instance, set the interval during which a switch keeps the Assert state to 100s.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] pim
[HUAWEI-pim] holdtime assert 100
```

8.3.39 holdtime join-prune (IPv4)

Function

The **holdtime join-prune** command sets the holdtime value in Join/Prune messages sent by all PIM interfaces. The devices that receive Join/Prune messages set the time during which the downstream interface keeps the Join or Prune state according to holdtime.

The **undo holdtime join-prune** command restores the default value.

By default, the holdtime value in Join/Prune messages sent by all PIM interfaces is 210 seconds.

Format

holdtime join-prune *interval*

undo holdtime join-prune

Parameters

Parameter	Description	Value
interval	Specifies the value of holdtime carried in Join/Prune messages sent by the local switch.	The value is an integer that ranges from 1 to 65535, in seconds.

Views

PIM view of public network instance or PIM view of VPN instance

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After receiving a Join/Prune message from the downstream device, the switch starts the hold timer. If this message carries group-join information and the switch does not receive subsequent Join/Prune messages from the downstream device when the timer expires, it suppresses multicast data forwarding to downstream interfaces of the specified group. If Join/Prune message carries group-prune information, the switch resumes multicast data forwarding to downstream interfaces when the hold timer expires.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command.

Precautions

This command is valid for PIM-SM and PIM-DM.

The holdtime of Join/Prune messages must be larger than the interval for sending Join/Prune messages and is generally 3.5 times the interval for sending Join/Prune messages.

The **holdtime join-prune** command has the same function as the **pim holdtime join-prune** command in the interface view. By default, if the holdtime value is not used on an interface, the holdtime value configured in the PIM view is used.

Example

In the PIM view of public network instance, set the time during which the downstream interface of a switch keeps the Join or Prune state to 280 seconds.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] pim
[HUAWEI-pim] holdtime join-prune 280
```


8.3.40 ipsec sa (IPv4)

Function

The **ipsec sa** command specifies an IPSec SA globally used for encrypting and authenticating PIM messages sent and received by the device.

The **undo ipsec sa** command deletes the IPSec SA globally used for encrypting and authenticating PIM messages sent and received by the device.

By default, no IPSec SA is specified for encrypting and authenticating PIM messages.

Format

ipsec [**unicast-message**] **sa** *sa-name*

undo ipsec [**unicast-message**] **sa**

Parameters

Parameter	Description	Value
unicast-message	Authenticates only PIM unicast messages. If you do not specify this keyword, the device authenticates only PIM multicast messages.	-
sa-name	Specifies the name of the globally used SA.	The value is an existing SA name.

Views

PIM view of public network instance or PIM view of VPN instance

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On an IPv4 multicast network, if multicast devices are attacked by forged PIM messages, multicast data forwarding between multicast devices will be interrupted. To protect multicast devices against such attacks, configure PIM IPSec on the multicast devices to authenticate PIM messages they send and receive.

Prerequisites

- IP multicast routing has been enabled using the **multicast routing-enable** command.

- Basic IPSec functions have been configured.

Precautions

If you run both the **ipsec sa** *sa-name* command and the **hello ipsec sa (IPv4)** command in the PIM view, the last configured one takes effect.

This command has the same function as the **pim ipsec sa** command used in the interface view, except for the effective scope. The configuration in the interface view takes precedence over the configuration in the PIM view. If SAs are specified in both the interface view and PIM view, the specified interface uses the SA configured in the interface view. If no SA is specified on an interface, the interface uses the SA specified in the PIM view.

Example

Configure the device to encrypt and authenticate PIM multicast messages using the PIM IPSec SA named **sa1**. (This SA has been created.)

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] pim
[HUAWEI-pim] ipsec sa sa1
```

8.3.41 join-prune max-packet-length (IPv4)

Function

The **join-prune max-packet-length** command sets the maximum size of each PIM-SM Join/Prune message to be sent.

The **undo join-prune max-packet-length** command restores the default maximum size of each PIM-SM Join/Prune message to be sent.

By default, the maximum length of Join/Prune message sent by PIM-SM is 8100 bytes.

Format

join-prune max-packet-length *packet-length*

undo join-prune max-packet-length

Parameters

Parameter	Description	Value
packet-length	Specifies the maximum size of each PIM-SM Join/Prune message to be sent.	The value is an integer ranging from 100 to 8100, in bytes.

Views

PIM view of public network instance or PIM view of VPN instance

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If the peer device has low performance and takes a long time to process a large Join/Prune message carrying a lot of (S, G) entries, the maximum size of each Join/Prune message can be reduced to relieve the burden on the peer device.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command.

Precautions

This command is valid for PIM-SM and PIM-DM.

If the maximum size specified in the **join-prune max-packet-length** command is greater than the interface MTU, the maximum size of each message to be sent is equal to the interface MTU.

Example

Set the maximum size of each Join/Prune message to be sent to 2100 bytes.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] pim
[HUAWEI-pim] join-prune max-packet-length 2100
```

8.3.42 join-prune periodic-messages queue-size (IPv4)

Function

The **join-prune periodic-messages queue-size** command sets the maximum number of (S, G) entries carried in a PIM-SM Join/Prune message that is sent every second.

The **undo join-prune periodic-messages queue-size** command restores the default maximum number of (S, G) entries carried in a PIM-SM Join/Prune message that is sent every second.

By default, a PIM-SM Join/Prune message that is sent every second contains 1020 entries.

Format

join-prune periodic-messages queue-size *queue-size*

undo join-prune periodic-messages queue-size

Parameters

Parameter	Description	Value
queue-size	Specifies the maximum number of (S, G) entries carried in a PIM-SM Join/Prune message that is sent every second.	The value is an integer ranging from 16 to 4096.

Views

PIM view of public network instance or PIM view of VPN instance

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If the peer device has a low throughput, reduce the length of a queue for periodically sending messages to control the number of (S, G) entries. This setting allows the local device to send Join/Prune messages with a small number of (S, G) entries multiple times, preventing packet loss or route flapping.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command.

Precautions

This command is valid for PIM-SM and PIM-DM.

Example

Allow each PIM-SM Join/Prune message that is sent every second to carry a maximum of 2000 (S, G) entries.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] pim
[HUAWEI-pim] join-prune periodic-messages queue-size 2000
```

8.3.43 join-prune triggered-message-cache disable (IPv4)

Function

The **join-prune triggered-message-cache disable** command disables the Join/Prune message package function.

The **undo join-prune triggered-message-cache disable** command enables the Join/Prune message package function.

By default, the Join/Prune message package function is enabled.

Format

join-prune triggered-message-cache disable

undo join-prune triggered-message-cache disable

Parameters

None

Views

PIM view of public network instance or PIM view of VPN instance

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The system performs more efficiently when sending package of PIM Join/Prune messages than when sending a large number of individual PIM Join/Prune messages. A switch sends PIM Join/Prune messages in packages. To disable the package function, run the **join-prune triggered-message-cache disable** command.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command.

Precautions

This command is valid for PIM-SM and PIM-DM.

Example

Disable the Join/Prune message package function.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] pim
[HUAWEI-pim] join-prune triggered-message-cache disable
```

8.3.44 neighbor-check (IPv4)

Function

The **neighbor-check** command enables the PIM neighbor check function.

The **undo neighbor-check** command restores the default setting.

By default, the PIM neighbor check function is not enabled.

Format

neighbor-check { **receive** | **send** }

undo neighbor-check { **receive** | **send** }

Parameters

Parameter	Description	Value
receive	Checks whether the Join/Prune and Assert messages are received from a PIM neighbor. If not, these messages are discarded.	-
send	Checks whether the Join/Prune and Assert messages are sent to a PIM neighbor. If not, these messages are not sent.	-

Views

PIM view of public network instance or PIM view of VPN instance

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

PIM devices send Join/Prune messages to the upstream PIM neighbor to perform join, and prune actions and PIM neighbors often exchange Assert messages. To save system resources and protect security of Join/Prune messages and Assert messages, run the **neighbor-check** command to enable the PIM neighbor check function.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command.

Configuration Impact

You can specify both **receive** and **send** to enable the PIM neighbor check function for the received and sent Join/Prune and Assert messages.

Precautions

This command is valid only for PIM-SM.

Example

In the PIM view of public network instance, enable the PIM neighbor check function for the received Join/Prune and Assert messages.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] pim
[HUAWEI-pim] neighbor-check receive
```


8.3.45 pim

Function

The **pim** command displays the PIM view.

The **undo pim** command clears the configuration in the PIM view.

Format

pim [**vpn-instance** *vpn-instance-name*]

undo pim [**vpn-instance** *vpn-instance-name*]

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Specifies the name of a VPN instance.	The value must be an existing VPN instance name.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Before performing PIM configurations, run the **pim** command to enter the PIM view.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command.

Precautions

NOTE

Running the **undo pim** command in the system view may interrupt IPv4 PIM services and deletes all global IPv4 PIM configurations of the public network instance. To restore the IPv4 PIM services, you have to re-run the deleted commands.

Example

Enter the PIM view.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
```



```
[HUAWEI] pim
[HUAWEI-pim]
```

8.3.46 pim bfd

Function

The **pim bfd** command adjusts the PIM BFD parameters on an interface.

The **undo pim bfd** command restores the default values of PIM BFD parameters.

By default, the minimum interval for transmitting BFD packets and minimum interval for receiving BFD packets are 1000 ms, and the BFD detection multiplier is 3.

NOTE

Only the S5720I-SI, S5735-S, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6720S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Format

pim bfd { **min-tx-interval** *tx-value* | **min-rx-interval** *rx-value* | **detect-multiplier** *multiplier-value* } *

undo pim bfd { **min-tx-interval** | **min-rx-interval** | **detect-multiplier** } *

undo pim bfd { **min-tx-interval** *tx-value* | **min-rx-interval** *rx-value* | **detect-multiplier** *multiplier-value* } *

Parameters

Parameter	Description	Value
min-tx-interval *tx-value*	Specifies the minimum interval for transmitting BFD packets.	The value is an integer that ranges from 100 to 1000, in milliseconds. • After the **set service-mode enhanced** command is configured on the S5731-H, S5731-S, S5731S-H, and S5731S-S, the value ranges from 3 to 1000. • After the **set service-mode enhanced-bfd** command is configured on the S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S, the value ranges from 3 to 1000.

Parameter	Description	Value
min-rx-interval *rx-value*	Specifies the minimum interval for receiving BFD packets.	The value is an integer that ranges from 100 to 1000, in milliseconds. • After the **set service-mode enhanced** command is configured on the S5731-H, S5731-S, S5731S-H, and S5731S-S, the value ranges from 3 to 1000. • After the **set service-mode enhanced-bfd** command is configured on the S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S, the value ranges from 3 to 1000.
detect-multiplier *multiplier-value*	Specifies the BFD detection multiplier.	The value is an integer that ranges from 3 to 50. The default value is 3.

Views

GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, Eth-Trunk interface view, 100GE interface view, GE sub-interface view, XGE sub-interface view, MultiGE sub-interface view, 25GE sub-interface view, 40GE sub-interface view, 100GE sub-interface view, Eth-Trunk sub-interface view, VLANIF interface view, loopback interface view, tunnel interface view, VBDIF interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After PIM BFD is enabled, you may need to run the **pim bfd** command to adjust PIM BFD parameters to adapt to the state of the link. This command can set the minimum interval for sending BFD packets, minimum interval for receiving PIM BFD packets, and local detection multiplier.

In application, you can continuously configure one or more parameters. If some parameters are configured, other parameters that are not configured reserve the existing configurations.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command.

Precautions

This command is valid only for PIM-SM.

Before setting PIM BFD parameters, run the **pim bfd enable** command to enable PIM BFD. Otherwise, the configured parameters do not take effect.

The minimum values of *tx-value* and *rx-value* vary with products.

Example

Adjust the minimum interval for transmitting BFD packets on VLANIF 10.

```
<HUAWEI> system-view
[HUAWEI] bfd
[HUAWEI-bfd] quit
[HUAWEI] multicast routing-enable
[HUAWEI] interface vlanif 10
[HUAWEI-Vlanif10] pim sm
[HUAWEI-Vlanif10] pim bfd enable
[HUAWEI-Vlanif10] pim bfd min-tx-interval 100
```

Adjust the minimum interval for transmitting BFD packets on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] bfd
[HUAWEI-bfd] quit
[HUAWEI] multicast routing-enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] pim sm
[HUAWEI-GigabitEthernet0/0/1] pim bfd enable
[HUAWEI-GigabitEthernet0/0/1] pim bfd min-tx-interval 100
```

8.3.47 pim bfd enable

Function

The **pim bfd enable** command enables PIM BFD on an interface.

The **undo pim bfd enable** command disables PIM BFD on an interface.

By default, PIM BFD is not enabled on an interface.

NOTE

Only the S5720I-SI, S5735-S, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6720S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Format

pim bfd enable

undo pim bfd enable

Parameters

None

Views

GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, Eth-Trunk interface view, 100GE interface view, GE sub-interface view, XGE sub-interface view, MultiGE sub-interface view, 25GE sub-

interface view, 40GE sub-interface view, 100GE sub-interface view, Eth-Trunk sub-interface view, VLANIF interface view, loopback interface view, tunnel interface view, VBDIF interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

This command enables PIM BFD on an interface to quickly detect link failures on the interface.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command.

Run the **pim sm** command on the interface to enable PIM-SM. You can run the **undo pim sm** command to disable PIM BFD on the interface.

Precautions

This command is valid for only PIM-SM.

PIM BFD depends on the BFD protocol. If global BFD is not enabled using the **bfd** command, PIM BFD sessions can still be set up but the session state is **BFD global disable**.

Example

Enable PIM BFD on VLANIF100.

```
<HUAWEI> system-view
[HUAWEI] bfd
[HUAWEI-bfd] quit
[HUAWEI] multicast routing-enable
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] pim sm
[HUAWEI-Vlanif100] pim bfd enable
```

Enable PIM BFD on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] bfd
[HUAWEI-bfd] quit
[HUAWEI] multicast routing-enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] pim sm
[HUAWEI-GigabitEthernet0/0/1] pim bfd enable
```

8.3.48 pim bsr-boundary

Function

The **pim bsr-boundary** command configures the BSR boundary of a PIM-SM domain on an interface.

The **undo pim bsr-boundary** command restores the default configuration.

By default, the BSR boundary of a PIM-SM domain is not set.

Format

pim bsr-boundary

undo pim bsr-boundary

Parameters

None

Views

GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, GE sub-interface view, XGE sub-interface view, MultiGE sub-interface view, 25GE sub-interface view, 40GE sub-interface view, 100GE sub-interface view, Eth-Trunk sub-interface view, VLANIF interface view, loopback interface view, tunnel interface view, VBDIF interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

As the management core of the PIM-SM network, the BSR is responsible for sending collected RP-set information to PIM neighbors through Bootstrap messages.

You can divide a large PIM-SM network into multiple PIM-SM domains by configuring the bsr boundary on an interface. Each BSR then serves the local PIM-SM domain.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command.

Configuration Impact

The Bootstrap messages cannot traverse the BSR boundary but other multicast packets can.

Example

Configure the BSR boundary of a PIM-SM domain on VLANIF100.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] pim bsr-boundary
```

Configure the BSR boundary of a PIM-SM domain on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
```



```
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] pim bsr-boundary
```

8.3.49 pim dm

Function

The **pim dm** command enables PIM-DM on an interface.

The **undo pim dm** command restores the default configuration.

By default, PIM-DM is disabled on an interface.

Format

pim dm

undo pim dm

Parameters

None

Views

GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, GE sub-interface view, XGE sub-interface view, MultiGE sub-interface view, 25GE sub-interface view, 40GE sub-interface view, 100GE sub-interface view, Eth-Trunk sub-interface view, VLANIF interface view, loopback interface view, tunnel interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On a PIM-DM network, after PIM-DM is enabled on an interface, the switch can set up the PIM neighbor relationship with the neighboring device. The switch can then process protocol packets received from the PIM neighbor.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command in the public network instance or VPN instance.

Precautions

- PIM-DM and PIM-SM cannot be enabled simultaneously on interfaces bound to the same VPN instance or public network instance.
- If PIM-DM and IGMP need to be enabled on the same interface, enable PIM-DM, and then enable IGMP.

- If Layer 2 multicast querier or Layer 2 multicast packet suppression is enabled in a VLAN, running the **pim dm** command on the corresponding VLANIF interface will fail.
- If both Layer 2 and Layer 3 multicast services are required in a VLAN, enable IPv4 PIM on the corresponding VLANIF interface first, and then enable IGMP snooping in the VLAN. If IGMP snooping is enabled in the VLAN first, IPv4 PIM cannot be enabled on the corresponding VLANIF interface.
- PIM-DM cannot be deployed on the public network of the MVPN.
- Since V200R010, the S5720-HI, S5730-HI, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6720-HI, S6730-H, S6730S-H, S6730-S, and S6730S-S support IPv4 PIM configuration on dot1q and QinQ termination sub-interfaces only when the VLAN tag to be terminated (or both inner and outer VLAN tags on the QinQ termination sub-interface) is a single VLAN ID, but not a range of VLAN IDs. Sub-interfaces running PIM can only be used as inbound interfaces of multicast streams and cannot be used as outbound interfaces. The S5720-EI, S6720-EI, S6735-S, and S6720S-EI also support IPv4 PIM command configuration on dot1q and QinQ termination sub-interfaces, but they do not support multicast traffic forwarding on these sub-interfaces.
- PIM-DM and PIM-SM cannot be configured simultaneously in a VPN instance or the public network instance. IPv4 PIM can be configured in a VPN instance, but the VPN instance cannot be bound to a physical interface that has been switched to Layer 3 mode using the **undo portswitch** command. Only the following products and versions support the IPv4 PIM multi-instance feature:
  - S5730-HI, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6720-HI, S6730-H, S6730S-H, S6730-S, and S6730S-S: all versions
  - S6700-EI and S5700-HI: V200R005C01
  - S6700-EI, S5700-HI, and S5710-HI: V200R005C02
  - S5710-HI: V200R005C03
  - S5720-EI, S5720-HI, S6720-EI, S6735-S, and S6720S-EI: V200R010 and later versions
- Secondary IP addresses does not support PIM, and the direct routes generated based on secondary IP addresses are not involved during multicast RPF check. Therefore, if the source IP address of multicast packets is on the same network segment as the secondary IP address of a Layer 3 interface, these multicast packets received on the Layer 3 interface cannot pass the RPF check.

Example

Enable PIM-DM on VLANIF100.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] pim dm
```

Enable PIM-DM on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] pim dm
```


8.3.50 pim dr-election dr-priority

Function

The **pim dr-election dr-priority** command configures an IP address and a priority for PIM DR election.

The **undo dr-election dr-priority** command restores the default IP address and priority for PIM DR election.

By default, no IP address or priority is configured for PIM DR election.

NOTE

This command is supported only on the S6730-H, S6730S-H, S6730-S, S6730S-S, S5732-H, S5731-S, S5731S-S, S5731S-H, and S5731-H.

Format

pim dr-election *ip-address* **dr-priority** *priority-value*

undo pim dr-election *ip-address* **dr-priority** *priority-value*

Parameters

Parameter	Description	Value
ip-address	Specifies the IP address used for PIM DR election.	The value is in dotted decimal notation.
dr-priority *priority-value*	Specifies the DR priority of a PIM interface. A larger value indicates a higher priority.	The value is an integer in the range from 0 to 4294967295.

Views

VBDIF interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In a VXLAN multi-border distributed gateway scenario, the same primary IP address is configured for VBDIF interfaces on multiple border nodes. These VBDIF interfaces use the primary IP address to send PIM protocol packets. During PIM negotiation, the local device considers itself as a PIM DR and forwards multicast traffic. As a result, excessive multicast traffic instead of only one copy of multicast traffic is forwarded. In this case, you can run this command to specify the IP address used to send PIM protocol packets.

During PIM DR election, the IP address and DR priority configured using the **pim dr-election dr-priority** command take precedence over the interface IP address and the DR priority configured using the **pim hello-option dr-priority** command.

During PIM Assert election, the IP address configured using the **pim dr-election dr-priority** command takes precedence over the interface IP address.

Precautions

- PIM can be configured on a VBDIF interface, which supports only DR election.
- In the multi-border distributed gateway scenario, to solve the problem of multiple copies of multicast traffic on the network segment where the VBDIF interface resides, configure different IP addresses for PIM DR election.
- If a fault occurs in the multi-border scenario, PIM needs to be associated with BFD to implement fast route switchover. In this case, you need to configure a secondary IP address that is the same as the IP address for PIM DR election on the VBDIF interface to send BFD packets.
- After the **pim dr-election dr-priority** command is run on a VBDIF interface, the **pim hello-option dr-priority** command no longer takes effect.

Example

Set the IP address and priority for DR election on VBDIF 10 to 10.0.0.1 and 20 respectively.

```
<HUAWEI> system-view
[HUAWEI] bridge-domain 10
[HUAWEI-bd10] quit
[HUAWEI] interface vbdif 10
[HUAWEI-Vbdif10] pim dr-election 10.1.1.2 dr-priority 20
```

8.3.51 pim hello ipsec sa

Function

The **pim hello ipsec sa** command specifies an IPSec SA used for encrypting and authenticating PIM Hello messages sent and received on an interface.

The **undo pim hello ipsec sa** command deletes the IPSec SA used for encrypting and authenticating PIM Hello messages sent and received on an interface.

By default, no IPSec SA is specified for encrypting and authenticating PIM Hello messages on an interface.

Format

pim hello ipsec sa *sa-name*

undo pim hello ipsec sa

Parameters

Parameter	Description	Value
sa-name	Specifies the name of the SA used on an interface.	The value is an existing SA name.

Views

GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, GE sub-interface view, XGE sub-interface view, MultiGE sub-interface view, 25GE sub-interface view, 40GE sub-interface view, 100GE sub-interface view, Eth-Trunk sub-interface view, VLANIF interface view, loopback interface view, tunnel interface view, VBDIF interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When a Huawei device connects to a non-Huawei device that can only encrypt and authenticate PIM Hello messages, run this command to configure the Huawei device to encrypt and authenticate only PIM Hello messages.

Prerequisites

- IP multicast routing has been enabled using the **multicast routing-enable** command.
- Basic IPSec functions have been configured.

Precautions

If you run both this command and the **pim ipsec sa** command on an interface, the last configured one takes effect.

This command has the same function as the **hello ipsec sa (IPv4)** command used in the PIM view, except for the effective scope. The configuration in the interface view takes precedence over the configuration in the PIM view. If SAs are specified in both the interface view and PIM view, the specified interface uses the SA configured in the interface view. If no SA is specified on an interface, the interface uses the SA specified in the PIM view.

Example

Configure the device to encrypt and authenticate PIM Hello messages sent and received on VLANIF100 using the PIM IPSec SA named **sa1**. (This SA has been created.)

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
```



```
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] pim hello ipsec sa sa1
```

Configure the device to encrypt and authenticate PIM Hello messages sent and received on GE0/0/1 using the PIM IPSec SA named **sa1**. (This SA has been created.)

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] pim hello ipsec sa sa1
```

8.3.52 pim hello-option dr-priority

Function

The **pim hello-option dr-priority** command sets the priority for the PIM interface that is elected as DR.

The **undo pim hello-option dr-priority** command restores the default value of the priority.

By default, the priority for the PIM interface that is elected as DR is 1.

Format

pim hello-option dr-priority *priority*

undo pim hello-option dr-priority

Parameters

Parameter	Description	Value
priority	Specifies the priority of the PIM interface that is elected as DR. The greater the value, the higher the priority.	The value is an integer ranging from 0 to 4294967295.

Views

GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, GE sub-interface view, XGE sub-interface view, MultiGE sub-interface view, 25GE sub-interface view, 40GE sub-interface view, 100GE sub-interface view, Eth-Trunk sub-interface view, VLANIF interface view, loopback interface view, tunnel interface view, VBDIF interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On a PIM network, switches on a shared network segment are candidates for the DR. The DR is responsible for registration of local multicast sources and the joining of receivers.

The DR is elected based on the priority and the IP address. Candidates send Hello messages with their priorities, and the switch with the highest priority becomes the DR. If multiple switches have the same priority, the switch with the largest IP address becomes the DR.

If at least one switch in the network does not support Hello packets that contain the priority, the switch with the largest IP address becomes the DR.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command.

Precautions

The **pim hello-option dr-priority** command has the same function as the **hello-option dr-priority (IPv4)** command in the PIM view. By default, if the **pim hello-option dr-priority** command is not used, the value configured in the PIM view is used; otherwise, the value configured in the interface view is used.

Example

Set the priority of VLANIF100 that is elected as DR to 3.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] pim hello-option dr-priority 3
```

Set the priority of GE0/0/1 that is elected as DR to 3.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] pim hello-option dr-priority 3
```

8.3.53 pim hello-option holdtime

Function

The **pim hello-option holdtime** command sets the timeout period during which the PIM interface waits to receive the Hello message from its neighbor.

The **undo pim hello-option holdtime** command restores the default value of the timeout.

By default, the timeout period during which the PIM interface waits to receive the Hello message from its neighbor is 105 seconds.

Format

pim hello-option holdtime *interval*

undo pim hello-option holdtime

Parameters

Parameter	Description	Value
interval	Specifies the timeout period during which the PIM interface waits to receive Hello messages from its neighbor.	The value is an integer that ranges from 1 to 65535, in seconds.

Views

GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, GE sub-interface view, XGE sub-interface view, MultiGE sub-interface view, 25GE sub-interface view, 40GE sub-interface view, 100GE sub-interface view, Eth-Trunk sub-interface view, VLANIF interface view, loopback interface view, tunnel interface view, VBDIF interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On a PIM network, after the switch receives a Hello message from its PIM neighbor, it starts a timer. The timer length is the value of Holdtime in the Hello message. If the switch does not receive any Hello message from its PIM neighbor when the timer expires, it considers the neighbor invalid or unreachable.

The **pim hello-option holdtime** command sets the timeout period during which the PIM interface waits to receive the Hello message from its neighbor.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command.

Precautions

The timeout period must be greater than the interval for sending Hello messages, which is set using the **pim timer hello** command.

The **pim hello-option holdtime** command has the same function as the **hello-option holdtime (IPv4)** command in the PIM view. By default, if the **pim hello-option holdtime** command is not used, the value configured in the PIM view is used; otherwise, the value configured in the interface view is used.

Example

Set the timeout period during which VLANIF100 waits to receive Hello messages from its neighbor to 120 seconds.


```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] pim hello-option holdtime 120
```

Set the timeout period during which GE0/0/1 waits to receive Hello messages from its neighbor to 120 seconds.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] pim hello-option holdtime 120
```

8.3.54 pim hello-option lan-delay

Function

The **pim hello-option lan-delay** command sets the delay in transmitting messages in a shared network in the interface view.

The **undo pim hello-option lan-delay** command restores the default value of the delay.

By default, the delay in transmitting messages in the shared network is 500 ms.

Format

pim hello-option lan-delay *interval*

undo pim hello-option lan-delay

Parameters

Parameter	Description	Value
interval	Specifies the delay in transmitting messages in the shared network.	The value is an integer that ranges from 1 to 32767, in milliseconds.

Views

GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, GE sub-interface view, XGE sub-interface view, MultiGE sub-interface view, 25GE sub-interface view, 40GE sub-interface view, 100GE sub-interface view, Eth-Trunk sub-interface view, VLANIF interface view, loopback interface view, tunnel interface view, VBDIF interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Hello messages sent from switches carry **lan-delay** and **override-interval** values. The **lan-delay** parameter indicates the delay in transmitting messages in the LAN. If switches on the same link have different **lan-delay** values, the maximum value is used.

When a switch sends a Prune message to the upstream device in the same network segment, other switches that still request multicast data need to send a Join message to the upstream device within the override-interval period.

The value of the Prune-Pending Timer (PPT) is the sum of the **lan-delay** and **override-interval** values, and refers to the delay from the switch receiving a Prune message from the downstream interface to performing the prune action. If the switch receives a Join message from the downstream interface in PPT, the switch cancels the prune action.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command.

Precautions

This command is valid for PIM-SM and PIM-DM.

If the prune delay is set too short, the upstream switch stops forwarding multicast packets before the downstream switch overrides Prune messages of neighbors. Exercise caution when you run this command.

The function of this command in the interface view is the same as that of the **hello-option lan-delay (IPv4)** command in the PIM view. By default, if the configuration on the interface is not performed, the value configured in the PIM view is used; otherwise, the value configured in the interface view is used.

Example

Set the delay in transmitting messages to 200 ms in VLANIF100.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] pim hello-option lan-delay 200
```

Set the delay in transmitting messages to 200 ms in GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] pim hello-option lan-delay 200
```

8.3.55 pim hello-option neighbor-tracking

Function

The **pim hello-option neighbor-tracking** command enables the neighbor tracking function in the interface view.

The **undo pim hello-option neighbor-tracking** command restores the default configuration.

By default, the neighbor tracking function is not enabled.

Format

pim hello-option neighbor-tracking

undo pim hello-option neighbor-tracking

Parameters

None

Views

GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, GE sub-interface view, XGE sub-interface view, MultiGE sub-interface view, 25GE sub-interface view, 40GE sub-interface view, 100GE sub-interface view, Eth-Trunk sub-interface view, VLANIF interface view, loopback interface view, tunnel interface view, VBDIF interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When sending a Hello message, the switch generates a Generation ID and encapsulates it into the message. The Generation ID changes only when the status of the switch changes. In this case, the neighboring device detects the Generation ID change after receiving the Hello message and immediately sends a Join message to the switch to update the neighbor relationship. If multiple devices on the shared network segment prepare to send Join messages to the same upstream PIM neighbor, only one device is allowed to send the Join message. After other devices detect the Join message, they do not send Join messages to the upstream neighbor. This means that the upstream neighbor cannot update neighbor relationships with downstream devices after a Generation ID change.

After the neighbor tracking function is enabled, when the device detects Join messages from other devices, the device still sends the Join messages to the same upstream PIM neighbor.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command.

Precautions

This command is valid for only PIM-SM.

Neighbor tracking can be implemented only when all devices on the shared network segment have this function enabled.

The **pim hello-option neighbor-tracking** command has the same function as the **hello-option neighbor-tracking (IPv4)** command in the PIM view. By default, if

the **pim hello-option neighbor-tracking** command is not used, the configuration in the PIM view takes effect; otherwise, the configuration in the interface view takes effect.

Example

Enable the neighbor tracking function on VLANIF100.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] pim hello-option neighbor-tracking
```

Enable the neighbor tracking function on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] pim hello-option neighbor-tracking
```

8.3.56 pim hello-option override-interval

Function

The **pim hello-option override-interval** command sets the interval carried in Hello messages for overriding the prune action on the interface.

The **undo pim hello-option override-interval** command, restores the default configuration.

By default, the interval carried in Hello messages for overriding the prune action on the interface is 2500 milliseconds.

Format

pim hello-option override-interval *interval*

undo pim hello-option override-interval

Parameters

Parameter	Description	Value
interval	Specifies the interval of overriding the prune action.	The value is an integer that ranges from 1 to 65535, in milliseconds.

Views

GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, GE sub-interface view, XGE sub-interface view, MultiGE sub-interface view, 25GE sub-interface view, 40GE sub-interface view, 100GE sub-interface view, Eth-Trunk sub-interface view, VLANIF interface view, loopback interface view, tunnel interface view, VBDIF interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Hello messages sent from switches carry **lan-delay** and **override-interval** parameters. The **override-interval** parameter indicates the period during which a downstream switch can override the prune action.

When a switch sends a Prune message to the upstream device in the same network segment, other switches that still request multicast data need to send a Join message to the upstream device within the override-interval period.

When a device has only one PIM neighbor on a link and receives a Prune message from the neighbor, the device immediately deletes the downstream interface of the multicast routing entry. If a device has two or more PIM neighbors on a link and the **override-interval** values in the messages sent from the two neighbors are different, the largest **override-interval** value takes effect.

The value of Prune-Pending Timer (PPT) is the sum of **lan-delay** and **override-interval** values. When receiving a Prune message from a downstream interface, the switch does not perform the prune action until the PPT times out. If the switch receives a Join message from the downstream interface in PPT, the interface cancels the Prune action.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command.

Configuration Impact

If you run the **pim hello-option override-interval** command multiple times, only the latest configuration takes effect.

Precautions

This command is valid for PIM-SM and PIM-DM.

The **pim hello-option override-interval** command has the same function as the **hello-option override-interval (IPv4)** command in the PIM view. By default, if the **pim hello-option override-interval** command is not used, the value configured in the PIM view is used; otherwise, the value configured in the interface view is used.

Example

Set the interval for overriding the prune action in Hello messages to 2000 ms in VLANIF100.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] pim hello-option override-interval 2000
```

Set the interval for overriding the prune action in Hello messages to 2000 ms in GE0/0/1.


```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] pim hello-option override-interval 2000
```

8.3.57 pim holdtime assert

Function

The **pim holdtime assert** command sets the timeout period during which a PIM interface keeps the Assert state.

The **undo pim holdtime assert** command restores the default value of the timeout.

By default, the timeout period during which a PIM interface keeps the Assert state is 180 seconds.

Format

pim holdtime assert *interval*

undo pim holdtime assert

Parameters

Parameter	Description	Value
interval	Specifies the timeout period during which a PIM interface keeps the Assert state.	The value is an integer that ranges from 7 to 65535, in seconds.

Views

GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, GE sub-interface view, XGE sub-interface view, MultiGE sub-interface view, 25GE sub-interface view, 40GE sub-interface view, 100GE sub-interface view, Eth-Trunk sub-interface view, VLANIF interface view, loopback interface view, tunnel interface view, VBDIF interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On the shared network segment connected to multiple PIM devices, if the same multicast packets reach these PIM devices and pass the RPF check, multiple copies of the same multicast packets are forwarded to this network segment. In this situation, these PIM devices need to initiate the assert mechanism. The device that

wins assert election is responsible for multicast forwarding on the shared network segment. Other devices suppress multicast data forwarding and retain the Assert state for a period of time. After the timer for a PIM interface in the Assert state expires, devices that failed the previous election triggers a new round of election.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command.

Precautions

The **pim holdtime assert** command has the same function as the **holdtime assert (IPv4)** command in the PIM view. By default, if the **pim holdtime assert** command is not used, the value configured in the PIM view is used; otherwise, the value configured in the interface view is used.

Example

Set the timeout period for the interface VLANIF100 to keep the Assert state to 100s.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] pim holdtime assert 100
```

Set the timeout period for the interface GE0/0/1 to keep the Assert state to 100s.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] pim holdtime assert 100
```

8.3.58 pim holdtime join-prune

Function

The **pim holdtime join-prune** command sets the holdtime in a Join/Prune message sent by the PIM interface.

The **undo pim holdtime join-prune** command restores the default value of the holdtime.

By default, the holdtime in a Join/Prune message sent by the PIM interface is 210 seconds.

Format

pim holdtime join-prune *interval*

undo pim holdtime join-prune

Parameters

Parameter	Description	Value
interval	Specifies the value of holdtime in a Join/Prune message sent by the PIM interface.	The value is an integer that ranges from 1 to 65535, in seconds.

Views

GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, GE sub-interface view, XGE sub-interface view, MultiGE sub-interface view, 25GE sub-interface view, 40GE sub-interface view, 100GE sub-interface view, Eth-Trunk sub-interface view, VLANIF interface view, loopback interface view, tunnel interface view, VBDIF interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After receiving a Join/Prune message from the downstream device, the switch starts the holdtime timer. If the switch does not receive subsequent Join/Prune messages from the downstream device within the holdtime interval, the switch suppresses forwarding of Join/Prune messages carrying group join information on the downstream interface in the group. If Join/Prune messages carry group prune information, the downstream interface is restored.

The **pim holdtime join-prune** command sets the holdtime interval for Join/Prune messages.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command.

Precautions

This command is valid for PIM-SM and PIM-DM.

The holdtime of Join/Prune messages must be larger than the interval for sending Join/Prune messages and is generally 3.5 times the interval for sending Join/Prune messages.

The **pim holdtime join-prune** command has the same function as the **holdtime join-prune (IPv4)** command in the PIM view. By default, if the **pim holdtime join-prune** command is not used, the value configured in the PIM view is used; otherwise, the value configured in the interface view is used.

Example

Set the holdtime in a Join/Prune message sent by the interface VLANIF100 to 280 seconds.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] pim holdtime join-prune 280
```

Set the holdtime in a Join/Prune message sent by the interface GE0/0/1 to 280 seconds.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] pim holdtime join-prune 280
```

8.3.59 pim ipsec sa

Function

The **pim ipsec sa** command specifies an IPSec SA used for encrypting and authenticating PIM messages sent and received on an interface.

The **undo pim ipsec sa** command deletes the IPSec SA used for encrypting and authenticating PIM messages sent and received on an interface.

By default, no IPSec SA is specified for encrypting and authenticating PIM messages on an interface.

Format

pim ipsec sa *sa-name*

undo pim ipsec sa

Parameters

Parameter	Description	Value
sa-name	Specifies the name of the SA used on an interface.	The value is an existing SA name.

Views

GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, GE sub-interface view, XGE sub-interface view, MultiGE sub-interface view, 25GE sub-interface view, 40GE sub-interface view, 100GE sub-interface view, Eth-Trunk sub-interface view, VLANIF interface view, loopback interface view, tunnel interface view, VBDIF interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On an IPv4 multicast network, if multicast devices are attacked by forged PIM messages, multicast data forwarding between multicast devices will be interrupted. To protect multicast devices against such attacks, configure PIM IPSec on some interfaces to authenticate PIM messages sent and received on these interfaces.

Prerequisites

- IP multicast routing has been enabled using the **multicast routing-enable** command.
- Basic IPSec functions have been configured.

Precautions

If you run both this command and the **pim hello ipsec sa** command on an interface, the last configured one takes effect.

This command has the same function as the **ipsec sa (IPv4)** command used in the PIM view, except for the effective scope. The configuration in the interface view takes precedence over the configuration in the PIM view. If SAs are specified in both the interface view and PIM view, the specified interface uses the SA configured in the interface view. If no SA is specified on an interface, the interface uses the SA specified in the PIM view.

Example

Configure the device to encrypt and authenticate PIM messages sent and received on VLANIF100 using the PIM IPSec SA named **sa1**. (This SA has been created.)

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] pim ipsec sa sa1
```

Configure the device to encrypt and authenticate PIM messages sent and received on GE0/0/1 using the PIM IPSec SA named **sa1**. (This SA has been created.)

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] pim ipsec sa sa1
```

8.3.60 pim join-policy

Function

The **pim join-policy** command enables the system to filter join information in Join/Prune messages.

The **undo pim join-policy** command restores the default setting.

By default, join information in Join/Prune message is not filtered.

Format

pim join-policy { **asm** { *basic-acl-number* } | **ssm** { *advanced-acl-number* } | *advanced-acl-number* }

undo pim join-policy [**asm** | **ssm**]

Parameters

Parameter	Description	Value
asm	Filters join information, with the group address in the ASM group address range.	-
basic-acl-number	Specifies the basic ACL number.	The value is an integer that ranges from 2000 to 2999.
ssm	Filters join messages, with the group addresses within the SSM group address range and specified source address.	-
advanced-acl-number	Specifies the advanced ACL number.	The value is an integer that ranges from 3000 to 3999.

Views

GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, GE sub-interface view, XGE sub-interface view, MultiGE sub-interface view, 25GE sub-interface view, 40GE sub-interface view, 100GE sub-interface view, Eth-Trunk sub-interface view, VLANIF interface view, loopback interface view, tunnel interface view, VBDIF interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To prevent unauthorized users from joining multicast groups on a PIM-SM network by filtering join information in Join/Prune messages, run the **pim join-policy** command.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command.

Configuration Impact

The **pim join-policy** command is valid for only PIM-SM.

The **pim join-policy** command and the **acl** command are used together.

- If **asm** is specified, you can set the multicast group address range of join information in the basic ACL view by specifying the **source** parameter in the **rule** command.
- If **ssm** is specified, you can set the source address range and multicast group address range of join information in the advanced ACL view by specifying the **source** parameter and **destination** parameter in the **rule** command.

Example

Configure VLANIF100 to accept the join information with the group address in the range of 225.1.0.0/16.

```
<HUAWEI> system-view
[HUAWEI] acl number 2001
[HUAWEI-acl-basic-2001] rule permit source 225.1.0.0 0.0.255.255
[HUAWEI-acl-basic-2001] quit
[HUAWEI] multicast routing-enable
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] pim join-policy asm 2001
```

Configure GE0/0/1 to accept the join information with the group address in the range of 225.1.0.0/16.

```
<HUAWEI> system-view
[HUAWEI] acl number 2001
[HUAWEI-acl-basic-2001] rule permit source 225.1.0.0 0.0.255.255
[HUAWEI-acl-basic-2001] quit
[HUAWEI] multicast routing-enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] pim join-policy asm 2001
```

8.3.61 pim neighbor-policy

Function

The **pim neighbor-policy** command configures a policy for filtering PIM neighbors on an interface.

The **undo pim neighbor-policy** command restores the default setting.

By default, PIM neighbors on the interface are not filtered.

Format

pim neighbor-policy *basic-acl-number*

undo pim neighbor-policy

Parameters

Parameter	Description	Value
basic-acl-number	Specifies the basic ACL number.	The value is an integer that ranges from 2000 to 2999.

Views

GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, GE sub-interface view, XGE sub-interface view, MultiGE sub-interface view, 25GE sub-interface view, 40GE sub-interface view, 100GE sub-interface view, Eth-Trunk sub-interface view, VLANIF interface view, loopback interface view, tunnel interface view, VBDIF interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To prevent unauthorized neighbors from being involved in the PIM protocol, run the **pim neighbor-policy** command to configure a policy for filtering PIM neighbors and set the address range of PIM neighbors. The switch sets up neighbor relationships with the addresses matching the filtering rules and deletes the neighbors that do not match the filtering rules.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command.

Configuration Impact

The **pim neighbor-policy** command and the **acl** command are used together. In the ACL view, set the address range of PIM neighbors by specifying **source** in the **rule** command.

Precautions

This command is valid for both PIM-DM and PIM-SM.

When configuring the neighbor filtering function on the interface, you must also configure the neighbor filtering function correspondingly on the PIM neighbor of the interface.

If a PIM device has established a neighbor relationship with the switch but its IP address is not in the configured range of valid neighbor addresses, the switch will no longer receive Hello messages from this PIM neighbor. When the holdtime of Hello messages expires, the neighbor relationship between the PIM device and the switch is terminated.

Example

Allow VLANIF100 to set up a PIM neighbor relationship with a PIM device at 10.4.4.4.

```
<HUAWEI> system-view
[HUAWEI] acl number 2001
[HUAWEI-acl-basic-2001] rule permit source 10.4.4.4 0.0.0.0
[HUAWEI-acl-basic-2001] quit
[HUAWEI] multicast routing-enable
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] pim neighbor-policy 2001
```

Allow GE0/0/1 to set up a PIM neighbor relationship with a PIM device at 10.4.4.4.

```
<HUAWEI> system-view
[HUAWEI] acl number 2001
[HUAWEI-acl-basic-2001] rule permit source 10.4.4.4 0.0.0.0
[HUAWEI-acl-basic-2001] quit
[HUAWEI] multicast routing-enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] pim neighbor-policy 2001
```

8.3.62 pim require-genid

Function

The **pim require-genid** command configures a PIM interface to reject the Hello messages without the Generation ID.

The **undo pim require-genid** command restores the default configuration.

By default, a PIM interface receives the Hello messages without the Generation ID.

Format

pim require-genid

undo pim require-genid

Parameters

None

Views

GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, GE sub-interface view, XGE sub-interface view, MultiGE sub-interface view, 25GE sub-interface view, 40GE sub-interface view, 100GE sub-interface view, Eth-Trunk sub-interface view, VLANIF interface view, loopback interface view, tunnel interface view, VBDIF interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After an interface on the switch is enabled with PIM, the switch generates a random number as the Generation ID of the Hello message. If the status of the switch is updated, the switch generates a new Generation ID. When the switch finds that the Hello message received from a PIM neighbor contains a different Generation ID, it considers that the status of the PIM neighbor has changed.

To ensure that PIM neighbors work properly, run the **pim require-genid** command to configure a PIM interface to reject the Hello messages without the Generation ID.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command.

Precautions

This command is valid for both PIM-DM and PIM-SM.

Example

Configure VLANIF100 to reject the Hello messages without the Generation ID.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] pim require-genid
```

Configure GE0/0/1 to reject the Hello messages without the Generation ID.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] pim require-genid
```

8.3.63 pim silent

Function

The **pim silent** command enables the PIM silent function on an interface.

The **undo pim silent** command cancels the PIM silent function on an interface.

By default, the PIM silent function is disabled on an interface.

Format

pim silent

undo pim silent

Parameters

None

Views

GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, GE sub-interface view, XGE sub-interface view, MultiGE sub-interface view, 25GE sub-interface view, 40GE sub-interface view, 100GE sub-interface view, Eth-Trunk sub-interface view, VLANIF interface view, loopback interface view, tunnel interface view, VBDIF interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To protect the switch against pseudo PIM Hello messages sent from malicious hosts, configure the **pim silent** command on the interface directly connected to the host network segment to set the interface to PIM silent mode. Then the interface cannot receive or forward any PIM packet, and all PIM neighbors and PIM state machines on this interface are deleted. This interface becomes the DR, but the IGMP function on the interface is not affected.

The PIM silent function applies only to the interface directly connected to a host network segment, and only one PIM switch can be connected to this network segment.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command.

Precautions

Running the **pim silent** command failed on the VLANIF interface because Layer 2 multicast querier or report-suppress is enabled for this VLAN.

If PIM BFD function is enabled on the interface, this command cannot be configured.

This command and **pim timer dr-switch-delay** command are mutually exclusive.

NOTICE

After you run this command on an interface, the interface no longer receives or sends any PIM packets and other PIM functions on the interface become invalid. Confirm your action before using this command.

If a host network segment is connected to multiple switches and PIM silent is enabled on multiple interfaces, all these interfaces become static DRs. This causes multicast forwarding failures.

Example

Configure the PIM silent function on VLANIF100.


```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] pim silent
```

Configure the PIM silent function on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] pim silent
```

8.3.64 pim sm

Function

The **pim sm** command enables PIM-SM on an interface.

The **undo pim sm** command restores the default configuration.

By default, PIM-SM is disabled on an interface.

Format

pim sm

undo pim sm

Parameters

None

Views

GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, GE sub-interface view, XGE sub-interface view, MultiGE sub-interface view, 25GE sub-interface view, 40GE sub-interface view, 100GE sub-interface view, Eth-Trunk sub-interface view, VLANIF interface view, loopback interface view, tunnel interface view, VBDIF interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

With PIM-SM enabled on interfaces, switches can set up PIM neighbor relationships and process protocol packets received from PIM neighbors.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command.

Precautions

- PIM-DM and PIM-SM cannot be enabled simultaneously on interfaces bound to the same VPN instance or public network instance.
- If PIM-SM and IGMP need to be enabled on the same interface, enable PIM-SM, and then enable IGMP.
- Running the **pim sm** command failed on the VLANIF interface because Layer 2 multicast querier or report-suppress is enabled for this VLAN.
- If both Layer 2 and Layer 3 multicast services are required in a VLAN, enable PIM on the corresponding VLANIF interface first, and then enable IGMP snooping in the VLAN. If IGMP snooping is enabled in the VLAN first, PIM cannot be enabled on the VLANIF interface.
- In versions earlier than V200R022C10, VBDIF interfaces cannot be configured as inbound or outbound interfaces of multicast entries. In V200R022C10, VBDIF interfaces can only be configured as outbound interfaces of multicast entries, and cannot be configured as inbound interfaces. In V200R023C00 and later versions, VBDIF interfaces can be configured as both inbound and outbound interfaces of multicast entries.
- After super VXLAN resource mode is configured using the **set vxlan resource super-mode** command, a maximum of 12,288 VBDIF interfaces can be configured as inbound interfaces of multicast entries. If the number of VBDIF interfaces to be configured as inbound interfaces exceeds the upper limit, the configuration takes effect only for the first 12,288 VBDIF interfaces.
- PIM can be configured on VBDIF interfaces. A VBDIF interface that has PIM configured can only connect the multicast source and receives, and it cannot function as a PIM interconnection interface.
- Since V200R010, the S5720-HI, S5730-HI, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6720-HI, S6730-H, S6730S-H, S6730-S, and S6730S-S support IPv4 PIM configuration on dot1q and QinQ termination sub-interfaces only when the VLAN tag to be terminated (or both inner and outer VLAN tags on the QinQ termination sub-interface) is a single VLAN ID, but not a range of VLAN IDs. Sub-interfaces running PIM can only be used as inbound interfaces of multicast streams and cannot be used as outbound interfaces. The S5720-EI, S6720-EI, S6735-S, and S6720S-EI also support IPv4 PIM command configuration on dot1q and QinQ termination sub-interfaces, but they do not support multicast traffic forwarding on these sub-interfaces.
- PIM-DM and PIM-SM cannot be configured simultaneously in a VPN instance or the public network instance. IPv4 PIM can be configured in a VPN instance, but the VPN instance cannot be bound to a physical interface that has been switched to Layer 3 mode using the **undo portswitch** command. Only the following products and versions support the IPv4 PIM multi-instance feature:
  - S5730-HI, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6720-HI, S6730-H, S6730S-H, S6730-S, and S6730S-S: all versions
  - S6700-EI and S5700-HI: V200R005C01
  - S6700-EI, S5700-HI, and S5710-HI: V200R005C02
  - S5710-HI: V200R005C03
  - S5720-EI, S5720-HI, S6720-EI, S6735-S, and S6720S-EI: V200R010 and later versions
- Secondary IP addresses does not support PIM, and the direct routes generated based on secondary IP addresses are not involved during multicast RPF check. Therefore, if the source IP address of multicast packets is on the same

network segment as the secondary IP address of a Layer 3 interface, these multicast packets received on the Layer 3 interface cannot pass the RPF check.

Example

Enable PIM-SM on VLANIF100.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] pim sm
```

Enable PIM-SM on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] pim sm
```

8.3.65 pim state-refresh-capable

Function

The **pim state-refresh-capable** command enables PIM-DM state refresh on an interface.

The **undo pim state-refresh-capable** command disables PIM-DM state refresh.

By default, PIM-DM state refresh is enabled.

Format

pim state-refresh-capable

undo pim state-refresh-capable

Parameters

None

Views

GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, GE sub-interface view, XGE sub-interface view, MultiGE sub-interface view, 25GE sub-interface view, 40GE sub-interface view, 100GE sub-interface view, Eth-Trunk sub-interface view, VLANIF interface view, loopback interface view, tunnel interface view, VBDIF interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

PIM-DM state refresh is implemented by periodically sending State-Refresh messages in the network. After receiving a State-Refresh message, the switch in the pruned state resets the prune-status timer, preventing the downstream interface from forwarding packets.

After PIM-DM state refresh is disabled on an interface, the interface starts to forward multicast data when the prune timer expires. The downstream routers that do not want to receive the data send Prune messages. The process repeats, wasting a lot of network resources. Enabling PIM-DM state refresh can reduce traffic on the network.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command in the public network instance or VPN instance.

Precautions

This command is valid for only PIM-DM.

Example

Disable PIM-DM state refresh on VLANIF100.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] undo pim state-refresh-capable
```

Disable PIM-DM state refresh on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] undo pim state-refresh-capable
```

8.3.66 pim timer dr-switch-delay

Function

The **pim timer dr-switch-delay** command enables PIM DR switching delay and configures the delay on an interface. When the interface changed from a DR to a non-DR, the interface continues to forward data before the delay expires.

The **undo pim timer dr-switch-delay** command disables PIM DR switching delay on the interface.

By default, when the interface changes from a DR to a non-DR, the interface stops forwarding data immediately.

Format

pim timer dr-switch-delay *interval*

undo pim timer dr-switch-delay

Parameters

Parameter	Description	Value
interval	Specifies the delay.	The value is an integer that ranges from 10 to 3600, in seconds.

Views

GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, GE sub-interface view, XGE sub-interface view, MultiGE sub-interface view, 25GE sub-interface view, 40GE sub-interface view, 100GE sub-interface view, Eth-Trunk sub-interface view, VLANIF interface view, loopback interface view, tunnel interface view, VBDIF interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If the DR on a shared network segment becomes the non-DR, original multicast forwarding entries will be deleted immediately, causing multicast data interruption in a short time. To solve the problem, set the DR switching delay. Original multicast forwarding entries still take effect until the delay is reached.

After a new PIM neighbor joins, the outbound interface may not function as a DR any more; however, within the switching delay or before the new DR takes effect to forward multicast traffic, the original outbound interface still has the DR function and continues to forward multicast data. In this manner, non-stop multicast traffic forwarding is ensured during DR switchover.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command.

Precautions

This command is valid for only PIM-SM.

This command and **pim silent** command are mutually exclusive.

Example

Enable PIM DR switching delay on VLANIF100 and set the delay to 20 seconds.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] pim timer dr-switch-delay 20
```

Enable PIM DR switching delay on GE0/0/1 and set the delay to 20 seconds.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
```



```
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] pim timer dr-switch-delay 20
```

8.3.67 pim timer graft-retry

Function

The **pim timer graft-retry** command sets the interval for retransmitting Graft messages on an interface.

The **undo pim timer graft-retry** command restores the default value of the interval.

By default, the interval for retransmitting Graft messages on an interface is 3 seconds.

Format

pim timer graft-retry *interval*

undo pim timer graft-retry

Parameters

Parameter	Description	Value
interval	Specifies the interval of retransmitting Graft messages.	The value is an integer that ranges from 1 to 65535, in seconds.

Views

GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, GE sub-interface view, XGE sub-interface view, MultiGE sub-interface view, 25GE sub-interface view, 40GE sub-interface view, 100GE sub-interface view, Eth-Trunk sub-interface view, VLANIF interface view, loopback interface view, tunnel interface view, VBDIF interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In PIM-DM mode, when a member joins a pruned group, the switch sends a Graft message and waits to receive an ACK message from the upstream switch. If the downstream switch does not receive the ACK message in the period configured through the command, the switch resends the Graft message until the switch receives the ACK message from the upstream switch.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command in the public network instance or VPN instance.

Precautions

This command is valid for only PIM-DM.

Example

Set the interval for retransmitting Graft messages to 80s on the interface VLANIF100.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] pim timer graft-retry 80
```

Set the interval for retransmitting Graft messages to 80s on the interface GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] pim timer graft-retry 80
```

8.3.68 pim timer hello

Function

The **pim timer hello** command sets the interval for sending Hello messages on an interface.

The **undo pim timer hello** command restores the default value of the interval.

By default, the interval for sending Hello messages on an interface is 30 seconds.

Format

pim timer hello *interval*

undo pim timer hello

Parameters

Parameter	Description	Value
interval	Specifies the interval for sending Hello messages.	The value is an integer that ranges from 1 to 18000, in seconds.

Views

GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, GE sub-interface view, XGE sub-interface view, MultiGE sub-interface view, 25GE sub-interface view, 40GE sub-interface view, 100GE sub-interface view, Eth-Trunk sub-interface view, VLANIF interface view, loopback interface view, tunnel interface view, VBDIF interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

PIM devices periodically send Hello messages to maintain PIM neighbor relationships. You can run the **pim timer hello** command to set the interval for sending Hello messages.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command.

Precautions

This command is valid for both PIM-DM and PIM-SM.

The interval for sending Hello messages must be shorter than the timeout period of PIM neighbors, which is set using the **hello-option holdtime (IPv4)** command.

The configuration is the same as the **timer hello (IPv4)** command in the PIM view but takes precedence over the command used in the PIM view. The value configured in the PIM view is used if no value is configured on the interface.

Example

Set the interval for sending Hello messages to 40 seconds on VLANIF100.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] pim timer hello 40
```

Set the interval for sending Hello messages to 40 seconds on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] pim timer hello 40
```

8.3.69 pim timer join-prune

Function

The **pim timer join-prune** command sets the interval for periodically sending Join/Prune messages to the upstream device.

The **undo pim timer join-prune** command restores the default interval.

By default, the interval for periodically sending Join/Prune messages to the upstream device is 60 seconds.

Format

pim timer join-prune *interval*

undo pim timer join-prune

Parameters

Parameter	Description	Value
interval	Specifies the interval at which Join/Prune messages are sent.	The value is an integer that ranges from 1 to 18000, in seconds.

Views

GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, GE sub-interface view, XGE sub-interface view, MultiGE sub-interface view, 25GE sub-interface view, 40GE sub-interface view, 100GE sub-interface view, Eth-Trunk sub-interface view, VLANIF interface view, loopback interface view, tunnel interface view, VBDIF interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The device sends join information to the upstream device, requesting the upstream device to forward multicast data. The device sends prune information to the upstream device, requesting the upstream device to stop forwarding multicast data. Join information and prune information are encapsulated in Join/Prune messages. The device periodically sends Join/Prune messages to the upstream device to update the forwarding status.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command.

Precautions

This command is valid only for PIM-SM.

The interval configured through this command must be shorter than the interval configured through the **pim holdtime join-prune** command. The interval at which Join or Prune messages are sent must be shorter than the holdtime carried in Join/Prune messages.

The configuration is the same as that of the **timer join-prune (IPv4)** command in the PIM view. The system prefers the configuration in the interface view. The value configured in the PIM view is used if no value is configured on the interface.

Example

Set the interval for sending Join or Prune messages to 80 seconds on VLANIF100.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] pim timer join-prune 80
```

Set the interval for sending Join or Prune messages to 80 seconds on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] pim timer join-prune 80
```

8.3.70 pim triggered-hello-delay

Function

The **pim triggered-hello-delay** command sets the maximum delay for triggering Hello messages.

The **undo pim triggered-hello-delay** command restores the default maximum delay.

By default, the maximum delay for triggering Hello messages is 5 seconds.

Format

pim triggered-hello-delay *interval*

undo pim triggered-hello-delay

Parameters

Parameter	Description	Value
interval	Specifies the maximum delay for triggering Hello messages.	The value is an integer that ranges from 1 to 5, in seconds.

Views

GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, GE sub-interface view, XGE sub-interface view, MultiGE sub-interface view, 25GE sub-interface view, 40GE sub-interface view, 100GE sub-interface view, Eth-Trunk sub-interface view, VLANIF interface view, loopback interface view, tunnel interface view, VBDIF interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Conflicts will occur if multiple PIM devices send Hello message at the same time. To avoid such conflicts, when a PIM device detects Hello messages on the network, it waits for a random delay that is smaller than the value configured using this command before sending a Hello message.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command.

Example

Set the maximum delay for triggering the Hello message to 3 seconds on VLANIF100.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] pim triggered-hello-delay 3
```

Set the maximum delay for triggering the Hello message to 3 seconds on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] pim triggered-hello-delay 3
```

8.3.71 probe-interval (IPv4)

Function

The **probe-interval** command sets the interval for a switch to send Probe messages (null Register message) to the RP.

The **undo probe-interval** command restores the default value of the interval.

By default, the interval for a switch to send Probe messages to the RP is 5 seconds.

Format

probe-interval *interval*

undo probe-interval

Parameters

Parameter	Description	Value
interval	Specifies the interval for sending Probe messages to RP.	The value is an integer that ranges from 1 to 1799, in seconds.

Views

PIM view of public network instance or PIM view of VPN instance

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When receiving a Register-Stop message sent by the RP, the DR at the source side stops sending Register messages and enters the register suppression state.

During the register suppression, the DR at the source side sends Probe messages to notify the RP that the multicast source is still in the Active state. After the register suppression times out, the DR at the source side starts to send Register messages.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command.

Precautions

This command is valid for only PIM-SM.

The interval set using the **probe-interval** command must be less than half the interval set using the **register-suppression-timeout (IPv4)** command.

Example

In the PIM view of public network instance, set the interval for sending Probe messages to RP to 6 seconds.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] pim
[HUAWEI-pim] probe-interval 6
```

8.3.72 register-header-checksum

Function

The **register-header-checksum** command configures devices to calculate the checksum based on the header of a Register message only.

The **undo register-header-checksum** command restores the default configuration.

By default, the checksum is calculated according to all the contents of a Register message.

Format

register-header-checksum

undo register-header-checksum

Parameters

None

Views

PIM view of public network instance or PIM view of VPN instance

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

By default, the source's DR calculates the checksum based on all fields in a Register message. After the **register-header-checksum** command is executed, the source's DR calculates the checksum based on the Register message header. This shortens the checksum calculation time and improves efficiency of encapsulating multicast data in Register messages.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command.

Precautions

This command is valid for only PIM-SM.

Example

Calculate the checksum based only on the header of a Register message PIM view of public network instance.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] pim
[HUAWEI-pim] register-header-checksum
```

8.3.73 register-policy (IPv4)

Function

The **register-policy** command sets the rules used by an RP to filter Register messages.

The **undo register-policy** command restores the default setting.

By default, the rules for filtering Register messages are not configured.

Format

register-policy *advanced-acl-number*

undo register-policy

Parameters

Parameter	Description	Value
advanced-acl-number	Specifies the number of the advanced ACL that defines the rules for filtering packets based on source addresses or group addresses.	The value is an integer that ranges from 3000 to 3999.

Views

PIM view of public network instance or PIM view of VPN instance

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To prevent the attack of invalid Register messages, you can configure devices to receive or deny Register messages according to the packet filtering rules.

If the (S, G) entry contained in a Register message does not pass the filtering of the ACL or the ACL does not filter the entry, RP discards the Register message. The multicast source cannot register with the RP.

If *advanced-acl-number* is set in the **register-policy** command but the corresponding ACL is not defined, the RP discards all Register messages. The RP cannot register with any multicast source.

The **register-policy** command and the **acl** command are used together. In the ACL view, you can set the multicast source address range by specifying the **source** parameter in the **rule** command, and set the multicast group address range by specifying the **destination** parameter in the **rule** command.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command.

Precautions

NOTICE

When the **register-policy** command is used on the RP, only Register messages matching the rule of the ACL are received by the RP. If an undefined ACL is specified, the RP denies all Register messages.

This command is valid for only PIM-SM.

The **register-policy** command takes effect for only subsequently received Register messages. The multicast entries that have been registered successfully are not deleted and can still be used for multicast data forwarding.

Example

Configure the RP to receive Register packets sent by the source on network segment 10.10.0.0/16 to group 225.1.0.0/16.

```
<HUAWEI> system-view
[HUAWEI] acl number 3000
[HUAWEI-acl-adv-3000] rule permit ip source 10.10.0.0 0.0.255.255 destination 225.1.0.0 0.0.255.255
[HUAWEI-acl-adv-3000] quit
[HUAWEI] multicast routing-enable
[HUAWEI] pim
[HUAWEI-pim] register-policy 3000
```

8.3.74 register-source

Function

The **register-source** command specifies the source address used by the source's DR to send Register messages.

The **undo register-source** command restores the default setting.

By default, the source address used by the source's DR to send Register messages is not specified.

Format

register-source *interface-type interface-number*

undo register-source

Parameters

Parameter	Description	Value
interface-type interface-number	Specifies the type and number of the source's DR.	-

Views

PIM view of public network instance or PIM view of VPN instance

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the source IP address for sending Register messages is no longer the only IP address in the network for the RP router or the source IP address is filtered out,

errors occur in the registration process and extra traffic occupies bandwidth on the network. In this case, use the **register-source** command to specify an appropriate interface as the source IP address for sending Register messages. Using the loopback address of the source's DR as the source IP address is recommended.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command.

Before specifying the source IP address for sending Register messages, enable PIM-SM.

Precautions

The command is effective only when the specified interface is in Up state.

Example

In the PIM view of public network instance, specify the IP address of loopback 0 as the source IP address for source's DR to send Register messages.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] pim
[HUAWEI-pim] register-source loopback 0
```

8.3.75 register-suppression-timeout (IPv4)

Function

The **register-suppression-timeout** command sets the timeout period during which a switch keeps the register suppression state.

The **undo register-suppression-timeout** command restores the default timeout period.

By default, a switch keeps the register suppression state for 60 seconds.

Format

register-suppression-timeout *interval*

undo register-suppression-timeout

Parameters

Parameter	Description	Value
interval	Specifies the timeout period during which the switch keeps the register suppression state.	The value is an integer that ranges from 11 to 3600, in seconds.

Views

PIM view of public network instance or PIM view of VPN instance

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After receiving a Register-Stop message from the RP, the switch immediately stops sending Register messages and enters the register suppression state.

The **register-suppression-timeout** command determines how long the switch keeps the register suppression state. When the timeout period expires, the switch (source DR) starts to send Register messages to the RP.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command.

Configuration Impact

If the timeout period is too short, the RP receives burst multicast data more frequently. If the timeout period is too long, there will be a long delay for new receivers to join a group after an (S, G) entry on the RP times out.

You can use the **probe-interval (IPv4)** command to configure the switch to send null Register messages before the suppression timer times out. This configuration reduces burst Register messages and shortens the timeout period to reduce the delay for a new receiver to join a group.

Precautions

This command is valid only for PIM-SM.

The interval set by the **register-suppression-timeout** command must be larger than two times the interval set by the **probe-interval (IPv4)** command.

Example

In the PIM view of public network instance, set the timeout period during which the switch keeps the register suppression state to 70 seconds.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] pim
[HUAWEI-pim] register-suppression-timeout 70
```

8.3.76 reset pim control-message counters

Function

The **reset pim control-message counters** command resets the statistics about PIM Control messages.

Format

reset pim [**vpn-instance** *vpn-instance-name* | **all-instance**] **control-message counters** [**interface** *interface-type interface-number*]

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Specifies a VPN instance. *vpn-instance-name* specifies the name of the VPN instance.	The value must be an existing VPN instance name.
all-instance	Specifies all the instances.	-
interface *interface-type interface-number*	Specifies the name and the number of an interface. It is used to reset the statistics about PIM control messages on a specified interface.	-

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

If a PIM-enabled interface on the switch has been forwarding multicast packets for a long period of time, the switch stores statistics on a large number of control messages. You can run this command to reset statistics on control messages.

Example

Reset the statistics about PIM control messages on all interfaces in the public network instance.

```
<HUAWEI> reset pim control-message counters
```

Reset the statistics about PIM control messages on VLANIF100 in the public network instance.

```
<HUAWEI> reset pim control-message counters interface vlanif 100
```

8.3.77 reset pim routing-table

Function

The **reset pim routing-table** command resets PIM status of a specified downstream interface in a specified PIM routing entry.

Format

reset pim [**vpn-instance** *vpn-instance-name*] **routing-table group** *group-address* **mask** { *group-mask-length* | *group-mask* } **source** *source-address* **interface** *interface-type interface-number*

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Specifies the name of a VPN instance.	The value must be an existing VPN instance name.
group *group-address*	Specifies the multicast group address of a PIM routing entry.	The value ranges from 224.0.1.0 to 239.255.255.255, in dotted decimal notation.
mask *group-mask-length*	Specifies the mask length of a multicast group address.	The value is an integer that ranges from 4 to 32.
mask *group-mask*	Specifies the mask of a multicast group address.	It is in dotted decimal notation.
source *source-address*	Specifies the source address of a PIM routing entry.	The value is in dotted decimal notation. If a (*, G) entry is specified, the source address is 0.0.0.0.
interface *interface-type interface-number*	Specifies the type and number of an interface.	-

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

The **reset pim routing-table** command resets PIM status of a specified downstream interface in a specified PIM routing entry.

Configuration Impact

This command can reset the PIM status of the specified interface in a specified PIM routing entry. It cannot reset the IGMP state and static group memberships on a specified interface.

Precautions

This command is valid only for PIM-SM.

NOTICE

Resetting PIM status of downstream interfaces can trigger transmission of Join/Prune messages, which causes multicast service interruption.

Example

In the public network instance, reset PIM status of downstream interface VLANIF100 of (10.1.1.1, 225.0.0.1).

```
<HUAWEI> reset pim routing-table group 225.0.0.1 mask 255.255.255.0 source 10.1.1.1 interface vlanif 100
```

8.3.78 source-lifetime (IPv4)

Function

The **source-lifetime** command specifies the timeout period of (S, G) or (*, G) entries on the switch.

The **undo source-lifetime** command restores the default value of the timeout period.

By default, the timeout period is 210 seconds.

Format

source-lifetime { *interval* | **infinity** } [**group-policy** *acl-number*]

undo source-lifetime

undo source-lifetime { *interval* | **infinity** } [**group-policy** *acl-number*]

Parameters

Parameter	Description	Value
interval	Specifies the timeout period of (S, G) or (*, G) entries on the switch.	The value is an integer that ranges from 60 to 65535, in seconds.
infinity	Indicates that (S, G) entries on the switch will never age out.	-
group-policy	Specifies a group policy to determine to which the configured timeout period takes effect.	-
acl-number	Specifies the number of a basic or advanced ACL.	The value is an integer that ranges from 2000 to 3999.

Views

PIM view of public network instance or PIM view of VPN instance

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A switch starts a timer for each (S, G) or (*, G) entry. The **source-lifetime** command sets the timer value. After receiving a multicast packet from S, the interface resets the timer. If the timer times out, the (S, G) or (*, G) entry is considered invalid.

- If you configure **source-lifetime** *interval*, the configured timeout period applies to all (S, G) entries.
- If you configure **source-lifetime** *interval* { **group-policy** *acl-number* }:
  - If you specify a basic ACL number in the command, the configured timeout period applies to the (S, G) entries in which the source addresses are permitted by the specified ACL.
  - If you specify an advanced ACL number in the command, the configured timeout period applies to the (S, G) entries in which the source and group addresses are permitted by the specified ACL.
  - If you specify an advanced ACL name in the command, the configured timeout period applies to the (S, G) entries in which the source and group addresses are permitted by the specified ACL.
- If you configure **source-lifetime infinity**, all (S, G) entries will never age out.
- If you configure **source-lifetime infinity** { **group-policy** *acl-number* }:
  - If you specify a basic ACL number in the command, the (S, G) entries in which the source addresses are permitted by the specified ACL will never age out.
  - If you specify an advanced ACL number in the command, the (S, G) entries in which the source and group addresses are permitted by the specified ACL will never age out.
  - If you specify an advanced ACL name in the command, the (S, G) entries in which the source and group addresses are permitted by the specified ACL will never age out.

If you run this command multiple times for the same range of multicast forwarding entries and specify *interval* and **infinity** respectively in the commands, **infinity** takes precedence over *interval*.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command.

Precautions

This command is valid for both PIM-DM and PIM-SM.

Example

In the PIM view of public network instance, set the timeout period of an (S, G) or (*, G) entry of the switch to 200 seconds.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] pim
[HUAWEI-pim] source-lifetime 200
```

8.3.79 source-policy (IPv4)

Function

The **source-policy** command configures a policy to filter received multicast data packets based on source addresses or source-group addresses.

The **undo source-policy** command deletes the configuration.

By default, a switch does not filter received multicast data packets based on source addresses or source-group addresses.

Format

source-policy *acl-number*

undo source-policy

Parameters

Parameter	Description	Value
acl-number	Specifies number of the basic or advanced ACL.	The value is an integer that ranges from 2000 to 3999.

Views

PIM view of public network instance or PIM view of VPN instance

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To prevent unauthorized source information from being advertised on the PIM network, run the **source-policy** command to configure the switch to filter received multicast data packets based on source addresses or source/group addresses.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command.

Configuration Impact

If a basic ACL is referenced in the policy, multicast data packets that do not match the specified source addresses are discarded.

If an advanced AC is referenced in the policy, multicast data packets that do not match the specified group-source addresses are discarded.

Precautions

This command is valid for both PIM-DM and PIM-SM.

Example

In the PIM view of public network instance, configure the switch to receive multicast data packets with the source address of 10.10.1.2 and to discard those with the source address of 10.10.1.1.

```
<HUAWEI> system-view
[HUAWEI] acl number 2001
[HUAWEI-acl-basic-2001] rule permit source 10.10.1.2 0
[HUAWEI-acl-basic-2001] rule deny source 10.10.1.1 0
[HUAWEI-acl-basic-2001] quit
[HUAWEI] multicast routing-enable
[HUAWEI] pim
[HUAWEI-pim] source-policy 2001
```

8.3.80 spt-switch-threshold (IPv4)

Function

The **spt-switch-threshold** command sets the rate threshold of the multicast packets when the DR at the member side joins the SPT.

The **undo spt-switch-threshold** command restores the default value.

By default, the system performs SPT switchover on receiving the first multicast data packet through the RPT.

Format

spt-switch-threshold { *traffic-rate* | **infinity** } [**group-policy** *basic-acl-number* [**order** *order-value*]]

undo spt-switch-threshold [*traffic-rate* | **infinity**] [**group-policy***basic-acl-number*]

Parameters

Parameter	Description	Value
traffic-rate	Specifies the threshold rate for the switchover from the RPT to the SPT. **NOTE** Setting this parameter may affect operation of multicast services. You are advised to use the default triggering condition. That is, an SPT switchover is triggered immediately after the first multicast data packet is received from the RPT. The default triggering condition can reduce the number of multicast packets forwarded on the RPT.	The value is an integer that ranges from 1 to 4194304, in kbit/s.
infinity	Indicates that the SPT switchover is never triggered.	-
basic-acl-number	Specifies an entry of the group-policy list. It works with the multicast group that matches **group-policy** *basic-acl-number* to enable the threshold. *basic-acl-number* specifies the number of the basic ACL that defines the range of multicast groups.	If the parameter is not set, the threshold is applied to all multicast groups. The value ranges from 2000 to 2999.
order *order-value*	Adjusts the order of the ACLs in the group-policy list.	If a group matches multiple ACLs, the threshold is selected in the order specified by *order-value*. *order-value* specifies the updated number. It is an integer. The value is any value other than original one in the current group-policy list. If the parameter is not set, the order of the ACLs in the group-policy list does not change.

Views

PIM view of public network instance or PIM view of VPN instance

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The source's DR encapsulates multicast packets in a Register message, and then transmits the unicast Register message to the RP. Then, the RP decapsulates the Register message and forwards the multicast packets to the receivers along the RPT. By default, when the RP or receiver's DR receives the first multicast packet, it initiates an SPT switchover to the source.

After the **spt-switch-threshold** command is executed on the receiver's DR, the receiver's DR periodically checks the forwarding rate of multicast packets. When the forwarding rate exceeds the threshold, the receiver's DR sends a Join messages to the source, triggering the SPT switchover.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command.

Precautions

This command is valid to all devices that may function as the DR at the member side, but is invalid to RPs.

This command is valid for only PIM-SM.

If this command is used several times for the same group, the first matching command takes effect.

Example

In the PIM view of public network instance, set the traffic rate threshold to 4 kbit/s. If the transmission rate of packets from the source to the multicast group exceeds the threshold, the switch triggers an SPT switchover so that packets are forwarded along the SPT towards the source.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] pim
[HUAWEI-pim] spt-switch-threshold 4
```

In the public network instance, create a group-policy that uses ACL 2010, specify the **infinity** keyword in the command to ensure that an SPT switchover will never be triggered, and set the order of ACL 2010 in the group-policy to 1.

```
<HUAWEI> system-view
[HUAWEI] acl number 2010
[HUAWEI-acl-basic-2010] rule permit source 225.1.1.1 0
[HUAWEI-acl-basic-2010] quit
[HUAWEI] multicast routing-enable
[HUAWEI] pim
[HUAWEI-pim] spt-switch-threshold infinity group-policy 2010 order 1
```

8.3.81 ssm-policy (IPv4)

Function

The **ssm-policy** command sets the range of SSM group addresses.

The **undo ssm-policy** command restores the default configuration.

By default, the range of SSM group addresses is 232.0.0.0/8.

Format

ssm-policy *basic-acl-number*

undo ssm-policy

Parameters

Parameter	Description	Value
basic-acl-number	Specifies the number of the basic ACL that defines the range of SSM group addresses.	The value is an integer that ranges from 2000 to 2999.

Views

PIM view of public network instance or PIM view of VPN instance

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

By default, the address of an SSM group ranges from 232.0.0.0 to 232.255.255.255. You can run the **ssm-policy** command to specify the range of PIM SSM group addresses. All the PIM-SM interfaces consider that PIM SSM is enabled on all the multicast groups in the specified address range. The specified SSM group address range can be beyond 232.0.0.0/8.

You can enable SSM mode under the following conditions:

- The address of the multicast group is in the range of SSM group addresses, the network segment where the host resides runs IGMPv3, and the source address is specified in the Report message.
- The address of the multicast group is in the range of SSM group addresses, the network segment where the host resides runs IGMPv1 or IGMPv2, and the switch is configured with SSM mapping.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command.

Precautions

This command is valid for only PIM-SM.

The **ssm-policy** command and the **acl** command are used together.

- For the numbered ACL, in the ACL view, you can set the address range of SSM multicast groups by specifying the **source** parameter in the **rule** command.

- For the Named ACL, in the ACL view, when the **rule** command is used to configure a filtering rule, the filtering rule is effective only with the multicast group address range specified by the **destination** parameter and the period specified by the **time-range** parameter.

Example

In the PIM view of public network instance, set the range of PIM SSM multicast addresses to 232.1.0.0/16.

```
<HUAWEI> system-view
[HUAWEI] acl number 2000
[HUAWEI-acl-basic-2000] rule permit source 232.1.0.0 0.0.255.255
[HUAWEI-acl-basic-2000] quit
[HUAWEI] multicast routing-enable
[HUAWEI] pim
[HUAWEI-pim] ssm-policy 2000
```

8.3.82 state-refresh-interval (IPv4)

Function

The **state-refresh-interval** command sets the interval for sending PIM State-Refresh messages.

The **undo state-refresh-interval** command restores the default value of the interval.

By default, the interval for sending PIM State-Refresh messages is 60 seconds.

Format

state-refresh-interval *interval*

undo state-refresh-interval

Parameters

Parameter	Description	Value
interval	Specifies the interval for sending PIM State-Refresh messages.	The value is an integer that ranges from 1 to 255, in seconds.

Views

PIM view of public network instance or PIM view of VPN instance

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On the PIM-DM network, the device periodically sends State-Refresh messages to update the timeout interval of the prune timer on the downstream device. By doing this, the interface that has no multicast requirements retains in prune state. You can use the **state-refresh-interval** command to set the interval at which State-Refresh messages are sent.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command in the public network instance or VPN instance.

Precautions

To prevent a pruned interface from forwarding packets when the Prune status times out, the interval for sending State-Refresh messages is shorter than the period for keeping the Prune status.

You can run the **holdtime join-prune (IPv4)** command to set the period during which the device keeps the Prune status.

This command is valid for only PIM-DM.

This command takes effect only on the switch directly connected to a source.

Example

Set the interval for sending PIM State-Refresh messages to 70s in the PIM view of public network instance.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] pim
[HUAWEI-pim] state-refresh-interval 70
```

8.3.83 state-refresh-rate-limit (IPv4)

Function

The **state-refresh-rate-limit** command sets the minimum period to wait before receiving the next PIM State-Refresh message.

The **undo state-refresh-rate-limit** command restores the default value.

By default, the minimum period to wait to receive the next PIM State-Refresh message is 30 seconds.

Format

state-refresh-rate-limit *interval*

undo state-refresh-rate-limit

Parameters

Parameter	Description	Value
interval	Specifies the minimum period for waiting to receive the next PIM State-Refresh message.	The value is an integer that ranges from 1 to 65535, in seconds.

Views

PIM view of public network instance or PIM view of VPN instance

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A switch can receive multiple PIM State-Refresh messages in a short period. Some of the messages are the same. To avoid duplicate messages, you can run the **state-refresh-rate-limit** command to set the period to wait to receive the next State-Refresh message.

- Before the State-Refresh timer times out, the switch discards the received duplicate State-Refresh messages.
- After the State-Refresh timer times out, the switch can receive the next State-Refresh message.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command in the public network instance or VPN instance.

Precautions

This command is valid for only PIM-DM.

Example

Set the minimum period to wait to receive the next PIM State-Refresh message to 45s in the PIM view of public network instance.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] pim
[HUAWEI-pim] state-refresh-rate-limit 45
```

8.3.84 state-refresh-ttl (IPv4)

Function

The **state-refresh-ttl** command sets the TTL value for sending PIM State-Refresh messages.

The **undo state-refresh-ttl** command restores the default value of the TTL.

By default, the TTL value for sending PIM State-Refresh messages is 255.

Format

state-refresh-ttl *ttl-value*

undo state-refresh-ttl

Parameters

Parameter	Description	Value
ttl-value	Specifies the TTL value of the PIM State-Refresh message sent by an interface.	The value is an integer that ranges from 1 to 255.

Views

PIM view of public network instance or PIM view of VPN instance

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After receiving a State-Refresh message, a switch decreases the TTL value in the message by 1, and then sends the message to the downstream device until the value of the TTL becomes 0. If the network is small, the message is delivered in a loop. You can use the **state-refresh-ttl** command to set an appropriate TTL value depending on the scale of your network.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command in the public network instance or VPN instance.

Precautions

This command is valid for only PIM-DM.

This command takes effect only on the switch directly connected to a source.

Example

Set the TTL value for sending PIM State-Refresh messages to 45 in the PIM view of public network instance.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] pim
[HUAWEI-pim] state-refresh-ttl 45
```


8.3.85 static-rp (IPv4)

Function

The **static-rp** command configures a static RP.

The **undo static-rp** command restores the default configuration.

By default, no static RP is configured.

Format

static-rp *rp-address* [*basic-acl-number*] [**preferred**]

undo static-rp *rp-address*

Parameters

Parameter	Description	Value
rp-address	Specifies address of a static RP.	The address is in dotted decimal notation. It must be a valid unicast IP address and cannot be configured as an address of network segment 127.0.0.0/8.
basic-acl-number	Specifies the basic ACL that is used to control the range of multicast groups served by a static RP.	The value is an integer that ranges from 2000 to 2999.
preferred	Indicates that the static RP is preferred.	-

Views

PIM view of public network instance or PIM view of VPN instance

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When only one RP exists on a network, you can manually specify the static RP address and do not need to configure dynamic RP. This saves the bandwidth used for information exchange between the C-RPs and the BSR.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command.

Configuration Impact

If the static RP address is the address of an Up interface on the local device, the local device works as the static RP. PIM does not need to be enabled on the interface where the static RP address is located.

If no ACL is specified, the static RP serves all the multicast groups of 224.0.0.0/4. If an ACL is specified but no rule is configured in the ACL, the static RP serves all the groups of 224.0.0.0/4. If ACL rules are configured, the static RP serves only the multicast groups permitted by the ACL.

If the **static-rp** command does not contain **preferred**, devices apply the BSR mechanism to elect a dynamic RP. If dynamic RP is not configured or the dynamic RP is invalid, the static RP becomes valid. If the **static-rp** command contains **preferred**, the static RP is preferred over the dynamic RP.

If you run this command multiple times, multiple static RPs are configured. If multiple static RPs serve the same group, the RP with the largest IP address is selected to serve the group. If you specify the same RP address when running the **static-rp** command multiple times, the latest RP takes effect.

Precautions

NOTE

Up to 50 static RPs can be configured by using this command, but an ACL cannot be applied to multiple static RPs. If no ACL is referenced, only one static RP can be configured.

To ensure normal operating of a static RP, run the **static-rp** command to configure the same RP information on all devices in the PIM-SM domain.

The **static-rp** and **acl** commands are used together. In the ACL view, when the **rule** command is used to configure a filtering rule, you can set the address range of multicast groups that are served by the static RP by specifying the **source** parameter in the **rule** command. The filtering rule is effective only with the **source** parameter and the time period specified by the **time-range** parameter.

This command is valid only for PIM-SM.

Example

In the PIM view of public network instance, configure the switch with address 10.110.0.6 as a static RP serving the groups permitted by ACL 2001, and configure the static RP to be preferred.

```
<HUAWEI> system-view
[HUAWEI] acl number 2001
[HUAWEI-acl-basic-2001] rule permit source 225.1.0.0 0.0.255.255
[HUAWEI-acl-basic-2001] quit
[HUAWEI] multicast routing-enable
[HUAWEI] pim
[HUAWEI-pim] static-rp 10.110.0.6 2001 preferred
```

8.3.86 timer hello (IPv4)

Function

The **timer hello** command sets the interval at which the PIM switch sends Hello messages.

The **undo timer hello** command restores the default interval.

By default, the interval at which the PIM switch sends Hello messages is 30 seconds.

Format

timer hello *interval*

undo timer hello

Parameters

Parameter	Description	Value
interval	Specifies the interval at which Hello messages are sent.	The value is an integer ranging from 1 to 18000, in seconds.

Views

PIM view of public network instance or PIM view of VPN instance

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

PIM routers periodically send Hello messages to maintain PIM neighbor relationships. You can run the **pim timer hello** command to set the interval for sending Hello messages.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command.

Configuration Impact

This command is valid for both PIM-DM and PIM-SM.

The interval at which the PIM switch sends Hello messages should be less than the timeout period of the PIM neighbor. You can run the **hello-option holdtime (IPv4)** command to set the timeout period of PIM neighbors.

The **timer hello** command has the same function as the **pim timer hello** command in the interface view. By default, if the **pim timer hello** command is not used, the value configured in the PIM view is used; otherwise, the value configured in the interface view is used.

Example

Set the interval at which PIM Hello messages are sent to 40s in the PIM view of public network instance.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
```



```
[HUAWEI] pim
[HUAWEI-pim] timer hello 40
```

8.3.87 timer join-prune (IPv4)

Function

The **timer join-prune** command configures the interval at which Join/Prune messages are sent to an upstream device.

The **undo timer join-prune** command restores the default interval.

By default, the interval at which Join/Prune messages are sent to an upstream device is 60 seconds.

Format

timer join-prune *interval*

undo timer join-prune

Parameters

Parameter	Description	Value
interval	Specifies the interval for sending Join/Prune messages.	The value is an integer that ranges from 1 to 18000, in seconds.

Views

PIM view of public network instance or PIM view of VPN instance

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The switch sends join information to the upstream device, requesting the upstream device to forward multicast data. The switch sends prune information to the upstream device, requesting the upstream device to stop forwarding multicast data. Join information and prune information are encapsulated in Join/Prune messages. The PIM router periodically sends Join/Prune messages to the upstream router to update the forwarding status.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command.

Precautions

This command is valid only for PIM-SM.

The interval configured using the **timer join-prune** command must be shorter than the interval configured using the **holdtime join-prune (IPv4)** command.

The **timer join-prune** command has the same function as the **pim timer join-prune** command in the interface view. By default, if the **pim timer join-prune** command is not used, the value configured in the PIM view is used; otherwise, the value configured in the interface view is used.

Example

Set the interval at which Join/Prune messages are sent to 80s in the PIM view of public network instance.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] pim
[HUAWEI-pim] timer join-prune 80
```

8.3.88 timer spt-switch (IPv4)

Function

The **timer spt-switch** command sets the interval for checking whether the rate for transmitting multicast data exceeds the threshold before the switchover from the RPT to the SPT.

The **undo timer spt-switch** command restores the default value of the interval.

By default, the interval for checking whether the rate for transmitting multicast data exceeds the threshold before the switchover from the RPT to the SPT is 15 seconds.

Format

timer spt-switch *interval*

undo timer spt-switch

Parameters

Parameter	Description	Value
interval	Specifies the interval for checking whether the rate for transmitting multicast data exceeds the threshold before the switchover from RPT to SPT.	The value is an integer that ranges from 15 to 65535, in seconds.

Views

PIM view of public network instance or PIM view of VPN instance

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can run the **timer spt-switch** command to set the interval for checking whether the rate for transmitting multicast data exceeds the threshold.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command.

Precautions

This command is valid for only PIM-SM.

Before running this command, you must set the threshold for SPT switchover by using the **spt-switch-threshold (IPv4)** command; otherwise, the **timer spt-switch** command takes no effect.

Example

In the PIM view of public network instance, set the interval for checking the rate for transmitting the multicast data before the switchover from RPT to SPT to 30 seconds.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] pim
[HUAWEI-pim] spt-switch-threshold 100
[HUAWEI-pim] timer spt-switch 30
```

8.4 IPv6 PIM Configuration Commands

8.4.1 Command Support

Product	Support
S1700	Not supported.
S300	Supported.
S500	Supported.
S2700	Supported.
S5700	Supported except S5731-L and S5731S-L.
S6700	Supported.

8.4.2 bsm semantic fragmentation (IPv6)

Function

The **bsm semantic fragmentation** command enables BSR message fragmentation.

The **undo bsm semantic fragmentation** command disables BSR message fragmentation.

By default, BSR message fragmentation is not enabled.

Format

bsm semantic fragmentation

undo bsm semantic fragmentation

Parameters

None

Views

PIM-IPv6 view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A BSR message carries information about all C-RPs on the network. Therefore, if there is a large number of C-RPs on the network, the length of a BSR message exceeds the MTU of the outgoing interface. As a result, the BSR message cannot be processed and RP election fails. Consequently, multicast services cannot be transmitted normally. In this case, you can enable BSR message fragmentation to ensure that the devices on the network can learn consistent RP information and MDTs can be successfully established.

Prerequisites

IPv6 multicast routing has been enabled globally using the **multicast ipv6 routing-enable** command in the system view.

Configuration Impact

You can also configure IP fragmentation to solve the preceding problem. The difference between IP fragmentation and BSR message fragmentation is as follows:

- If IP fragmentation is enabled, the protocol layer transmits the entire BSR message up to the IP layer regardless of the length of the BSR message. The BSR message is then fragmented at the IP layer. If one fragment is lost during

transmission, the destination cannot parse the entire BSR message. As a result, the destination cannot learn RP information and MDTs cannot be established, which causes a multicast data forwarding failure.

- If BSR message fragmentation is enabled, the protocol layer directly fragments a long BSR message. If one fragment is lost during transmission, only the information carried in this fragment is lost. As a result, only MDTs corresponding to the information carried in the lost fragments cannot be established. Since the other BSR message fragments can still reach the destination, the corresponding MDTs can be correctly established.

BSR message fragmentation is recommended because IP fragmentation causes all fragments to become unavailable when fragment information is lost.

Precautions

Enable BSR message fragmentation on all devices on the network. If BSR message fragmentation is not enabled on some devices, RP information on these devices is inconsistent with that on other devices and an MDT cannot be established correctly.

Example

Enable BSR message fragmentation in the PIM-IPv6 view.

```
<HUAWEI> system-view
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] pim-ipv6
[HUAWEI-pim6] bsm semantic fragmentation
```

8.4.3 bsr-policy (IPv6)

Function

The **bsr-policy** command specifies the range of valid bootstrap router (BSR) addresses so that the device discards BSR messages sent from addresses out of this range. This prevents BSR spoofing.

The **undo bsr-policy** command restores the default configuration.

By default, the range of BSR addresses is not limited, and all BSR packets are considered valid.

Format

bsr-policy *basic-acl6-number*

undo bsr-policy

Parameters

Parameter	Description	Value
basic-acl6-number	Specifies the basic ACL number. The ACL defines the filtering policy for the range of source addresses of BSR packets.	The value is an integer that ranges from 2000 to 2999.

Views

PIM-IPv6 view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On a PIM-SM network that applies the BSR mechanism, you can configure any switch as a C-BSR to take part in the BSR election. Once a switch is elected as the BSR, it is responsible for advertising RP information in the network. To prevent the valid BSR from being maliciously replaced, take the following measures:

- Attacking hosts change the RP mapping to spoof the switch by forging BSR packets.

  Solution: Such attacks often occur on edge devices because a BSR packet is a multicast packet with TTL value of 1. As the BSR is inside the network and hosts are outside the network, the switches can perform neighbor check and RPF check on the received BSR packets to prevent the attacks.
- A switch is controlled by an attacker or an authorized switch is connected to the network. The attacker configures the switch as a C-BSR and makes the switch win the BSR election, so as to obtain the right of advertising RP information in the network.

  Solution: After the switch is configured as a C-BSR, it spreads multicast BSR packets in the network. The BSR packets have a TTL value of 1 and are forwarded hop by hop. As long as the neighboring device does not accept the BSR packets, the packets will not spread in the entire network. The solution is to use the **bsr-policy** command on every device in the network to specify the valid BSR range. For example, you can configure a policy to allow only switches with addresses FC00:0:0:2001::1/62 and FC00:0:0:2001::2/64 to function as BSRs. Then switches will not accept or forward BSR packets with addresses out of this range.

The two countermeasures mentioned above can partially protect BSRs in the network. If attackers control a valid BSR, it also brings problems to the network.

Prerequisites

IPv6 multicast routing has been enabled globally using the **multicast ipv6 routing-enable** command in the system view.

Configuration Impact

After the **bsr-policy** command is run, the switch accepts only BSR messages matching the configured policy.

Precautions

The **bsr-policy** command and the **acl ipv6 (system view)** command are used together. In the ACL view, you can set the source address range for BSR packets by specifying the **source** parameter in the **rule (basic ACL6 view)** command.

Example

In the PIM-IPv6 view, configure address FC00:0:0:2001::/64 as the valid BSR address range.

```
<HUAWEI> system-view
[HUAWEI] acl ipv6 2001
[HUAWEI-acl6-basic-2001] rule permit source fc00:0:0:2001:: 64
[HUAWEI-acl6-basic-2001] quit
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] pim-ipv6
[HUAWEI-pim6] bsr-policy 2001
```

8.4.4 c-bsr (IPv6)

Function

The **c-bsr** command configures a C-BSR.

The **undo c-bsr** command restores the default configuration.

By default, the C-BSR is not configured.

Format

c-bsr *ipv6-address* [*hash-length* [*priority*]]

undo c-bsr

Parameters

Parameter	Description	Value
ipv6-address	Specifies the global IPv6 unicast address of a C-BSR. **NOTE** To avoid frequent protocol changes caused by interface flapping, use the loopback interface address as the global IPv6 unicast address of the C-BSR.	The address is a 32-digit hexadecimal number, in the format X:X:X:X:X:X:X:X.
hash-length	Specifies the hash mask length of the C-BSR. The mask is used in a hash function to calculate the RP.	The value is an integer that ranges from 0 to 128. By default, the value is 126.

Parameter	Description	Value
priority	Specifies a priority of the C-BSR. A larger value indicates a higher priority.	The value is an integer ranging from 0 to 255. By default, the value is 0.

Views

PIM-IPv6 view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

One or more C-BSRs need to be configured in a PIM-SM domain. A BSR is elected from multiple C-BSRs and is responsible for collecting C-RP information and summarizing C-RP information into an RP-set. The RP-set is then encapsulated in a BootStrap message and advertised to all the devices in the PIM domain.

The process of BSR election is as follows:

- Each C-BSR considers itself as the BSR of the local PIM-SM domain and uses the IPv6 address of this interface as the address of the BSR to send Bootstrap messages.
- When a C-BSR receives a Bootstrap message from other devices, it compares the BSR in the received Bootstrap message with the current BSR. The BSR with the highest priority is preferred. If BSRs have the same priority, the BSR with a larger IPv6 address is preferred. If the BSR carried in the received Bootstrap message is superior to the current BSR, the C-BSR replaces its BSR address with the BSR address carried in the received Bootstrap message.

Prerequisites

IPv6 multicast routing has been enabled using the **multicast ipv6 routing-enable** command in the system view.

Precautions

If PIM-SM (IPv6) is disabled on an interface, the interface can be configured as a C-BSR but the configuration does not take effect.

For the multicast BSR messages learned through the GRE tunnel, you need to configure a static multicast route to ensure that the next hop to the BSR is a GRE interface. You need to configure static multicast routes properly to avoid routing loops.

Example

In the PIM-IPv6 view, set the IPv6 address of the C-BSR to FC00:0:0:3001::1.

```
<HUAWEI> system-view
[HUAWEI] multicast ipv6 routing-enable
```



```
[HUAWEI] pim-ipv6
[HUAWEI-pim6] c-bsr fc00:0:0:3001::1
```

8.4.5 c-bsr admin-scope (IPv6)

Function

The **c-bsr admin-scope** command configures a BSR administrative scope in a PIM-SM domain.

The **undo c-bsr admin-scope** command restores the default configuration.

By default, no BSR administrative scope is configured.

Format

c-bsr admin-scope

undo c-bsr admin-scope

Parameters

None

Views

PIM-IPv6 view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

By default, each PIM-SM domain has only one BSR that serves all the devices in the entire PIM-SM domain. To achieve more effective management, you can divide a PIM-SM domain into multiple BSR administrative scopes and a global domain. This can reduce the workload of a single BSR and designate a private-network group address for users in a specific domain.

Each BSR administrative scope maintains a BSR that serves the multicast groups in a specified range. The multicast packets for the groups in a BSR administrative domain cannot travel across the boundary of the domain. The global domain maintains a BSR that serves all multicast groups that do not belong to any BSR administrative domains.

The relationship between the BSR administrative domain and the global domain is described as follows from the aspects of the region, group address range, and multicast function.

- Region

  Though different BSR administrative domains may serve the same group, devices in each BSR administrative domain differ. One device cannot belong to multiple BSR administrative domains. Each BSR administrative domain is

independent of and isolated from each other geographically. A BSR administrative domain manages the multicast groups in a specific group address range. The multicast packets for the group in the range can be transmitted only in this administrative domain and cannot pass through the border of the BSR administrative domain.

A global domain contains all the switches on the PIM-SM network. The multicast packet that does not belong to any BSR administrative domain can be transmitted on the entire PIM network.

- Group address range

  Each BSR administrative domain serves the multicast groups in a specific group address range. The multicast groups that different BSR administrative domains serve can overlap. The address of the multicast group that the BSR administrative domain serves is valid only in its BSR administrative domain. That is, the multicast address is used as a private group address.

  The multicast group that does not belong to any BSR administrative domain belongs to a global domain.

- Multicast function

  The global domain and each BSR administrative domain have their respective Candidate-Rendezvous Point (C-RP) and BSR devices. Functions enabled on these devices take effect only in the local domain. That is, the BSR mechanism and the RP election are independent of each other among administrative domains.

  Each BSR administrative domain has its border. Multicast information of this domain, such as the C-RP Advertisement message and BSR BootStrap message, can be transmitted only within the domain. Multicast information of a global domain can be transmitted in the entire global domain and traverse any BSR administrative domain.

NOTE

Each BSR administrative domain corresponds to a scope ID defining the range of multicast groups.

Prerequisites

IPv6 multicast routing has been enabled globally using the **multicast ipv6 routing-enable** command in the system view.

Precautions

The **c-bsr admin-scope** command needs to be run on all the devices in a PIM-SM domain.

Example

Configure a BSR administrative scope in a PIM-SM domain.

```
<HUAWEI> system-view
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] pim-ipv6
[HUAWEI-pim6] c-bsr admin-scope
```


8.4.6 c-bsr global (IPv6)

Function

The **c-bsr global** command configures the switch as a C-BSR in the global domain.

The **undo c-bsr global** command restores the default configuration.

By default, no C-BSR is configured in the global domain.

Format

c-bsr global [**hash-length** *hash-length* | **priority** *priority*] *

undo c-bsr global

Parameters

Parameter	Description	Value
hash-length *hash-length*	Specifies the hash mask length of a C-BSR in the global domain.	The value is an integer that ranging from 0 to 128. By default, the value is 126.
priority *priority*	Specifies the priority of the C-BSR in the global domain.	The value is an integer that ranges from 0 to 255. By default, it is 0. The greater the value, the higher the priority of the C-BSR.

Views

PIM-IPv6 view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A PIM-SM network is divided into multiple BSR administrative domains and a global domain. The global domain maintains a BSR that serves the remaining multicast groups.

The **c-bsr global** command configures the switch as a C-BSR in the global domain. The BSR in the global domain is generated through election.

The rules of electing a BSR from C-BSRs in the global domain are as follows:

1. The C-BSR with the highest priority is elected as the BSR.
2. In the case of the same priority, the C-BSR with the highest IP address is elected as the BSR.

NOTE

A global domain contains all the switches on the PIM-SM network. The multicast packet that does not belong to any BSR administrative domain can be transmitted on the entire PIM network.

The multicast group that does not belong to any BSR administrative domain belongs to a global domain.

Multicast information of a global domain can be transmitted in the entire global domain and traverse any BSR administrative domain.

Prerequisites

IPv6 multicast routing has been enabled using the **multicast ipv6 routing-enable** command in the system view.

Precautions

The **c-bsr global** command takes effect only in a BSR administrative domain and can enable a device in this BSR administrative domain to accept multicast data for groups beyond the address range of the administrative domain.

Example

In the PIM-IPv6 view, configure the switch as a C-BSR in the global domain, and then set the priority of the C-BSR to 1.

```
<HUAWEI> system-view
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] pim-ipv6
[HUAWEI-pim6] c-bsr global priority 1
```

8.4.7 c-bsr hash-length (IPv6)

Function

The **c-bsr hash-length** command configures the global hash mask length of a C-BSR.

The **undo c-bsr hash-length** command restores the default configuration.

By default, the global hash mask length of a C-BSR is 126.

Format

c-bsr hash-length *hash-length*

undo c-bsr hash-length

Parameters

Parameter	Description	Value
hash-length	Specifies the global hash mask length of a C-BSR.	The value is an integer that ranges from 0 to 128.

Views

PIM-IPv6 view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

During dynamic RP election, if C-RPs have the same interface address mask and priority for a specified multicast group, a hash function needs to be executed to select the RP for the multicast group. The switch performs hash calculation for the group address of G, C-RP address, and hash mask length of the C-RPs with the same priority and compares the hash values. The C-RP with the greatest hash value acts as the RP for G.

The hash mask length is used to adjust the hash calculation result.

Prerequisites

IPv6 multicast routing has been enabled using the **multicast ipv6 routing-enable** command in the system view.

Precautions

You can also run the **c-bsr** *ipv6-address hash-length* command in the PIM-IPv6 view configure the hash mask length while configuring a C-BSR address. The **c-bsr hash-length** *hash-length* command specifies the global hash mask length. If both the two commands are configured, the hash mask length configured by the **c-bsr** *ipv6-address hash-length* command takes effect.

Example

In the PIM-IPv6 view, set the global hash mask length of a C-BSR to 16.

```
<HUAWEI> system-view
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] pim-ipv6
[HUAWEI-pim6] c-bsr hash-length 16
```

8.4.8 c-bsr holdtime (IPv6)

Function

The **c-bsr holdtime** command configures the timeout period during which the C-BSR waits to receive Bootstrap messages sent by the BSR.

The **undo c-bsr holdtime** command restores the default configuration.

By default, the timeout period during which the C-BSR waits to receive Bootstrap messages sent by the BSR is 130s.

Format

c-bsr holdtime *interval*

undo c-bsr holdtime

Parameters

Parameter	Description	Value
interval	Specifies the timeout time during which C-BSR waits for the Bootstrap message to be sent by BSR.	The value is an integer that ranges from 1 to 214748364, in seconds.

Views

PIM-IPv6 view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After a C-BSR is elected as the BSR, it periodically sends Bootstrap messages carrying its own IPv6 address and the RP-set information. The interval for sending Bootstrap messages is BS_interval, which can be configured using the **c-bsr interval** command.

Other C-BSRs that fail in the election are suppressed from sending Bootstrap messages and start the timer to monitor the elected BSR. The timeout period of a timer is holdtime, which can be configured using the **c-bsr holdtime** command.

- If the C-BSR receives the Bootstrap messages sent by the BSR, the C-BSR refreshes the timer. The C-BSRs that fail in the election also refresh the timeout period of the BSR according to the holdtime.
- If the timer times out, the elected BSR is considered faulty. The C-BSRs that fail the previous election elect a new BSR. Services are not interrupted.

Prerequisites

IPv6 multicast routing has been enabled using the **multicast ipv6 routing-enable** command in the system view.

Precautions

In actual applications, all C-BSRs in the same PIM domain must use the same BS_interval and holdtime. If the configured values are different, the BSR may become unstable. This may result in multicast faults. Note the following points:

- If BS_interval and holdtime are configured at the same time, ensure that BS_interval is less than holdtime.
- If BS_interval or holdtime is configured, use the following formula to calculate the other one: holdtime = 2 x BS_interval + 10. The following determines which value is used:
  - If holdtime is configured and the calculated BS_interval is less than the minimum value of BS_interval, the minimum value is used.

  - If BS_interval is configured and the calculated holdtime is more than the maximum value of holdtime, the maximum value is used.
- If neither BS_interval nor holdtime is configured, the default values are used. The default BS_interval is 60s and the default holdtime is 130s.

Example

In the PIM-IPv6 view, set the timeout interval during which the C-BSR waits for the Bootstrap message to be sent by BSR to 150 seconds.

```
<HUAWEI> system-view
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] pim-ipv6
[HUAWEI-pim6] c-bsr holdtime 150
```

8.4.9 c-bsr interval (IPv6)

Function

The **c-bsr interval** command configures the interval at which the BSR continuously sends Bootstrap messages.

The **undo c-bsr interval** command restores the default interval.

By default, the BSR sends Bootstrap messages at a 60-second interval.

Format

c-bsr interval *interval*

undo c-bsr interval

Parameters

Parameter	Description	Value
interval	Specifies the interval at which a BSR continuously sends Bootstrap messages.	The value is an integer that ranges from 1 to 107374177, in seconds.

Views

PIM-IPv6 view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After a C-BSR is elected as the BSR, it periodically sends Bootstrap messages carrying its own IPv6 address and the RP-set information.

The interval for sending Bootstrap messages is BS_interval, which can be configured using the **c-bsr interval** command.

Other C-BSRs that fail in the election are suppressed from sending Bootstrap messages and start the timer to monitor the BSR. The timeout period of a timer is holdtime, which can be configured using the **c-bsr holdtime** command. The following applies to the timer:

- If the C-BSR receives the Bootstrap messages sent by the BSR, the C-BSR refreshes the timer.
- If the timer times out, the BSR is considered to be faulty. The C-BSRs that failed in the election triggers a new BSR election to prevent service interruption.

Prerequisites

IPv6 multicast routing has been enabled using the **multicast ipv6 routing-enable** command in the system view.

Precautions

In actual applications, all C-BSRs in the same PIM domain must use the same BS_interval and holdtime values. If C-BSRs use different BS_interval or holdtime values, the BSR changes frequently, causing multicast forwarding errors. Note the following points:

- If BS_interval and holdtime are configured at the same time, ensure that BS_interval is less than holdtime.
- If only one of the BS_interval and holdtime is configured, use the following formula to calculate the other parameter: holdtime = 2 x BS_interval + 10. The following determines which value is used:
  - If holdtime is configured and the calculated BS_interval is less than the minimum value of BS_interval, the minimum value is used.
  - If BS_interval is configured and the calculated holdtime is more than the maximum value of holdtime, the maximum value is used.
- If neither the BS_interval nor the holdtime is configured, default values are used. The default value of BS_interval is 60s, and the default value of holdtime is 130s.

Example

In the PIM-IPv6 view, set the interval for the C-BSR to continuously send Bootstrap messages to 30 seconds.

```
<HUAWEI> system-view
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] pim-ipv6
[HUAWEI-pim6] c-bsr interval 30
```

8.4.10 c-bsr priority (IPv6)

Function

The **c-bsr priority** command configures the global C-BSR priority.

The **undo c-bsr priority** command restores the default configuration.

By default, the global C-BSR priority is 0.

Format

c-bsr priority *priority*

undo c-bsr priority

Parameters

Parameter	Description	Value
priority	Specifies the global priority of the C-BSR.	The value is an integer that ranges from 0 to 255. A larger value indicates a higher priority.

Views

PIM-IPv6 view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When multiple C-BSRs participate in the BSR election in the PIM-SM domain:

- The switch with the highest priority wins in the BSR election.
- If they have the same priority, the switch with the largest IPv6 address wins in the BSR election.

To enable a C-BSR to function as the BSR, you can run the **c-bsr priority** command to increase the priority value of the C-BSR.

Prerequisites

IPv6 multicast routing has been enabled globally using the **multicast ipv6 routing-enable** command in the system view.

Precautions

You can also run the **c-bsr** *ipv6-address hash-length priority* command in the PIM-IPv6 view to set the C-BSR priority while configuring a C-BSR. The **c-bsr priority** *priority* command sets the global priority. When both the two commands are configured, the priority configured by the **c-bsr** *ipv6-address hash-length priority* command takes effect.

Example

In the PIM-IPv6 view, set the global C-BSR priority to 5.

```
<HUAWEI> system-view
[HUAWEI] multicast ipv6 routing-enable
```



```
[HUAWEI] pim-ipv6
[HUAWEI-pim6] c-bsr priority 5
```

8.4.11 c-bsr scope

Function

The **c-bsr scope** command specifies the scope ID of the BSR administrative domain served by a C-BSR.

The **undo c-bsr scope** command restores the default configuration.

By default, no scope ID is specified for a C-BSR. That is, the C-BSR does not belong to any BSR administrative domain.

Format

c-bsr scope *scope-id* [**hash-length** *hash-length* | **priority** *priority*] *

undo c-bsr scope *scope-id*

Parameters

Parameter	Description	Value
scope-id	Specifies the scope ID of the administrative domain served by a C-BSR.	The value is an integer that ranges from 3 to 15.
hash-length *hash-length*	Specifies the hash mask length of a C-BSR in a BSR administrative domain.	The value is an integer that ranges from 0 to 128. The default value is 126.
priority *priority*	Specifies the priority of a C-BSR in a BSR administrative domain.	The value is an integer that ranges from 0 to 255. The default value is 0. The greater the value, the higher the priority.

Views

PIM-IPv6 view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Each BSR administrative domain is assigned a scope ID. To configure a C-BSR to serve a BSR administrative domain, use the **c-bsr scope** command to specify the scope ID of the BSR administrative domain. Packets forwarded by the C-BSR cannot travel across the boundary of the BSR administrative domain.

Prerequisites

IPv6 multicast routing has been enabled using the **multicast ipv6 routing-enable** command in the system view.

A BSR administrative domain has been configured using the **c-bsr admin-scope (IPv6)** command in the PIM-IPv6 view.

Precautions

The multicast group that does not belong to any BSR administrative domain belongs to a global domain.

Example

In the PIM-IPv6 view, configure the switch as a C-BSR in the BSR administrative domain to serve groups of Scope 5, and set the priority of the C-BSR to 10.

```
<HUAWEI> system-view
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] pim-ipv6
[HUAWEI-pim6] c-bsr scope 5 priority 10
```

8.4.12 c-rp (IPv6)

Function

The **c-rp** command configures the switch to advertise itself as a C-RP to the BSR.

The **undo c-rp** command restores the default configuration.

By default, no C-RP is configured.

Format

c-rp *ipv6-address* [**advertisement-interval** *adv-interval* | [**group-policy** *basic-acl6-number* | **scope** *scope-id*] | **holdtime** *hold-interval* | **priority** *priority*] *

undo c-rp *ipv6-address* [**scope** *scope-id*]

Parameters

Parameter	Description	Value
ipv6-address	Specifies the global IPv6 unicast address of a C-RP. **NOTE** To avoid frequent protocol changes caused by interface flapping, use the loopback interface address as the global IPv6 unicast address of the C-RP.	The address is a 32-digit hexadecimal number, in the format X:X:X:X:X:X:X:X.

Parameter	Description	Value
advertisement-interval *adv-interval*	Specifies the interval at which the C-RP sends Advertisement messages.	The value is an integer that ranges from 1 to 65535, in seconds. By default, the value is 60 seconds.
group-policy *basic-acl6-number*	Specifies the range of multicast groups that the C-RP serves. The range is limited through the ACL6. *basic-acl6-number* specifies the number of the basic ACL6 used to limit the range of multicast groups that the C-RP serves.	The value is an integer that ranges from 2000 to 2999.
scope *scope-id*	Specifies the scope ID of the BSR administrative domain that a C-RP serves.	The value is an integer that ranges from 3 to 15.
holdtime *hold-interval*	Specifies the holdtime period during which the C-RP sends Advertisement messages. *hold-interval* specifies the time remaining before the C-RP sends Advertisement messages.	The value is an integer that ranges from 1 to 65535, in seconds. By default, the value is 150 seconds.
priority *priority*	Specifies the priority of a C-RP. The value of *priority* indicates the priority of a C-RP.	The value is an integer that ranges from 0 to 255. By default, the value is 192. The greater the value is, the lower the priority is.

Views

PIM-IPv6 view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

An RP is the core of a PIM-SM (IPv6) domain, and therefore a C-RP must be able to communicate with the other devices in the PIM-SM (IPv6) domain. It is recommended that you configure a C-RP on the device that aggregates multicast traffic and reserve enough bandwidth between this device and each of the other devices in the PIM-SM (IPv6) domain.

The rules used to elect an RP from multiple C-RPs are as follows, in descending order of precedence:

1. The C-RP with the longest mask length of the served group address range matching the multicast group that users have joined wins.
2. The C-RP with highest priority wins.
3. The C-RP with the largest hash value wins.
4. The C-RP with the largest IPv6 address wins.

Prerequisites

IPv6 multicast routing has been enabled globally using the **multicast ipv6 routing-enable** command in the system view.

Configuration Impact

The **group-policy** *basic-acl6-number*, **priority** *priority*, **holdtime** *hold-interval* and **advertisement-interval** *adv-interval* set by using the command take precedence over the values of the global parameters configured in the PIM-IPv6 view because this command specifies an interface address. If this command is run several times on the same interface, only the latest configuration is valid.

Precautions

- If PIM-SM (IPv6) is disabled on an interface, the interface can be configured as a C-RP but the configuration does not take effect.
- **group-policy** *basic-acl6-number* specifies a group range. All permitted group ranges will be advertised as the ranges of groups that the RP serves. If no group range is specified for a C-RP or a C-RP is configured to serve all addresses, the C-RP serves all multicast groups.

The **c-rp** command and the **acl** command are used together.

- For the IPv6 numbered ACL, in the ACL6 view, you can set the address range of multicast groups that are serviced by the candidate RP by specifying the **source** parameter in the **rule** command.
- For the IPv6 Named ACL, in the ACL6 view, you can set the address range of multicast groups that are serviced by the candidate RP by specifying the **destination** parameter in the **rule** command.

If you want the switch to function as C-RPs in multiple BSR administrative domains, you need to specify the scope ID of each BSR administrative domain. For each scope ID, the settings of **advertisement-interval** *interval*, **priority** *priority-value*, and **holdtime** *interval* will overwrite the global settings in the PIM view.

Example

In the PIM-IPv6 view, configure an interface with the IPv6 address FC00:0:0:2001::1 as a C-RP of the PIM-SM (IPv6) domain.

```
<HUAWEI> system-view
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] pim-ipv6
[HUAWEI-pim6] c-rp fc00:0:0:2001::1
```


8.4.13 c-rp advertisement-interval (IPv6)

Function

The **c-rp advertisement-interval** command sets the interval at which a C-RP sends Advertisement messages.

The **undo c-rp advertisement-interval** command restores the default interval.

By default, a C-RP sends Advertisement messages at an interval of 60 seconds.

Format

c-rp advertisement-interval *interval*

undo c-rp advertisement-interval

Parameters

Parameter	Description	Value
interval	Specifies the interval at which a C-RP sends Advertisement messages.	The value ranges from 1 to 65535, in seconds.

Views

PIM-IPv6 view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

All C-RPs in a PIM-SM domain periodically send Advertisement messages to the same BSR. The BSR can collect the integrated RP-Set.

The **c-rp advertisement-interval** command sets the interval at which a C-RP sends Advertisement messages to the BSR.

Prerequisites

IPv6 multicast routing has been enabled using the **multicast ipv6 routing-enable** command in the system view.

Precautions

You can also run the **c-rp** *ipv6-address* **advertisement-interval** *interval* command in the PIM-IPv6 view to configure the advertisement interval while configuring a C-RP. The **c-rp advertisement-interval** *interval* command specifies the global interval. If both the commands are configured, the interval configured by the **c-rp** *ipv6-address* **advertisement-interval** *interval* command takes effect.

Example

In the PIM-IPv6 view, set the interval at which a C-RP sends Advertisement messages to 30s.

```
<HUAWEI> system-view
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] pim-ipv6
[HUAWEI-pim6] c-rp advertisement-interval 30
```

8.4.14 c-rp holdtime (IPv6)

Function

The **c-rp holdtime** command configures the holdtime for a received Advertisement message on a BSR.

The **undo c-rp holdtime** command restores the default holdtime.

By default, the holdtime for a received Advertisement message is 150 seconds.

Format

c-rp holdtime *hold-interval*

undo c-rp holdtime

Parameters

Parameter	Description	Value
hold-interval	Specifies the timeout period for a BSR to wait the Advertisement message from a C-RP.	The value ranges from 1 to 65535, in seconds.

Views

PIM-IPv6 view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When *hold-interval* is set on a C-RP, the C-RP encapsulates *hold-interval* in an Advertisement message and sends it to the BSR. The BSR obtains this *hold-interval* from the message and starts the timer. If the BSR receives no Advertisement message from the C-RP within the timeout period, the BSR regards the C-RP invalid or unreachable.

Prerequisites

IPv6 multicast routing has been enabled using the **multicast ipv6 routing-enable** command in the system view.

Precautions

You can also run the **c-rp** *ipv6-address* **holdtime** *hold-interval* command in the PIM-IPv6 view to configure the advertisement message holdtime while configuring a C-RP. The **c-rp holdtime** *hold-interval* configures the global holdtime for Advertisement messages. If both the two commands are configured, the holdtime configured by the **c-rp** *ipv6-address* **holdtime** *hold-interval* command takes effect.

Example

In the PIM-IPv6 view, set the holdtime for a received Advertisement message to 100s.

```
<HUAWEI> system-view
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] pim-ipv6
[HUAWEI-pim6] c-rp holdtime 100
```

8.4.15 c-rp priority (IPv6)

Function

The **c-rp priority** command configures the global C-RP priority.

The **undo c-rp priority** command restores the default configuration.

By default, the global C-RP priority is 192.

Format

c-rp priority *priority*

undo c-rp priority

Parameters

Parameter	Description	Value
priority	Specifies the global C-RP priority.	The value is an integer that ranges from 0 to 255. A larger value indicates a lower priority.

Views

PIM-IPv6 view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The following rules are used to elect an RP from multiple C-RPs, in descending order of precedence:

- The C-RP with the interface address that has the longest mask wins.
- The C-RP with highest priority wins.
- The C-RP with the largest hash value wins.
- The C-RP with the largest IPv6 address wins.

To enable a C-RP to function as an RP, you can run the **c-rp priority** command to increase the priority of the C-RP.

Prerequisites

IPv6 multicast routing has been enabled globally using the **multicast ipv6 routing-enable** command in the system view.

Precautions

You can also run the **c-rp** *ipv6-address* **priority** *priority* command in the PIM-IPv6 view to configure the C-RP priority while configuring a C-RP. The **c-rp priority** *priority* command specifies the global C-RP priority. If both the two commands are configured, the priority configured by the **c-rp** *ipv6-address* **priority** *priority* command takes effect.

Example

In the PIM-IPv6 view, set the global C-RP priority to 5.

```
<HUAWEI> system-view
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] pim-ipv6
[HUAWEI-pim6] c-rp priority 5
```

8.4.16 crp-policy (IPv6)

Function

The **crp-policy** command limits the range of valid C-RP addresses and the range of the multicast addresses served by a C-RP. The BSR drops the C-RP messages with addresses out of the specified range to protect valid C-RPs.

The **undo crp-policy** command restores the default configuration.

By default, the BSR does not limit the range of valid C-RP addresses and the range of the multicast groups served by a C-RP. The BSR considers all the received C-RP messages valid.

Format

crp-policy *advanced-acl6-number*

undo crp-policy

Parameters

Parameter	Description	Value
advanced-acl6-number	Specifies the number of an advanced ACL. The ACL defines the range of the C-RP addresses and the range of the group addresses served by a C-RP.	The value is an integer that ranges from 3000 to 3999.

Views

PIM-IPv6 view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On a PIM SM network that uses the BSR mechanism, any switch can be configured as a C-RP to serve the multicast groups in a specified range. Each C-RP sends its information to the BSR in unicast mode. The BSR summarizes all received C-RP information into an RP-set, and floods it to the entire network using BSR messaged. The local switch then works out the RP serving a specific multicast group address range according to the RP-set.

To protect valid C-RPs from being spoofed, configure **crp-policy** on the BSR to limit the range of valid C-RP addresses and the range of multicast group addresses served by a C-RP. Configure the same filtering rule on each C-BSR because any C-BSR can become the BSR.

Prerequisites

IPv6 multicast routing has been enabled globally using the **multicast ipv6 routing-enable** command in the system view.

Configuration Impact

The **crp-policy** command and the **acl ipv6 (system view)** command are used together. In the ACL6 view, you can set the valid source address range for the C-RP by specifying the **source** parameter in the **rule (advanced ACL6 view)** command. You can set the address range of multicast groups that are served by specifying the **destination** parameter in the **rule (advanced ACL6 view)** command.

If an ACL rule is specified but no C-RP address range is set, all C-RP messages are denied.

The **crp-policy** command and the **acl** command are used together. In the ACL6 view, you can set the valid source address range for the C-RP by specifying the **source** parameter in the **rule** command, and set the address range of multicast groups that are serviced by specifying the **destination** parameter in the **rule** command.

The matching of the received C-RP message succeeds only when the C-RP address carried in the message matches **source** and the address of the multicast groups carried in the message is a subset of the group address range in the ACL.

The configurations of the named ACL6 and the advanced ACL are the same, and can implement filtering of both source addresses and multicast group addresses. The named ACL can also be configured with the **time-range** parameter.

Example

Configure a C-RP policy on the C-BSR, which allows only the C-RP with the address FC00:0:0:2001::1/128 and allows the C-RP to serve only the multicast groups FF13::101/128.

```
<HUAWEI> system-view
[HUAWEI] acl ipv6 number 3100
[HUAWEI-acl6-adv-3100] rule permit ipv6 source fc00:0:0:2001::1 128 destination ff13::101 128
[HUAWEI-acl6-adv-3100] quit
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] pim-ipv6
[HUAWEI-pim6] crp-policy 3100
```

8.4.17 display default-parameter pim-dm6

Function

The **display default-parameter pim-dm6** command displays default PIM-DM (IPv6) configurations.

Format

display default-parameter pim-dm6

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The **display default-parameter pim-dm6** command displays default PIM-DM (IPv6) configurations. Even if PIM-DM (IPv6) parameters are modified, the **display default-parameter pim-dm6** command still displays default parameter settings. Therefore, you can use this command to check which parameters have been modified.

Example

Display default configurations about PIM-DM (IPv6).

```
<HUAWEI> display default-parameter pim-dm6
 PIM6 View Default Configurations:
 ---------------------------------
 Hello-option dr-priority: 1
 Hello-option holdtime: 105 s
 Hello-option lan-delay: 500 ms
 Hello-option neighbor-tracking: disabled
 Hello-option override-interval: 2500 ms
 Holdtime assert: 180 s
 Holdtime join-prune: 210 s
 Source-lifetime: 210 s
 State-refresh-interval: 60 s
 State-refresh-rate-limit: 30 s
 State-refresh-ttl: 255
 Hello periodic interval: 30 s
 Join-prune periodic interval: 60 s

 Interface View Default Configurations:
 --------------------------------------
 Pim bfd: disabled
 Pim hello-option dr-priority: 1
 Pim hello-option holdtime: 105 s
 Pim hello-option lan-delay: 500 ms
 Pim hello-option neighbor-tracking: disabled
 Pim hello-option override-interval: 2500 ms
 Pim holdtime assert: 180 s
 Pim holdtime join-prune: 210 s
 Pim require-genid: disabled
 Pim silent: disabled
 Pim state-refresh-capable: enabled
 Pim timer dr-switch-delay: disabled
 Pim timer graft-retry: 3 s
 Pim hello periodic interval: 30 s
 Pim join-prune periodic interval: 60 s
 Pim triggered-hello-delay: 5 s
 Pim version: 2
 Pim ipsec sa: disabled
 Pim neighbor-policy: disabled
```

Table 8-54 Description of the **display default-parameter pim-dm6** command output

Item	Description
PIM6 View Default Configurations	Default configurations in the PIM-IPv6 view.
Hello-option dr-priority	Priority for DR election. This parameter is configured by the **hello-option dr-priority (IPv6)** command.
Hello-option holdtime	Time period for the neighbor to hold the reachable state. This parameter is configured by the **hello-option holdtime (IPv6)** command.

Item	Description
Hello-option lan-delay	Delay in transmitting Prune messages at a shared network segment. This parameter is configured by the **hello-option lan-delay (IPv6)** command.
Hello-option neighbor-tracking	Whether neighbor tracking is enabled. • enabled: Neighbor tracking is enabled. • disabled: Neighbor tracking is disabled This function is configured using the **hello-option neighbor-tracking (IPv6)** command.
Hello-option override-interval	Interval for sending Prune Override messages. This parameter is configured by the **hello-option override-interval (IPv6)** command.
Holdtime assert	Time period for holding the Assert state. This parameter is configured by the **holdtime assert (IPv6)** command.
Holdtime join-prune	Time period for holding the Join or Prune state. This parameter is configured by the **holdtime join-prune (IPv6)** command.
Source-lifetime	Timeout period of an (S, G) entry. This parameter is configured by the **source-lifetime (IPv6)** command.
State-refresh-interval	Interval for sending State-Refresh messages. This parameter is configured by the **state-refresh-interval (IPv6)** command.
State-refresh-rate-limit	Minimum interval from when the last State-Refresh message is received to when the next State-Refresh message is received. This parameter is configured by the **state-refresh-rate-limit (IPv6)** command.
State-refresh-ttl	TTL value of the State-Refresh message. This parameter is configured by the **state-refresh-ttl (IPv6)** command.
Hello periodic interval	Interval for sending Hello messages. This parameter is configured by the **timer hello (IPv6)** command.
Join-prune periodic interval	Interval for sending Join/Prune messages. This parameter is configured by the **timer join-prune (IPv6)** command.

Item	Description
Interface View Default Configurations	Default configurations in the interface view.
Pim bfd	Whether the PIM BFD is enabled on the interface. This parameter is configured by the **pim ipv6 bfd enable** command.
Pim hello-option dr-priority	Priority for DR election on the interface. This parameter is configured by the **pim ipv6 hello-option dr-priority** command.
Pim hello-option holdtime	Time period for the neighbor on the interface to hold the reachable state. This parameter is configured by the **pim ipv6 hello-option holdtime** command.
Pim hello-option lan-delay	Delay in transmitting Prune messages at the shared network segment where the interface resides. This parameter is configured by the **pim ipv6 hello-option lan-delay** command.
Pim hello-option neighbor-tracking	Whether neighbor tracking is enabled on the interface. ● enabled: Neighbor tracking is enabled. ● disabled: Neighbor tracking is disabled This function is configured using the **pim ipv6 hello-option neighbor-tracking** command.
Pim hello-option override-interval	Interval for the interface to send Prune Override messages. This parameter is configured by the **pim ipv6 hello-option override-interval** command.
Pim holdtime assert	Time period for the interface to hold the Assert state. This parameter is configured by the **pim ipv6 holdtime assert** command.
Pim holdtime join-prune	Time period for the interface to hold the Join or Prune state. This parameter is configured by the **pim ipv6 holdtime join-prune** command.

Item	Description
Pim require-genid	Whether the received Hello message is required to carry the Generation ID. ● enabled: The received Hello message is required to carry the Generation ID. ● disabled: The received Hello message is not required to carry the Generation ID. This parameter is configured using the **pim ipv6 require-genid** command.
Pim silent	Whether the interface is in PIM silent state. ● enabled: The interface is in PIM silent state. ● disabled: The interface is not in PIM silent state. This parameter is configured using the **pim ipv6 silent** command.
Pim state-refresh-capable	Whether State-Refresh is enabled on the interface. ● enabled: State-Refresh is enabled on the interface. ● disabled: State-Refresh is disabled on the interface. This function is configured using the **pim ipv6 state-refresh-capable** command.
Pim timer dr-switch-delay	Whether the DR switch delay is set on the interface. ● enabled: The DR switch delay is set on the interface. ● disabled: The DR switch delay is not set on the interface. This function is configured using the **pim ipv6 timer dr-switch-delay** command.
Pim timer graft-retry	Interval for the interface to retransmit Graft messages. This parameter is configured by the **pim ipv6 timer graft-retry** command.
Pim hello periodic interval	Interval for the interface to send Hello messages. This parameter is configured by the **pim ipv6 timer hello** command.

Item	Description
Pim join-prune periodic interval	Interval for the interface to send Join/Prune messages. This parameter is configured by the **pim ipv6 timer join-prune** command.
Pim triggered-hello-delay	Maximum delay for the interface to send Hello messages. This parameter is configured by the **pim ipv6 triggered-hello-delay** command.
Pim version	Version of PIM enabled on the interface.
Pim ipsec sa	Whether PIM IPSec is enabled on the interface. The switch does not support this function.
Pim neighbor-policy	Whether the neighbor-policy is set on the interface. • enabled: A neighbor policy is configured on the interface. • disabled: No neighbor policy is configured on the interface. This function is configured using the **pim ipv6 neighbor-policy** command.

8.4.18 display default-parameter pim-sm6

Function

The **display default-parameter pim-sm6** command displays default PIM-SM (IPv6) configurations.

Format

display default-parameter pim-sm6

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The **display default-parameter pim-sm6** command displays default configurations about PIM-SM (IPv6) for both ASM and SSM. Even if PIM-SM (IPv6) parameters are modified, the **display default-parameter pim-sm6** command still displays default parameter settings. This command helps you determine which parameters have been modified.

Example

Display default PIM-SM (IPv6) configurations.

```
<HUAWEI> display default-parameter pim-sm6
 PIM6 View Default Configurations:
  ---------------------------------
  Bsr-policy: disabled
  C-bsr admin-scope: disabled
  C-bsr global: disabled
  C-bsr group: none
  C-bsr hash-length: 126
  C-bsr holdtime: 130 s
  C-bsr interval: 60 s
  C-bsr priority: 0
  C-rp advertisement-interval: 60 s
  C-rp holdtime: 150 s
  C-rp priority: 192
  Crp-policy: disabled
  Bsm semantic fragmentation: disabled
  Embedded-rp: enabled
  Hello-option dr-priority: 1
  Hello-option holdtime: 105 s
  Hello-option lan-delay: 500 ms
  Hello-option neighbor-tracking: disabled
  Hello-option override-interval: 2500 ms
  Holdtime assert: 180 s
  Holdtime join-prune: 210 s
  Probe-interval: 5 s
  Register-policy: disabled
  Register-suppression-timeout: 60 s
  Source-lifetime: 210 s
  Source-policy: disabled
  Spt-switch-threshold: disabled
  Ssm-policy: disabled
  Static-rp:  disabled
  Hello periodic interval: 30 s
  Join-prune periodic interval: 60 s
  Timer spt-switch: 15 s

  Interface View Default Configurations:
  --------------------------------------
  Pim bfd: disabled
  Pim bsr-boundary: disabled
  Pim hello-option dr-priority: 1
  Pim hello-option holdtime: 105 s
  Pim hello-option lan-delay: 500 ms
  Pim hello-option neighbor-tracking: disabled
  Pim hello-option override-interval: 2500 ms
  Pim holdtime assert: 180 s
  Pim holdtime join-prune: 210 s
  Pim require-genid: disabled
  Pim silent: disabled
  Pim timer dr-switch-delay: disabled
  Pim hello periodic interval: 30 s
  Pim join-prune periodic interval: 60 s
  Pim triggered-hello-delay: 5 s
  Pim version: 2
  Pim ipsec sa: disabled
```



```
Pim join-policy: disabled
Pim neighbor-policy: disabled
```

Table 8-55 Description of the **display default-parameter pim-sm6** command output

Item	Description
PIM6 View Default Configurations	Default configurations in the PIM-IPv6 view.
Bsr-policy	Whether the valid address range of the BSR is set. This parameter is configured by the **bsr-policy (IPv6)** command.
C-bsr admin-scope	Whether the BSR administrative domain is configured. This parameter is configured by the **c-bsr admin-scope (IPv6)** command.
C-bsr global	Whether the C-BSR in the global domain is configured. This parameter is configured by the **c-bsr global (IPv6)** command.
C-bsr group	Whether the C-BSR in the BSR administrative domain is configured. This parameter is configured by the **c-bsr scope** command.
C-bsr hash-length	Global hash mask length of the C-BSR. This parameter is configured by the **c-bsr hash-length (IPv6)** command.
C-bsr holdtime	Waiting time for the BSR to receive the Bootstrap message. This parameter is configured by the **c-bsr holdtime (IPv6)** command.
C-bsr interval	Interval for the BSR to send Bootstrap messages. This parameter is configured by the **c-bsr interval (IPv6)** command.
C-bsr priority	Global priority of the C-BSR. This parameter is configured by the **c-bsr priority (IPv6)** command.
C-rp advertisement-interval	Interval for the C-RP to send Advertisement messages. This parameter is configured by the **c-rp advertisement-interval (IPv6)** command.
C-rp holdtime	Waiting time for the BSR to receive the Advertisement message. This parameter is configured by the **c-rp holdtime (IPv6)** command.
C-rp priority	Global priority of the C-RP. This parameter is configured by the **c-rp priority (IPv6)** command.

Item	Description
Crp-policy	Whether the valid address range of the C-RP and the range of multicast groups that the C-RP serves are set. This parameter is configured by the **crp-policy (IPv6)** command.
Bsm semantic fragmentation	Whether the BSR fragmentation is enabled. This parameter is configured by the **bsm semantic fragmentation (IPv6)** command.
Embedded-rp	Whether the embedded RP is enabled. This parameter is configured by the **embedded-rp** command.
Hello-option dr-priority	Priority for DR election. This parameter is configured by the **hello-option dr-priority (IPv6)** command.
Hello-option holdtime	Time period for the neighbor to hold the reachable state. This parameter is configured by the **hello-option holdtime (IPv6)** command.
Hello-option lan-delay	Delay in transmitting Prune messages at a shared network segment. This parameter is configured by the **hello-option lan-delay (IPv6)** command.
Hello-option neighbor-tracking	Whether neighbor tracking is enabled. This parameter is configured by the **hello-option neighbor-tracking (IPv6)** command.
Hello-option override-interval	Interval for sending Prune Override messages. This parameter is configured by the **hello-option override-interval (IPv6)** command.
Holdtime assert	Time period for holding the Assert state. This parameter is configured by the **holdtime assert (IPv6)** command.
Holdtime join-prune	Time period for holding the Join or Prune state. This parameter is configured by the **holdtime join-prune (IPv6)** command.
Probe-interval	Interval for sending Probe messages (empty Register messages) to the RP. This parameter is configured by the **probe-interval (IPv6)** command.
Register-policy	Whether the rule for filtering Register messages is configured. This parameter is configured by the **register-policy (IPv6)** command.

Item	Description
Register-suppression-timeout	Time period for holding the register-suppression state. This parameter is configured by the **register-suppression-timeout (IPv6)** command.
Source-lifetime	Timeout period of an (S, G) entry. This parameter is configured by the **source-lifetime (IPv6)** command.
Source-policy	Whether the rule for filtering multicast sources is configured. This parameter is configured by the **source-policy (IPv6)** command.
Spt-switch-threshold	Whether the threshold of the multicast packet rate that triggers the switch from the RPT to the SPT is configured. This parameter is configured by the **spt-switch-threshold (IPv6)** command.
Ssm-policy	Whether the SSM group address range is set. This parameter is configured by the **ssm-policy (IPv6)** command.
Static-rp	Whether the static RP is configured. This parameter is configured by the **static-rp (IPv6)** command.
Hello periodic interval	Interval for sending Hello messages. This parameter is configured by the **timer hello (IPv6)** command.
Join-prune periodic interval	Interval for sending Join/Prune messages. This parameter is configured by the **timer join-prune (IPv6)** command.
Timer spt-switch	Whether the interval for checking whether the multicast packet rate exceeds the threshold before the switchover from RPT to SPT is configured. This parameter is configured by the **timer spt-switch (IPv6)** command.
Interface View Default Configurations	Default configurations in the interface view.
Pim bfd	Whether the PIM BFD is enabled on the interface. This parameter is configured by the **pim ipv6 bfd enable** command.
Pim bsr-boundary	Whether the PIM boundary is configured on the interface. This parameter is configured by the **pim ipv6 bsr-boundary** command.

Item	Description
Pim hello-option dr-priority	Priority for DR election on the interface. This parameter is configured by the **pim ipv6 hello-option dr-priority** command.
Pim hello-option holdtime	Time period for the neighbor on the interface to hold the reachable state. This parameter is configured by the **pim ipv6 hello-option holdtime** command.
Pim hello-option lan-delay	Delay in transmitting Prune messages at a shared network segment on the interface. This parameter is configured by the **pim ipv6 hello-option lan-delay** command.
Pim hello-option neighbor-tracking	Whether neighbor tracking is enabled on the interface. This parameter is configured by the **pim ipv6 hello-option neighbor-tracking** command.
Pim hello-option override-interval	Interval for the interface to send Prune Override messages. This parameter is configured by the **pim ipv6 hello-option override-interval** command.
Pim holdtime assert	Time period for the interface to hold the Assert state. This parameter is configured by the **pim ipv6 holdtime assert** command.
Pim holdtime join-prune	Time period for the interface to hold the Join or Prune state. This parameter is configured by the **pim ipv6 holdtime join-prune** command.
Pim require-genid	Whether the received Hello message is required to carry the Generation ID. This parameter is configured by the **pim ipv6 require-genid** command.
Pim silent	Whether PIM Silent is enabled on the interface. This parameter is configured by the **pim ipv6 silent** command.
Pim timer dr-switch-delay	Whether the DR switch delay is set on the interface. This parameter is configured by the **pim ipv6 timer dr-switch-delay** command.
Pim hello periodic interval	Interval for the interface to send Hello messages. This parameter is configured by the **pim ipv6 timer hello** command.
Pim join-prune periodic interval	Interval for the interface to send Join/Prune messages. This parameter is configured by the **pim ipv6 timer join-prune** command.

Item	Description
Pim triggered-hello-delay	Maximum delay for the interface to send Hello messages. This parameter is configured by the **pim ipv6 triggered-hello-delay** command.
Pim version	Version of PIM enabled on the interface.
Pim ipsec sa	Whether PIM IPSec is enabled on the interface. The switch does not support this function.
Pim join-policy	Whether the join-policy is configured on the interface. This parameter is configured by the **pim ipv6 join-policy** command.
Pim neighbor-policy	Whether the neighbor-policy is configured on the interface. This parameter is configured by the **pim ipv6 neighbor-policy** command.

8.4.19 display default-parameter pim-ssm6

Function

The **display default-parameter pim-ssm6** command displays default configurations of PIM-SM (IPv6) for SSM.

Format

display default-parameter pim-ssm6

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The **display default-parameter pim-ssm6** command displays default configuration of PIM-SM (IPv6) for SSM. Even if the configuration of PIM-SM (IPv6) for SSM is modified, the **display default-parameter pim-ssm6** command still displays default parameter settings. This command helps you determine which parameters have been modified.

Example

Display default configuration of PIM-SM (IPv6) for SSM.

```
<HUAWEI> display default-parameter pim-ssm6
 PIM6 View Default Configurations:
 ---------------------------------
 Hello-option dr-priority: 1
 Hello-option holdtime: 105 s
 Hello-option lan-delay: 500 ms
 Hello-option neighbor-tracking: disabled
 Hello-option override-interval: 2500 ms
 Holdtime assert: 180 s
 Holdtime join-prune: 210 s
 Probe-interval: 5 s
 Register-policy: disabled
 Register-suppression-timeout: 60 s
 Source-lifetime: 210 s
 Source-policy: disabled
 Ssm-policy: disabled
 Hello periodic interval: 30 s
 Join-prune periodic interval: 60 s

 Interface View Default Configurations:
 --------------------------------------
 Pim bfd: disabled
 Pim hello-option dr-priority: 1
 Pim hello-option holdtime: 105 s
 Pim hello-option lan-delay: 500 ms
 Pim hello-option neighbor-tracking: disabled
 Pim hello-option override-interval: 2500 ms
 Pim holdtime assert: 180 s
 Pim holdtime join-prune: 210 s
 Pim require-genid: disabled
 Pim silent: disabled
 Pim timer dr-switch-delay: disabled
 Pim hello periodic interval: 30 s
 Pim join-prune periodic interval: 60 s
 Pim triggered-hello-delay: 5 s
 Pim version: 2
 Pim ipsec sa: disabled
 Pim join-policy: disabled
 Pim neighbor-policy: disabled
```

Table 8-56 Description of the **display default-parameter pim-ssm6** command output

Item	Description
PIM6 View Default Configurations	Default configurations in the PIM-IPv6 view.
Hello-option dr-priority	Priority for DR election. This parameter is configured by the **hello-option dr-priority (IPv6)** command.
Hello-option holdtime	Time period for the neighbor to hold the reachable state. This parameter is configured by the **hello-option holdtime (IPv6)** command.

Item	Description
Hello-option lan-delay	Delay in transmitting Prune messages at a shared network segment. This parameter is configured by the **hello-option lan-delay (IPv6)** command.
Hello-option neighbor-tracking	Whether neighbor tracking is enabled. This parameter is configured by the **hello-option neighbor-tracking (IPv6)** command.
Hello-option override-interval	Interval for sending Prune Override messages. This parameter is configured by the **hello-option override-interval (IPv6)** command.
Holdtime assert	Time period for holding the Assert state. This parameter is configured by the **holdtime assert (IPv6)** command.
Holdtime join-prune	Time period for holding the Join or Prune state. This parameter is configured by the **holdtime join-prune (IPv6)** command.
Probe-interval	Interval for sending Probe messages (empty Register messages) to the RP. This parameter is configured by the **probe-interval (IPv6)** command.
Register-policy	Whether the rule for filtering Register messages is configured. This parameter is configured by the **register-policy (IPv6)** command.
Register-suppression-timeout	Time period for holding the register-suppression state. This parameter is configured by the **register-suppression-timeout (IPv6)** command.
Source-lifetime	Timeout period of an (S, G) entry. This parameter is configured by the **source-lifetime (IPv6)** command.
Source-policy	Whether the rule for filtering multicast sources is configured. This parameter is configured by the **source-policy (IPv6)** command.
Ssm-policy	Whether the SSM group address range is set. This parameter is configured by the **ssm-policy (IPv6)** command.
Hello periodic interval	Interval for sending Hello messages. This parameter is configured by the **timer hello (IPv6)** command.

Item	Description
Join-prune periodic interval	Interval for sending Join/Prune messages. This parameter is configured by the **timer join-prune (IPv6)** command.
Interface View Default Configurations	Default configurations in the interface view.
Pim bfd	Whether the PIM BFD is enabled on the interface. This parameter is configured by the **pim ipv6 bfd enable** command.
Pim hello-option dr-priority	Priority for DR election on the interface. This parameter is configured by the **pim ipv6 hello-option dr-priority** command.
Pim hello-option holdtime	Time period for the neighbor on the interface to hold the reachable state. This parameter is configured by the **pim ipv6 hello-option holdtime** command.
Pim hello-option lan-delay	Delay in transmitting Prune messages at a shared network segment on the interface. This parameter is configured by the **pim ipv6 hello-option lan-delay** command.
Pim hello-option neighbor-tracking	Whether neighbor tracking is enabled on the interface. This parameter is configured by the **pim ipv6 hello-option neighbor-tracking** command.
Pim hello-option override-interval	Interval for the interface to send Prune Override messages. This parameter is configured by the **pim ipv6 hello-option override-interval** command.
Pim holdtime assert	Time period for the interface to hold the Assert state. This parameter is configured by the **pim ipv6 holdtime assert** command.
Pim holdtime join-prune	Time period for the interface to hold the Join or Prune state. This parameter is configured by the **pim ipv6 holdtime join-prune** command.
Pim require-genid	Whether the received Hello message is required to carry the Generation ID. This parameter is configured by the **pim ipv6 require-genid** command.
Pim silent	Whether PIM Silent is enabled on the interface. This parameter is configured by the **pim ipv6 silent** command.

Item	Description
Pim timer dr-switch-delay	Whether the DR switch delay is set on the interface. This parameter is configured by the **pim ipv6 timer dr-switch-delay** command.
Pim hello periodic interval	Interval for the interface to send Hello messages. This parameter is configured by the **pim ipv6 timer hello** command.
Pim join-prune periodic interval	Interval for the interface to send Join/Prune messages. This parameter is configured by the **pim ipv6 timer join-prune** command.
Pim triggered-hello-delay	Maximum delay for the interface to send Hello messages. This parameter is configured by the **pim ipv6 triggered-hello-delay** command.
Pim version	Version of PIM enabled on the interface.
Pim ipsec sa	Whether PIM IPSec is enabled on the interface. The switch does not support this function.
Pim join-policy	Whether the join-policy is configured on the interface. This parameter is configured by the **pim ipv6 join-policy** command.
Pim neighbor-policy	Whether the neighbor-policy is configured on the interface. This parameter is configured by the **pim ipv6 neighbor-policy** command.

8.4.20 display pim ipv6 bsr-info

Function

The **display pim ipv6 bsr-info** command displays the BSRs in a PIM-SM (IPv6) domain.

Format

display pim ipv6 bsr-info

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can use this command to check BSR configuration on a PIM-SM (IPv6) network.

Example

Display information about BSR in the current PIM-SM (IPv6) domain. If the switch is configured with C-BSR, information about the elected BSR and C-BSR is displayed.

```
<HUAWEI> display pim ipv6 bsr-info
VPN-Instance: public net
 Elected AdminScoped BSR Count: 0
 Elected BSR Address: FC00:0:0:2004::2
     Priority: 0
     Hash mask length: 128
     State: Elected
     Scope: 5
     Uptime: 00:00:07
     Next BSR message scheduled at: 00:00:53
     C-RP Count: 0
 Candidate AdminScoped BSR Count: 0
 Candidate BSR Address: FC00:0:0:2004::2
     Priority: 0
     Hash mask length: 128
     State: Elected
     Scope: 5
     Wait to be BSR: 0
```

Table 8-57 Description of the **display pim ipv6 bsr-info** command output

Item	Description
Elected AdminScoped BSR Count	number of elected AdminScoped BSRs.
Elected BSR Address	IPv6 address of the elected BSR.
Priority	Priority of the BSR.
Hash mask length	Mask length in the RP hash calculation.

Item	Description
State	Status of the BSR. ● Accept Preferred: No C-BSR is configured on the device and another device functions as a BSR and does not time out. ● Accept Any: No C-BSR is configured on the device and the current BSR times out (applicable to the situation that a BSR administrative domain is set) ● Candidate: A C-BSR is configured on a device and another device functions as a BSR. ● Pending: The device changes from the non-BSR state to the BSR state or a C-BSR is configured on the device and the current BSR times out. ● Elected: The device is elected as the BSR.
Scope	Scope ID of the BSR administrative domain served by a BSR. Not scoped indicates that the BSR is not an AdminScoped BSR.
Uptime	Period during which the BSR exists.
Next BSR message scheduled at	Period after which the next BSR message is sent. BSR messages are sent only when the timer maintained by the elected BSR times out.
C-RP Count	Number of RPs learned through the BSR.
Candidate AdminScoped BSR Count	Number of AdminScoped C-BSRs.
Candidate BSR Address	IPv6 Address of the C-BSR.
Wait to be BSR	Whether the current C-BSR is valid. The values are as follows: ● 0: The current C-BSR is valid. The current C-BSR takes part in the BSR election. ● 1: The current C-BSR is invalid. The current C-BSR does not take part in the BSR election. When the number of C-BSRs configured on the switch exceeds the threshold, the value is 1.

8.4.21 display pim ipv6 bfd session

Function

The **display pim ipv6 bfd session** command displays information about PIM IPv6 BFD sessions.

NOTE

Only the S5720I-SI, S5735-S, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6720S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Format

display pim ipv6 bfd session statistics

display pim ipv6 bfd session [**interface** *interface-type interface-number* | **neighbor** *ipv6-link-local-address*]*

Parameters

Parameter	Description	Value
statistics	Displays statistics about PIM IPv6 BFD sessions.	-
interface *interface-type interface-number*	Displays information about PIM IPv6 BFD sessions on a specified interface. *interface-type interface-number* specifies the type and number of an interface.	-
neighbor *ipv6-link-local-address*	Displays information about PIM IPv6 BFD sessions on a specified neighbor. *ipv6-link-local-address* specifies the link-local address of a PIM neighbor.	The value ranges from FE80:: to FE80:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF, in hexadecimal notation.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

After PIM BFD (IPv6) is configured to detect the status of PIM neighbors, a PIM IPv6 BFD session needs to be established. The **display pim ipv6 bfd session** command can be used to view statistics about and configurations of PIM IPv6 BFD sessions.

Precautions

The two ends of a BFD session negotiate the actual interval at which PIM IPv6 BFD packets are sent, the interval at which PIM IPv6 BFD packets are received, and the detection period based on the following negotiation mechanisms:

- The formula used to calculate the interval for sending PIM IPv6 BFD packets and the formula used to calculate the interval for receiving PIM IPv6 BFD packets are as follows:
  - Interval for sending PIM IPv6 BFD packets = Max (Local **min-tx-interval**, Remote **min-rx-interval**)
  - Interval for receiving PIM IPv6 BFD packets = Max (Remote **min-tx-interval**, Local **min-rx-interval**)
- The formula used to calculate the detection period is as follows:
  - Detection period = Remote **detect-multiplier** x Max (Remote **min-tx-interval**, Local **min-rx-interval**)

Example

Display information about PIM IPv6 BFD sessions on all interfaces.

```
<HUAWEI> display pim ipv6 bfd session
 VPN-Instance: public net
 Total 1 BFD session Created

 Vlanif100 (FE80::7): Total 1 BFD session Created

 Neighbor        ActTx(ms) ActRx(ms) ActMulti Local/Remote State
 FE80::6         200       300       4        8211/8214   Up
```

Display information about the PIM IPv6 BFD session on VLANIF 100.

```
<HUAWEI> display pim ipv6 bfd session interface vlanif 100
 VPN-Instance: public net

 Vlanif100 (FE80::7): Total 1 BFD session Created

 Neighbor        ActTx(ms) ActRx(ms) ActMulti Local/Remote State
 FE80::6         200       300       4        8211/8214   Up
```


Table 8-58 Description of the **display pim ipv6 bfd session** command output

Item	Description
Total 1 BFD session Created	Total number of established PIM IPv6 BFD sessions.
Vlanif100 (FE80::7)	PIM interface name (Link-local address).
Neighbor	IPv6 link-local address of a PIM neighbor.
ActTx(ms)	Actual interval for sending PIM IPv6 BFD packets.
ActRx(ms)	Actual interval for receiving PIM IPv6 BFD packets.
ActMulti	Actual detection multiplier of PIM IPv6 BFD packets.
Local/Remote	Local/remote discriminator of a PIM IPv6 BFD session.
State	Status of a PIM IPv6 BFD session: ● Up: indicates that the BFD session is set up successfully and detection packets are periodically exchanged. ● Init: indicates that the local end can communicate with the remote end and wants the session status to be Up. ● Admin down: indicates that the session is in the administratively Down state (The **shutdown** command is run in the BFD session view). ● Down: indicates that the BFD session is down.

Display statistics about PIM IPv6 BFD sessions.

```
<HUAWEI> display pim ipv6 bfd session statistics
 VPN-Instance: public net
  Total 1 PIM BFD session in this instance.

  Total 1 PIM BFD session up.
  Total 0 PIM BFD session down.
```

Table 8-59 Description of the display pim ipv6 bfd session statistics command output

Item	Description
Total 1 PIM BFD session in this instance	Total number of PIM IPv6 BFD sessions.
Total 1 PIM BFD session up	Total number of PIM IPv6 BFD sessions in the Up state.

Item	Description
Total 0 PIM BFD session down	Total number of PIM IPv6 BFD sessions in the Down state, that is, the total number of PIM IPv6 BFD sessions minus the number of PIM IPv6 BFD sessions in the Up state.

8.4.22 display pim ipv6 claimed-route

Function

The **display pim ipv6 claimed-route** command displays the unicast routing information used by PIM (IPv6).

Format

display pim ipv6 claimed-route [*ipv6-source-address*]

Parameters

Parameter	Description	Value
ipv6-source-address	Specifies the IPv6 address of a multicast source.	The address is in hexadecimal format.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The **display pim ipv6 claimed-route** command displays the unicast routes used by PIM (IPv6), such as the RPF neighbors, detailed information about interfaces, route types, and route selection policy.

Example

Display the unicast route of multicast source FC00:0:0:2001::2.

```
<HUAWEI> display pim ipv6 claimed-route fc00:0:0:2001::2
VPN-Instance: public net
multicast load-splitting rule: source-group
RPF information about: FC00:0:0:2001::2 in PIM-SM routing table
   RPF interface: Vlanif100, RPF neighbor: FE80::A01:100:1
   Referenced route/mask: FC00:0:0:2001::/64
   Referenced route type: igp
   RPF-route selecting rule: preference-preferred
   The (S, G) or (*, G) list dependent on this route entry
   (FC00:0:0:2001::2, FF03::1)
```


Table 8-60 Description of the **display pim ipv6 claimed-route** command output

Item	Description
multicast load-splitting rule	Mode in which multi-cast loads are split. The following policies apply: • group: multicast group-based load splitting • source: multicast source-based load splitting • source-group: multicast source and group-based load splitting • stable-preferred: stable-preferred load splitting • balance-preferred: balance-preferred load splitting
RPF information about: FC00:0:0:2001::2 in PIM-SM routing table	RPF routing information with the source address of FC00:0:0:2001::2 in the PIM-SM (IPv6) routing table
RPF interface	RPF interface in a routing entry.
RPF neighbor	RPF neighbor in a routing entry.
Referenced route/mask	Route/mask used by PIM.
Referenced route type	Type of a route.
RPF-route selecting rule	Preferred rule for selecting the RPF-route.
The (S, G) or (*, G) list dependent on this route entry	List of multicast entries based on RPF routes.

8.4.23 display pim ipv6 control-message counters

Function

The **display pim ipv6 control-message counters** command displays the number of sent and received PIM (IPv6) control messages.

Format

display pim ipv6 control-message counters message-type { **probe** | **register** | **register-stop** | **crp** }

display pim ipv6 control-message counters [**message-type** { **assert** | **graft** | **graft-ack** | **hello** | **join-prune** | **state-refresh** | **bsr** } | **interface** *interface-type interface-number*] *

Parameters

Parameter	Description	Value
message-type	Indicates the types of PIM control message.	-
probe	Indicates the Probe message.	-
register	Indicates the Register message.	-
register-stop	Indicates the Register-stop message.	-
crp	Indicates the C-RP message.	-
assert	Indicates the Assert message.	-
graft	Indicates the Graft message.	-
graft-ack	Indicates the Graft-ack message.	-
hello	Indicates the Hello message.	-
join-prune	Indicates the Join-prune message.	-
state-refresh	Indicates the State-Refresh message.	-
bsr	Indicates the BSR message.	-
interface *interface-type interface-number*	Indicates the type and number of an interface.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

When multicast forwarding fails on a PIM (IPv6) network, run the **display pim control-message counters** command to view statistics about protocol packets. The command output helps you locate faults.

Example

Display the number of PIM (IPv6) control messages that were sent and received on VLANIF100.

```
<HUAWEI> display pim ipv6 control-message counters interface vlanif 100
VPN-Instance: public net
 PIM control-message counters for interface: Vlanif100
 Message Type     Received        Sent            Invalid     Filtered
 Assert           0               0               0           0
 Graft            0               0               0           0
 Graft-Ack        0               0               0           0
 Hello            328             331             0           0
 Join-prune       2               0               0           0
 State-Refresh    0               0               0           0
 BSR              9778            0               0           0
```


Table 8-61 Description of the **display pim ipv6 control-message counters** command output

Item	Description
PIM control-message counters for interface	Name of the interface for collecting statistics on PIM control messages
Message Type	Type of the control messages.
Received	Number of control messages received by the current interface.
Sent	Number of control messages sent by the current interface.
Invalid	Number of invalid control packets.
Filtered	Number of control messages filtered out by the current interface.
Assert	Number of Assert messages.
Graft	Number of Graft messages.
Graft-Ack	Number of Graft-Ack messages.
Hello	Number of Hello messages.
Join-prune	Number of Join/Prune messages.
State-Refresh	Number of State-Refresh messages.
BSR	Number of Bootstrap messages.

8.4.24 display pim ipv6 grafts

Function

The **display pim ipv6 grafts** command displays the information about unacknowledged PIM-DM (IPv6) Graft messages.

Format

display pim ipv6 grafts

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

In PIM-DM (IPv6), after sending the Graft message, the switch needs to wait to receive the Graft-Ack message from the upstream device.

You can run the **display pim ipv6 grafts** command to view the information about the PIM-DM (IPv6) Graft messages sent but unacknowledged.

Example

Display the unacknowledged PIM-DM (IPv6) graft messages.

```
<HUAWEI> display pim ipv6 grafts
Source                Group                 Expire    RetransmitIn
fc00:0:0:2001::2      ff03::101               00:02:52  00:00:02
```

Table 8-62 Description of the **display pim ipv6 grafts** command output

Item	Description
Source	Multicast source address.
Group	Multicast group address.
Expire	Timeout period of an (S, G) entry.
RetransmitIn	Amount of time before the next Graft message is transmitted.

8.4.25 display pim ipv6 interface

Function

The **display pim ipv6 interface** command displays information about PIM (IPv6) on an interface.

Format

display pim ipv6 interface [*interface-type interface-number* | **up** | **down**] [**verbose**]

Parameters

Parameter	Description	Value
interface-type interface-number	Indicates the type and number of an interface.	-

Parameter	Description	Value
up	Indicates that the IPv6 status is Up on the PIM interface.	-
down	Indicates that the IPv6 status is Down on the PIM interface.	-
verbose	Indicates detailed information about a PIM (IPv6) interface.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

An interface enabled with PIM (IPv6) is called a PIM (IPv6) interface. The **display pim ipv6 interface** command is used to display information about PIM (IPv6) interfaces, including status of the PIM (IPv6) interface, the number of PIM (IPv6) neighbors, interval at which Hello messages are sent, DR priority, and DR address.

Example

Display PIM (IPv6) information on VLANIF100.

```
<HUAWEI> display pim ipv6 interface vlanif 100
 VPN-Instance: public net
 Interface          State NbrCnt HelloInt   DR-Pri     DR-Address
 Vlanif100            up    0      30         1        FE80::2E0:3FFF:FE27:AE01(local)
```

Table 8-63 Description of the display pim ipv6 interface command output

Item	Description
Interface	Name of the PIM (IPv6) interface.
State	Status of the PIM (IPv6) interface, up or down.
NbrCnt	Number of PIM (IPv6) neighbors on the interface.
HelloInt	Interval for sending Hello messages, in seconds.
DR-Pri	DR priority.
DR-Address	DR address.

Display detailed information about PIM (IPv6) on VLANIF100.

```
<HUAWEI> display pim ipv6 interface vlanif 100 verbose
 VPN-Instance: public net
 Interface: Vlanif100, FE80::2E0:3FFF:FE27:AE01
    PIM version: 2
    PIM mode: Sparse
    PIM state: up
    PIM DR: FE80::2E0:3FFF:FE27:AE01 (local)
    PIM DR Priority (configured): 1
    PIM neighbor count: 0
    PIM hello interval: 30 s
    PIM LAN delay (negotiated): 500 ms
    PIM LAN delay (configured): 500 ms
    PIM hello override interval (negotiated): 2500 ms
    PIM hello override interval (configured): 2500 ms
    PIM Silent: disabled
    PIM neighbor tracking (negotiated): disabled
    PIM neighbor tracking (configured): disabled
    PIM generation ID: 0x18FF94EC
    PIM require-GenID: disabled
    PIM hello hold interval: 105 s
    PIM assert hold interval: 180 s
    PIM triggered hello delay: 5 s
    PIM J/P interval: 60 s
    PIM J/P hold interval: 210 s
    PIM BSR domain border: disabled
    PIM BFD: disabled
    PIM dr-switch-delay timer : not configured
    Number of routers on link not using DR priority: 0
    Number of routers on link not using LAN delay: 0
    Number of routers on link not using neighbor tracking: 1
    ACL of PIM neighbor policy: myacl6
    ACL of PIM ASM join policy: 2000
    ACL of PIM SSM join policy: -
    ACL of PIM join policy: -
```

Table 8-64 Description of the **display pim ipv6 interface verbose** command output

Item	Description
PIM version	Version number of PIM (IPv6) enabled on the interface.
PIM mode	PIM mode.
PIM state	Status of the PIM (IPv6) interface, up or down.
PIM DR	DR address on the interface.
PIM DR Priority (configured)	Configured DR priority on the interface.
PIM neighbor count	Number of PIM (IPv6) neighbors on the interface.
PIM hello interval	Interval for sending Hello messages.
PIM LAN delay (negotiated)	Negotiated delay for transmitting packets on the interface.
PIM LAN delay (configured)	Configured delay for transmitting packets on the interface.

Item	Description
PIM hello override interval (negotiated)	Negotiated override interval on the interface.
PIM hello override interval (configured)	Configured override interval on the interface.
PIM Silent	Whether the PIM Silent (IPv6) function is enabled on the interface.
PIM neighbor tracking (negotiated)	Whether the PIM (IPv6) neighbor tracking function is enabled on the interface after negotiation.
PIM neighbor tracking (configured)	Whether the PIM (IPv6) neighbor tracking function is configured on the interface.
PIM generation ID	Generation ID option on the interface.
PIM require-GenID	Whether the function of rejecting the Hello messages without the Generation ID option is enabled.
PIM hello hold interval	Interval for the receiver of the Hello message to keep its neighbor reachable.
PIM assert hold interval	Interval for sending Assert messages.
PIM triggered hello delay	Maximum random delay for triggering Hello messages.
PIM J/P interval	Interval for the interface to send Join/Prune messages.
PIM J/P hold interval	Period for holding the Join/Prune status on the interface.
PIM BSR domain border	Whether the BSR domain boundary is configured on the interface.
PIM dr-switch-delay timer	DR switching delay.
Number of routers on link not using DR priority	Number of switches that do not use DR priority in all the network segments connected to the interface.
Number of routers on link not using LAN delay	Number of switches that do not use LAN delay in all the network segments connected to the interface.
Number of routers on link not using neighbor tracking	Number of switches that are not enabled with the neighbor tracing function in the network segment where the interface resides.
ACL of PIM neighbor policy	Neighbor filtering policy configured on the interface.

Item	Description
ACL of PIM ASM join policy	ASM Join information filtering policy configured on the interface.
ACL of PIM SSM join policy	SSM Join information filtering policy configured on the interface.
ACL of PIM join policy	Join information filtering policy configured on the interface.

8.4.26 display pim ipv6 invalid-packet

Function

The **display pim ipv6 invalid-packet** command displays statistics about invalid PIM (IPv6) messages received by a device and details of these messages.

Format

display pim ipv6 invalid-packet [**interface** *interface-type interface-number* | **message-type** { **assert** | **bsr** | **hello** | **join-prune** | **graft** | **graft-ack** | **state-refresh** }] *

display pim ipv6 invalid-packet message-type { **crp** | **register** | **register-stop** }

display pim ipv6 invalid-packet [*packet-number*] **verbose**

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Displays statistics about invalid PIM (IPv6) messages received by a specified interface. *interface-type interface-number* specifies the interface type and interface number.	-
message-type	Displays statistics about invalid PIM (IPv6) messages of a specific type.	-
assert	Displays statistics about invalid Assert messages.	-
bsr	Displays statistics about invalid BSR messages.	-
hello	Displays statistics about invalid Hello messages.	-

Parameter	Description	Value
join-prune	Displays statistics about invalid Join/Prune messages.	-
graft	Displays statistics about invalid Graft messages.	-
graft-ack	Displays statistics about invalid Graft-Ack messages.	-
state-refresh	Displays statistics about invalid State-Refresh messages.	-
crp	Displays statistics about invalid C-RP messages.	-
register	Displays statistics about invalid Register messages.	-
register-stop	Displays statistics about invalid Register-Stop messages.	-
packet-number	Displays details of a specified number of invalid PIM (IPv6) messages recently received.	The value is an integer that ranges from 1 to 100. By default, details of all the invalid PIM (IPv6) messages currently stored are displayed.
verbose	Displays details of invalid PIM (IPv6) messages.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

When a fault occurs on a PIM (IPv6) network, use the **display pim ipv6 invalid-packet** command to check statistics and details about invalid PIM (IPv6) packets. The command output can help you locate the fault.

If PIM (IPv6) entries fail to be generated on a multicast network, you can run the **display pim ipv6 invalid-packet** command first to check whether devices have received invalid PIM (IPv6) messages. If the command output contains statistics about invalid PIM (IPv6) messages, run the **display pim ipv6 invalid-packet** [*packet-number*] **verbose** command to view details of invalid PIM (IPv6) messages to locate the fault.

You can run the following related commands to view information about specific invalid IPv6 PIM messages:

- Run the **display pim ipv6 invalid-packet** command to view statistics about invalid IPv6 PIM messages received by a device in the public network instance.
- Run the **display pim ipv6 invalid-packet interface** *interface-type interface-number* command to view statistics about invalid IPv6 PIM messages received by a specified interface.
- Run the **display pim ipv6 invalid-packet** *packet-number* **verbose** command to view details of invalid IPv6 PIM messages recently received. Currently, details of a maximum of 100 invalid IPv6 PIM messages can be displayed.

Example

Display statistics about invalid PIM (IPv6) messages received by a device.

```
<HUAWEI> display pim ipv6 invalid-packet

            Statistics of invalid packets for public net:
------------------------------------------------------------------------
PIM General invalid packet: Invalid PIM Version     : 0          Invalid PIM Type       : 0 Fault Length          :
0          Bad Checksum           : 0
PIM Register invalid packet:
Invalid Multicast Source: 0          Invalid Multicast Group : 0
Invalid Dest Addr       : 0

PIM Register-Stop invalid packet:
Invalid Multicast Source: 0          Invalid Multicast Group : 0
Invalid Dest Addr       : 0          IP Source not RP        : 0

PIM CRP invalid packet:
Invalid Dest Addr       : 0          Invalid CRP Addr        : 0
Fault Length            : 0          CRP Adv Fault Length    : 0
Invalid Multicast Group : 0

PIM Assert invalid packet:
Invalid Dest Addr       : 0          Invalid IP Source Addr  : 0
Invalid Multicast Source: 0          Invalid Multicast Group : 0

PIM BSR invalid packet:
Bad Payload             : 0          Fault Length            : 0
Bad Scope Mask          : 0          Invalid Multicast Group : 0
Not CBSR But BSR        : 0          Invalid BSR Addr        : 0
Fault Hash Length       : 0          Invalid IP Source Addr  : 0

PIM Hello invalid packet:
Invalid Addr List       : 0          Fault Length            : 0
Bad Holdtime Length     : 0          Bad LanPruneDelay Length: 0
Bad DrPriority Length   : 0          Bad GenID Length        : 0
Invalid Dest Addr       : 0          Invalid IP Source Addr  : 0

PIM Join/Prune invalid packet:
Invalid Multicast Source: 0          Invalid Multicast Group : 0
Invalid Up Neighbor     : 0          Invalid IP Source Addr  : 0
Invalid Dest Addr       : 0          Fault Length            : 0
 PIM Graft invalid packet: Invalid Multicast Source: 0          Invalid Multicast Group : 0 Invalid Up
```



```
Neighbor     : 0          Invalid IP Source Addr  : 0 Fault Length          : 0  PIM Graft-Ack invalid packet:
Invalid Multicast Source: 0          Invalid Multicast Group : 0 Invalid Up Neighbor     : 0          Invalid IP
Source Addr  : 0 Fault Length          : 0  PIM State Refresh invalid packet: Invalid Multicast Source: 0
Invalid Multicast Group : 0 Invalid Originator Addr : 0          Fault Length          : 0
------------------------------------------------------------------
```

Table 8-65 Description of the **display pim ipv6 invalid-packet** command output

Item	Description
PIM General invalid packet	Number of general invalid PIM (IPv6) messages.
Invalid PIM Version	Number of messages with invalid PIM (IPv6) version.
Invalid PIM Type	Number of messages with invalid PIM (IPv6) message type.
Fault Length	Number of messages with invalid lengths.
Bad Checksum	Number of messages with invalid checksum.
PIM Register invalid packet	Number of PIM Register messages.
Invalid Multicast Source	Number of messages with invalid multicast source addresses.
Invalid Multicast Group	Number of messages with invalid multicast group addresses.
Invalid Dest Addr	Number of messages with invalid destination addresses.
PIM Register-Stop invalid packet	Number of invalid Register-Stop messages.
IP Source not RP	Number of messages whose source addresses are not the RP address.
PIM CRP invalid packet	Number of invalid C-RP messages.
Invalid CRP Addr	Number of messages with invalid C-RP addresses.
CRP Adv Fault Length	Number of messages with CRP Adv fields of invalid lengths.
PIM Assert invalid packet	Number of invalid Assert messages.
Invalid IP Source Addr	Number of messages with invalid source addresses.
PIM BSR invalid packet	Number of invalid BSR messages.
Bad Payload	Number of messages with invalid payloads.
Bad Scope Mask	Number of messages with invalid scope masks.

Item	Description
Not CBSR But BSR	Number of messages received from non-C-BSRs.
Invalid BSR Addr	Number of messages with invalid BSR addresses.
Fault Hash Length	Number of messages whose hash mask fields of invalid lengths.
PIM Hello invalid packet	Number of invalid Hello messages.
Invalid Addr List	Number of messages with invalid address lists.
Bad Holdtime Length	Number of messages whose Holdtime fields are of invalid lengths.
Bad LanPruneDelay Length	Number of messages whose LanPruneDelay fields are of invalid lengths.
Bad DrPriority Length	Number of messages with DrPriority fields of invalid lengths.
Bad GenID Length	Number of messages with GenerationID fields of invalid lengths.
PIM Join/Prune invalid packet	Number of invalid Join/Prune messages.
Invalid Up Neighbor	Number of messages with invalid upstream neighbors.
PIM Graft invalid packet	Number of invalid Graft messages.
PIM Graft-Ack invalid packet	Number of invalid Graft-Ack messages.
PIM State Refresh invalid packet	Number of invalid State-Refresh messages.
Invalid Originator Addr	Number of messages with invalid Originator address.

Display details of one invalid PIM (IPv6) message recently received lately.

```
<HUAWEI> display pim ipv6 invalid-packet 1 verbose
      Detailed information of invalid packets
------------------------------------------------------
Packet information (Index 1):
------------------------------------------------------
Interface          :  Vlanif100
Time               :  2012-06-01 20:04:35 UTC-08:00
Message Length     :  26
Invalid Type       :  Invalid Multicast Source
0000: 25 00 96 77 01 00 00 20 e1 01 01 01 01 00 e0 00
0010: 00 00 80 00 00 64 00 00 00 00
------------------------------------------------------
```


Table 8-66 Description of the display pim ipv6 invalid-packet 1 verbose command output

Item	Description
Detailed information of invalid packets	Details about invalid PIM (IPv6) messages.
Packet information (Index 1)	Sequence number of an invalid PIM (IPv6) message (numbered in the opposite order).
Interface	Number of interfaces that receive the invalid PIM (IPv6) message.
Time	Time when the invalid SPT switch message was received, in any of the following formats: ● YYYY-MM-DD HH:MM:SS ● YYYY-MM-DD HH:MM:SS UTC±HH:MM DST ● YYYY-MM-DD HH:MM:SS UTC±HH:MM ● YYYY-MM-DD HH:MM:SS DST The format UTC±HH:MM indicates that a time zone was configured with the **clock timezone** command; DST indicates that the daylight saving time is configured through **clock daylight-saving-time** command.
Message Length	Length of the invalid PIM (IPv6) message.
Invalid Type	Type of the invalid PIM (IPv6) message.
0000: 25 00 96 77 01 00 00 20 e1 01 01 01 01 00 e0 00 0010: 00 00 80 00 00 64 00 00 00 00	Contents of the invalid PIM (IPv6) message.

8.4.27 display pim ipv6 neighbor

Function

The **display pim ipv6 neighbor** command displays information about PIM (IPv6) neighbors.

Format

display pim ipv6 neighbor [*ipv6-link-local-address* | **interface** *interface-type interface-number* | **verbose**] *

Parameters

Parameter	Description	Value
ipv6-link-local-address	Specifies the IPv6 link-local address of a neighbor.	The value ranges from FE80:: to FE80:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF, in hexadecimal notation.
interface *interface-type interface-number*	Specifies the type and number of an interface.	-
verbose	Indicates the details of PIM neighbors.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The **display pim ipv6 neighbor** command displays PIM (IPv6) neighbor information, including the number of PIM (IPv6) neighbors and DR priorities of neighbors. You can adjust PIM (IPv6) neighbor relationships according to the command output.

Example

Display detailed information about PIM (IPv6) neighbors on VLANIF100.

```
<HUAWEI> display pim ipv6 neighbor interface vlanif 100 verbose
 VPN-Instance: public net

 Total Number of Neighbors on this interface  = 1

Neighbor: FE80::FFE0:FFFF:FE4A:8E04
    Interface: Vlanif100
    Uptime: 00:01:18
    Expiry time: 00:01:31
    DR Priority: 1
    Generation ID: 0x7751638D
    Holdtime: 105 s
    LAN delay: 500 ms
    Override interval: 2500 ms
    Neighbor tracking: disabled
    PIM BFD-session: N
    Neighbor Secondary Address(es):
    FC00:0:0:2004::2
```


Table 8-67 Description of the **display pim ipv6 neighbor** command output

Item	Description
Total Number of Neighbors on this interface	Total number of PIM (IPv6) neighbors on an interface.
Neighbor	Address of a PIM (IPv6) neighbor.
Interface	Interface where the PIM (IPv6) neighbor resides.
Uptime	How long has the PIM (IPv6) neighbor been in Up state.
Expiry time	How soon the PIM (IPv6) neighbor will time out.
DR Priority	DR priority of the PIM (IPv6) neighbor.
Generation ID	Indicates the randomly generated 32-bit value of PIM (IPv6) neighbor.
Holdtime	Keepalive period of the PIM (IPv6) neighbor.
LAN delay	Delay in transmitting Prune messages.
Override interval	Interval for overriding the Prune action.
Neighbor tracking	Whether the neighbor tracking neighbor function is enabled.
PIM BFD-session	Whether a BFD session is set up.
Neighbor Secondary Address (es)	IPv6 address of the neighbor.

8.4.28 display pim ipv6 routing-table

Function

The **display pim ipv6 routing-table** command displays the PIM (IPv6) multicast routing table.

Format

display pim ipv6 routing-table [*ipv6-source-address* [**mask** *mask-length*] | *ipv6-group-address* [**mask** *mask-length*] | **flags** *flag-value* | **fsm** | **incoming-interface** { *interface-type interface-number* | **register** } | **mode** { **dm** | **sm** | **ssm** } | **outgoing-interface** { **exclude** | **include** | **match** } { *interface-type interface-number* | **none** | **register** }] * [**outgoing-interface-number** [*number*]]

display pim ipv6 routing-table brief [*ipv6-source-address* [**mask** *mask-length*] | *ipv6-group-address* [**mask** *mask-length*] | **incoming-interface** { *interface-type interface-number* | **register** }] *

Parameters

Parameter	Description	Value
ipv6-source-address	Specifies the IPv6 address of a multicast source.	The address is a 32-digit hexadecimal number, in the format X:X:X:X:X:X:X:X.
ipv6-group-address	Specifies the IPv6 address of a multicast group address.	The address is a 32-digit hexadecimal number, in the format X:X:X:X:X:X:X:X. An IPv6 multicast address starts with FF.
mask *mask-length*	Specifies the mask length of a multicast source or group.	The value is an integer. The mask length of a multicast source ranges from 0 to 128. The mask length of a multicast group ranges from 8 to 128.
flags *flag-value*	Displays of routing entries of a specified type. *flag-value* specifies the flag of a routing entry.	-
fsm	Displays detailed information about the finite state machine (FSM).	-
incoming-interface	Displays the routing entry with the specified upstream interface.	-
interface-type interface-number	Specifies the type and number of an interface.	-
register	Displays the register interface.	-
dm	Displays PIM-DM (IPv6) routing entries.	-
sm	Displays PIM-SM (IPv6) routing entries.	-
ssm	Displays PIM-SSM (IPv6) routing entries.	-

Parameter	Description	Value
outgoing-interface { **exclude** | **include** | **match** }	Displays the routing entries with or without a specified outbound interface. • exclude: displays the entries that do not contain the specified interface. • include: displays the entries that contain the specified interface. • match: displays the entries match the specified interface.	-
none	Displays the routing entry without the downstream interface.	-
outgoing-interface-number	Displays the number of the outbound interfaces of routing entries.	-
number	Specifies the number of the outbound interfaces to be queried.	-
brief	Displays only the name of upstream interface and the number of downstream interfaces of routing entries.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can use this command to:

- Check whether PIM (IPv6) has been configured successfully on the network.
- Check the inbound interfaces, outbound interfaces, flags, and other information in the routing entries to identify failure points when forwarding errors occur on the PIM (IPv6) network.

The PIM (IPv6) routing table includes both (*, G) and (S, G) entries. (*, G) entries are used to set up a rendezvous point tree (RPT), and (S, G) entries are used to set up a shortest path tree (SPT).

Table 8-68 lists the values of the **flags** *flag-value* parameter.

Table 8-68 Values of the *flag-value* parameter

Item	Description
act	Indicates that the multicast routing entry at which actual data arrives exists.
del	Indicates the multicast routing entry to be deleted.
exprune	Indicates that the entry on the RPT is pruned and no receiver on the RPT requests the information sent by the source.
ext	Indicates routing entries that contain downstream interfaces provided by other multicast routing protocols.
loc	Indicates routing entries on the switch directly connected to the network segment where the source resides.
niif	Indicates routing entries with unknown upstream interfaces.
nonbr	Indicates that the routing entry of the upstream neighbor address (link-local address) towards the RP or the source is not found.
none	Indicates routing entries without any flag.
rpt	Indicates the routing entries that are on the RPT but do not use the RPT data.
sg_rcvr	Indicates that the (S, G) receiver of S exists on the local switch and PIM (IPv6) is the owner of the downstream interface.
sgjoin	Indicates that the (S, G) receiver of S exists on the local switch and PIM (IPv6) is not the owner of the downstream interface.
spt	Indicates routing entries on the shortest path tree (SPT).
swt	Indicates routing entries during the SPT switchover.
upchg	Indicates a route change has occurred. The current entry uses the original upstream interface to forward data and waits for data received from a new interface.
wc	Indicates a (*, G) entry.

Example

Display the PIM (IPv6) multicast routing table.

```
<HUAWEI> display pim ipv6 routing-table
 VPN-Instance: public net
 Total 1 (*, G) entry; 1 (S, G) entry

 (*, FFE3::1)
     RP: FC00:0:0:1::1
     Protocol: pim-sm, Flag: WC
     UpTime: 00:57:31
     Upstream interface: NULL
         Upstream neighbor: NULL
```



```
    RPF prime neighbor: NULL
  Downstream interface(s) information:
  Total number of downstreams: 1
    1: Vlanif10
      Protocol: static, UpTime: 00:57:31, Expires: never

(FC00:0:0:2001::2, FFE3::1)
  RP: FC00:0:0:1::1
  Protocol: pim-sm, Flag: ACT WC
  UpTime: 00:04:24
    1: Vlanif20
    Upstream neighbor: FE80::A01:100:1
    RPF prime neighbor: FE80::A01:100:1
  Downstream interface(s) information:
  Upstream interface: Vlanif10
        Protocol: pim-dm, UpTime: 00:04:24, Expires:  -
```

Table 8-69 Description of the **display pim ipv6 routing-table** command output

Item	Description
Total 1 (*, G) entry; 1 (S, G) entry	Total number of the (S, G) entries and (*, G) entries in the PIM routing table.
(*, FFE3::1)	(*, G) entry in the PIM routing table.
RP	RP address.
Protocol	Type of PIM (IPv6) protocols, PIM-DM (IPv6), PIM-SM (IPv6), or PIM-SSM (IPv6).
Flag	Flag of a (S, G) entry or (*, G) entry in the PIM (IPv6) routing table.
UpTime	Lifetime of an interface.
Upstream interface	Upstream interface of a (S, G) entry or (*, G) entry.
Upstream neighbor	Upstream neighbor of a (S, G) entry or (*, G) entry.
RPF prime neighbor	RPF neighbor of a (S, G) entry or (*, G) entry. • For a (*, G) entry, when the local device is an RP, the RPF neighbor is Null. • For a (S, G) entry, when the local device is directly connected to the multicast source, the RPF neighbor is Null.

Item	Description
Downstream interface(s) information	Information about downstream interfaces, including: • Number of downstream interfaces • Names of downstream interfaces • Type of the PIM (IPv6) protocol configured on the downstream interfaces • Existing period and timeout period of downstream interfaces
Total number of downstreams	Number of downstream interfaces.
Vlanif10	Interface name.
Expires	Timeout period of an entry.

Display the brief information about PIM (IPv6) routing entries.

```
<HUAWEI> display pim ipv6 routing-table brief FF25::1
 VPN-Instance: public net
 Total 3 (*, G) entries; 3 (S, G) entries

 Total matched 1 (*, G) entry; 1 (S, G) entry

 00001. (FC00:0:0:2008::55, FF25::1)
     Upstream interface: Vlanif10
     Number of downstreams: 2
 00002. (*, FF25::1)
     Upstream interface: Vlanif10
     Number of downstreams: 2
```

Table 8-70 Description of the display pim ipv6 routing-table brief command output

Item	Description
Total 3 (*, G) entries; 3 (S, G) entries	Total number of the (S, G) entries and (*, G) entries in the PIM (IPv6) routing table.
Total matched 1 (*, G) entry; 1 (S, G) entry	Total number of the (S, G) entries and (*, G) entries that meet the query conditions in the PIM routing table.
00001. (FC00:0:0:2008::55, FF25::1)	(S, G) entry.
Number of downstreams	Number of downstream interfaces in (S, G) entries or (*, G) entries.

Display the number of the outbound interfaces of PIM (IPv6) routing entries.

```
<HUAWEI> display pim ipv6 routing-table outgoing-interface-number
 VPN-Instance: public net
```



```
Total 2 (*, G) entries; 0 (S, G) entry

(*, FF25::1)
    RP: FC00:0:0:2008::5:3:2 (local)
    Protocol: pim-sm, Flag: WC
    UpTime: 00:00:04
    Upstream interface: Register
        Upstream neighbor: NULL
        RPF prime neighbor: NULL
    Downstream interface(s) information:
    Total number of downstreams: 2

(*, FF25::2)
    RP: FC00:0:0:2008::5:3:2 (local)
    Protocol: pim-sm, Flag: WC
    UpTime: 00:00:05
    Upstream interface: Register
        Upstream neighbor: NULL
        RPF prime neighbor: NULL
    Downstream interface(s) information:
    Total number of downstreams: 2
```

8.4.29 display pim ipv6 rp-info

Function

The **display pim ipv6 rp-info** command displays information about the RP corresponding to a multicast group.

Format

display pim ipv6 rp-info [*ipv6-group-address*]

Parameters

Parameter	Description	Value
ipv6-group-address	Specifies a multicast group address.	The address is a 32-digit hexadecimal number, in the format X:X:X:X:X:X:X:X. An IPv6 multicast address starts with FF.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

The **display pim ipv6 rp-info** command displays information about the RP to which a multicast group corresponds. This command can help determine whether multicast forwarding errors are caused by faults of an RP.

Precautions

The RP information contains the information about the RP discovered through the BSR mechanism and static RP.

If the group address is not specified in this command, the corresponding RP information of all the multicast groups is displayed.

Example

Display the RP of multicast group FF1E::1.

```
<HUAWEI> display pim ipv6 rp-info ff1e::1
 VPN-Instance: public net
 BSR RP Address is: FE1E::1
     Priority: 192
     Uptime: 00:00:52
     Expires: 00:01:38
 RP mapping for this group is: FC00:0:0:2001::1 (local host)
```

Table 8-71 Description of the **display pim ipv6 rp-info** command output

Item	Description
VPN-Instance	VPN instance to which RP information belongs. **public net** indicates the public network instance.
BSR RP Address is	IP address of a dynamical RP
Priority	RP priority
Uptime	Period during which the RP exists
Expires	Time before an RP times out
RP mapping for this group is	Address of the RP to which multicast group corresponds

8.4.30 embedded-rp

Function

The **embedded-rp** command enables the embedded RP function.

The **undo embedded-rp** command disables the embedded RP function.

By default, the embedded RP function is enabled.

Format

embedded-rp [*basic-acl6-number*]

undo embedded-rp [*basic-acl6-number*]

Parameters

Parameter	Description	Value
basic-acl6-number	Specifies the number of the basic ACL.	The value is an integer that ranges from 2000 to 2999.

Views

PIM-IPv6 view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The embedded RP function is enabled by default after PIM-SM (IPv6) is enabled. This function enables the switch to obtain the RP address from the IPv6 multicast address of a received multicast packet, so that the switch does not need to know the RP information beforehand.

By default, the switch can parse group addresses in the range of FF7x::/12. The value of x can be 0 or any integer in the range of 3 to F. When the switch receives a multicast packet with an IPv6 group address in this range, the switch can obtain the RP address from the IPv6 group address. This RP will replace the static RP or dynamically elected RP. If you do not want the switch to use RP information obtained from IPv6 multicast addresses of multicast packets, run the **undo embedded-rp** command to disable the embedded RP function.

Prerequisites

IPv6 multicast routing has been enabled globally using the **multicast ipv6 routing-enable** command in the system view.

Precautions

If an IPv6 ACL is specified in the command, the final group address range for embedded RP is the intersection of the group address range specified by the IPv6 ACL and the default group address range. All the devices in the PIM (IPv6) domain must be configured with the same group address range.

The **embedded-rp** command and the **acl** command are used together.

- For the IPv6 numbered ACL, in the ACL6 view, you can set the source address range of multicast groups that is enabled with the embedded RP by specifying the **source** parameter in the **rule** command.
- For the IPv6 Named ACL, in the ACL6 view, when the **rule** command is used to configure a filtering rule, the filtering rule is effective only with the address range of multicast groups that is specified by the **destination** parameter and with the time period that is specified by the **time-range** parameter.

This command is cyclical in nature. That is, the latest command overwrites the previous one, and takes effect.

Example

Enable the embedded RP function on multicast group ff73::.

```
<HUAWEI> system-view
[HUAWEI] acl ipv6 number 2000
[HUAWEI-acl6-basic-2000] rule permit source ff73:: 12
[HUAWEI-acl6-basic-2000] quit
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] pim-ipv6
[HUAWEI-pim6] embedded-rp 2000
```

8.4.31 graceful-restart (IPv6)

Function

The **graceful-restart** command enables PIM GR.

The **undo graceful-restart** command disables PIM GR.

By default, PIM GR is not enabled.

Format

graceful-restart

undo graceful-restart

Parameters

None

Views

PIM-IPv6 view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If a stack is used on the PIM-SM (IPv6) network, multicast data transmission is interrupted after an active/standby switchover occurs in the stack, because the slave switch on the new master device does not have PIM (IPv6) forwarding entries.

PIM GR enables the system to back up join and prune information in PIM (IPv6) routing entries to the new master device when an active/standby switchover is performed in the system. This ensures normal multicast data forwarding during restoration of the multicast distribution tree. For details about stack configuration, see Stack Configuration in the *S300, S500, S2700, S5700, and S6700 V200R023C00 Configuration Guide - Device Management*.

Prerequisites

IPv6 multicast routing has been enabled globally using the **multicast ipv6 routing-enable** command in the system view.

Precautions

At least one interface must have PIM-SM (IPv6) enabled for the **graceful-restart** command to take effect.

Example

Enable PIM GR in the PIM-IPv6 view.

```
<HUAWEI> system-view
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] pim-ipv6
[HUAWEI-pim6] graceful-restart
```

8.4.32 graceful-restart period (IPv6)

Function

The **graceful-restart period** command configures the minimum PIM GR period.

The **undo graceful-restart period** command restores the default minimum PIM GR period.

By default, the minimum PIM GR period is 120 seconds.

Format

graceful-restart period *period*

undo graceful-restart period

Parameters

Parameter	Description	Value
period	Specifies the minimum PIM GR period.	The value is an integer that ranges from 90 to 3600 in seconds.

Views

PIM-IPv6 view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **graceful-restart period** command ensures the minimum time for maintaining forwarding entries.

Prerequisites

IPv6 multicast routing has been enabled globally using the **multicast ipv6 routing-enable** command in the system view.

Precautions

Unicast protocol GR forms the basis of PIM GR; therefore, the minimum PIM GR period should be longer than the corresponding unicast protocol GR period.

The PIM GR period also depends on the complexity of the network topology and increases with the expansion of unicast route capacity and multicast route capacity.

Example

Set the minimum PIM GR period in the PIM-IPv6 view to 150 seconds.

```
<HUAWEI> system-view
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] pim-ipv6
[HUAWEI-pim6] graceful-restart
[HUAWEI-pim6] graceful-restart period 150
```

8.4.33 hello-option dr-priority (IPv6)

Function

The **hello-option dr-priority** command configures the designated router (DR) priority for the switch.

The **undo hello-option dr-priority** command restores the default DR priority.

By default, the DR priority for the switch is 1.

Format

hello-option dr-priority *priority*

undo hello-option dr-priority

Parameters

Parameter	Description	Value
priority	Specifies the DR priority of the switch.	The value is an integer that ranges from 0 to 4294967295. The greater the value, the higher the priority.

Views

PIM-IPv6 view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On an IPv6 PIM-SM network, switches on a shared network segment are candidates for the DR. The DR is responsible for the registering of the local multicast source and the joining of the receivers.

The DR is elected based on the priority and the IPv6 address. The switches send Hello messages carrying the priority for DR election. The switch with the highest priority becomes the DR. If the switches have the same priority, the switch with the largest IPv6 address becomes the DR.

If at least one switch in the network does not support Hello packets that contain the priority, the switch with the largest IPv6 address functions as the DR.

Prerequisites

IPv6 multicast routing has been enabled globally using the **multicast ipv6 routing-enable** command in the system view.

Precautions

The **hello-option dr-priority** command has the same function as the **pim ipv6 hello-option dr-priority** command in the interface view. By default, if the **pim ipv6 hello-option dr-priority** command is not used, the value configured in the PIM-IPv6 view is used; otherwise, the value configured in the interface view is used.

Example

In the PIM-IPv6 view, configure the DR priority of a switch to 3.

```
<HUAWEI> system-view
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] pim-ipv6
[HUAWEI-pim6] hello-option dr-priority 3
```

8.4.34 hello-option holdtime (IPv6)

Function

The **hello-option holdtime** command sets the timeout period for a switch to wait to receive Hello messages from its PIM neighbor.

The **undo hello-option holdtime** command restores the default configuration.

By default, the timeout period for a switch to wait to receive Hello messages from its PIM neighbor is 105 seconds.

Format

hello-option holdtime *interval*

undo hello-option holdtime

Parameters

Parameter	Description	Value
interval	Specifies the timeout time during which a switch waits to receive a Hello message from its PIM neighbor.	The value is an integer that ranges from 1 to 65535, in seconds.

Views

PIM-IPv6 view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On the PIM (IPv6) network, after a switch receives a Hello message from its PIM neighbor, the switch starts a timer based on the Holdtime value in the Hello message. If the switch does not receive any Hello message from its PIM neighbor when the timer expires, it considers the neighbor invalid or unreachable.

The **hello-option holdtime (IPv6)** command sets the timeout period during which a PIM interface waits to receive the Hello message from its neighbor.

Prerequisites

IPv6 multicast routing has been enabled globally using the **multicast ipv6 routing-enable** command in the system view.

Precautions

The timeout period must be greater than the interval for sending Hello messages. You can run the **timer hello (IPv6)** command to set the interval for sending Hello messages.

The **hello-option holdtime** command has the same function as the **pim ipv6 hello-option holdtime** command in the interface view. By default, if the **pim ipv6 hello-option holdtime** command is not used, the value configured in the PIM-IPv6 view is used; otherwise, the value configured in the interface view is used.

Example

In the PIM-IPv6 view, set the timeout interval to 120 seconds. The timeout interval is the period during which a switch waits to receive the Hello message from its PIM neighbor.

```
<HUAWEI> system-view
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] pim-ipv6
[HUAWEI-pim6] hello-option holdtime 120
```


8.4.35 hello-option lan-delay (IPv6)

Function

The **hello-option lan-delay** command sets the delay in transmitting Prune message on the shared network segment.

The **undo hello-option lan-delay** command restores the default delay.

By default, the delay in transmitting Prune message on the shared network segment is 500 milliseconds.

Format

hello-option lan-delay *interval*

undo hello-option lan-delay

Parameters

Parameter	Description	Value
interval	Specifies the delay in transmitting Prune message on the shared network segment.	The value is an integer that ranges from 1 to 32767, in milliseconds (ms).

Views

PIM-IPv6 view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Hello messages sent switches carry **lan-delay** and **override-interval** values. The **lan-delay** parameter indicates the delay in transmitting messages in the LAN. If devices on the same link have different **lan-delay** values, the maximum value is used.

When a switch sends a Prune message to the upstream device in the same network segment, the other devices that still request multicast data need to send a Join message to the upstream device within the override-interval period.

The value of the Prune-Pending Timer (PPT) is the sum of **lan-delay** and **override-interval** values and refer to the delay from the current device receiving a Prune message from the downstream interface to performing the prune action. If the switch receives a Join message from the downstream interface before the PPT timer expires, it cancels the prune action.

Prerequisites

IPv6 multicast routing has been enabled using the **multicast ipv6 routing-enable** command in the system view.

Precautions

If the delay in transmitting Prune message is too short, the upstream device will stop forwarding multicast packets before the downstream device determines whether to override the Prune action or not. Exercise caution when you run the **hello-option lan-delay** command.

The **hello-option lan-delay** command has the same function as the **pim ipv6 hello-option lan-delay** command in the interface view. By default, if the **pim ipv6 hello-option lan-delay** command is not used, the value configured in the PIM-IPv6 view is used; otherwise, the value configured in the interface view is used.

Example

Set the delay in transmitting Prune message on the shared network segment to 200 ms in the PIM-IPv6 view.

```
<HUAWEI> system-view
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] pim-ipv6
[HUAWEI-pim6] hello-option lan-delay 200
```

8.4.36 hello-option neighbor-tracking (IPv6)

Function

The **hello-option neighbor-tracking** command enables the neighbor tracking function.

The **undo hello-option neighbor-tracking** command restores the default configuration.

By default, the neighbor tracking function is not enabled.

Format

hello-option neighbor-tracking

undo hello-option neighbor-tracking

Parameters

None

Views

PIM-IPv6 view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When sending a Hello message, the switch generates a Generation ID and encapsulates it into the message. The Generation ID changes only when the device status changes. In this case, the neighboring device detects the Generation ID change after receiving the Hello message and immediately sends a Join message to the device to update the neighbor relationship. If multiple devices on a shared network segment prepare to send Join messages to the same upstream PIM neighbor, only one device is allowed to send the Join message. After other devices detect the Join message, they do not send Join messages to the upstream neighbor. This means that the upstream neighbor cannot update neighbor relationships with downstream devices after a Generation ID change.

When the switch with neighbor tracking enabled detects Join messages from other devices, the switch still sends the Join messages to the same upstream PIM neighbor.

Prerequisites

IPv6 multicast routing has been enabled using the **multicast ipv6 routing-enable** command in the system view.

Precautions

This command is valid for only PIM-SM (IPv6).

Neighbor tracking can be implemented only when this function is enabled on all devices on the shared network segment.

The **hello-option neighbor-tracking** command has the same function as the **pim ipv6 hello-option neighbor-tracking** command in the interface view. By default, if neighbor tracking is not used on an interface, the neighbor tracking configuration in the PIM-IPv6 view takes effect.

Example

In the PIM-IPv6 view, enable the downstream neighbor tracking function.

```
<HUAWEI> system-view
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] pim-ipv6
[HUAWEI-pim6] hello-option neighbor-tracking
```

8.4.37 hello-option override-interval (IPv6)

Function

The **hello-option override-interval** command sets the interval for overriding the prune action in a Hello message.

The **undo hello-option override-interval** command restores the default interval.

By default, the interval for overriding the prune action in a Hello message is 2500 ms.

Format

hello-option override-interval *interval*

undo hello-option override-interval

Parameters

Parameter	Description	Value
interval	Specifies the interval for overriding the prune action in a Hello message.	The value is an integer that ranges from 1 to 65535, in milliseconds.

Views

PIM-IPv6 view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Hello messages sent from switches carry **lan-delay** and **override-interval** values. The **override-interval** parameter refers to the period during which a downstream switch can override the prune action.

When a switch sends a Prune message to the upstream device in the same network segment, the other devices that still request multicast data need to send a Join message to the upstream device within the override-interval period.

If switches on the same link have different values, the maximum value is used.

The value of PPT is the sum of **lan-delay** and **override-interval** values. When receiving a Prune message from a downstream interface, the switch does not perform the prune action until the PPT expires. If the switch receives a Join message from the downstream interface before the PPT expires, it cancels the Prune action.

Prerequisites

IPv6 multicast routing has been enabled globally using the **multicast ipv6 routing-enable** command in the system view.

Precautions

This command is valid for PIM-SM (IPv6) and PIM-DM (IPv6).

The **hello-option override-interval** command has the same function as the **pim ipv6 hello-option override-interval** command in the interface view. By default, if the **pim ipv6 hello-option override-interval** command is not used, the value configured in the PIM-IPv6 view is used; otherwise, the value configured in the interface view is used.

Example

In the PIM-IPv6 view, set the interval for denying the prune action in a Hello message to 2000 ms.

```
<HUAWEI> system-view
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] pim-ipv6
[HUAWEI-pim6] hello-option override-interval 2000
```

8.4.38 holdtime assert (IPv6)

Function

The **holdtime assert** command sets the timeout period for all PIM interfaces to keep the Assert state on the local switch.

The **undo holdtime assert** command restores the default timeout.

By default, the timeout period for all PIM interfaces to keep the Assert state on the local switch is 180 seconds.

Format

holdtime assert *interval*

undo holdtime assert

Parameters

Parameter	Description	Value
interval	Specifies the time during which the PIM interface keeps the Assert state.	The value is an integer that ranges from 7 to 65535, in seconds.

Views

PIM-IPv6 view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On the shared network segment connected to multiple PIM devices, if the same multicast packets reach these PIM devices and pass the RPF check, multiple copies of the same multicast packets are forwarded to this network segment. In this situation, these PIM devices need to initiate the assert mechanism. The device that wins assert election is responsible for multicast forwarding on the shared network segment. Other devices suppress multicast data forwarding and retain the Assert state for a period of time. After the timer for a PIM interface in the Assert state expires, the device that fails to be elected triggers a new round of election.

Prerequisites

IPv6 multicast routing has been enabled using the **multicast ipv6 routing-enable** command in the system view.

Precautions

This command is valid for PIM-SM (IPv6) and PIM-DM (IPv6).

The **holdtime assert** command has the same function as the **pim ipv6 holdtime assert** command in the interface view. By default, if the timeout period is not used on an interface, the timeout period configured in the PIM-IPv6 view is used.

Example

In the PIM-IPv6 view, set the interval during which a switch keeps the Assert state to 100s.

```
<HUAWEI> system-view
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] pim-ipv6
[HUAWEI-pim6] holdtime assert 100
```

8.4.39 holdtime join-prune (IPv6)

Function

The **holdtime join-prune** command sets the holdtime value in Join/Prune messages sent by all PIM interfaces. Devices that receive Join/Prune messages set the time during which the downstream interface keeps the Join or Prune state according to holdtime.

The **undo holdtime join-prune** command restores the default value.

By default, the holdtime value in Join/Prune messages sent by all PIM interfaces is 210 seconds.

Format

holdtime join-prune *interval*

undo holdtime join-prune

Parameters

Parameter	Description	Value
interval	Specifies the value of holdtime carried in Join/Prune messages sent by the local device.	The value is an integer that ranges from 1 to 65535, in seconds.

Views

PIM-IPv6 view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After receiving a Join/Prune message from the downstream device, the switch starts the hold timer. If this message carries group-join information and the switch does not receive subsequent Join/Prune messages from the downstream device when the timer expires, it suppresses multicast data forwarding to downstream interfaces of the specified group. If Join/Prune message carries group-prune information, the switch resumes multicast data forwarding to downstream interfaces when the hold timer expires.

Prerequisites

IPv6 multicast routing has been enabled using the **multicast ipv6 routing-enable** command in the system view.

Precautions

This command is valid for PIM-SM (IPv6) and PIM-DM (IPv6).

The **holdtime join-prune** command has the same function as the **pim ipv6 holdtime join-prune** command in the interface view. By default, if the holdtime value is not used on an interface, the holdtime value configured in the PIM-IPv6 view is used.

Example

In the PIM-IPv6 view, set the time during which the downstream interface of a switch keeps the Join or Prune state to 280 seconds.

```
<HUAWEI> system-view
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] pim-ipv6
[HUAWEI-pim6] holdtime join-prune 280
```

8.4.40 join-prune max-packet-length (IPv6)

Function

The **join-prune max-packet-length** command sets the maximum size of each Join/Prune message to be sent.

The **undo join-prune max-packet-length** command restores the default maximum size of each Join/Prune message to be sent.

By default, the maximum length of Join/Prune message sent by is 8100 bytes.

Format

join-prune max-packet-length *packet-length*

undo join-prune max-packet-length

Parameters

Parameter	Description	Value
packet-length	Specifies the maximum size of each PIM-SM Join/Prune message to be sent.	The value is an integer that ranges from 100 to 64000, in bytes.

Views

PIM-IPv6 view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If the peer device has low performance and takes a long time to process a large Join/Prune message carrying a lot of (S, G) entries, the maximum size of each Join/Prune message can be reduced to relieve the burden on the peer device.

Prerequisites

IPv6 multicast routing has been enabled globally using the **multicast ipv6 routing-enable** command in the system view.

Precautions

This command is valid for PIM-SM (IPv6) and PIM-DM (IPv6).

If the maximum size specified in the **join-prune max-packet-length** command is greater than the interface MTU, the maximum size of each message to be sent is equal to the interface MTU.

Example

Set the maximum size of each Join/Prune message to be sent to 2100 bytes.

```
<HUAWEI> system-view
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] pim-ipv6
[HUAWEI-pim6] join-prune max-packet-length 2100
```

8.4.41 join-prune periodic-messages queue-size (IPv6)

Function

The **join-prune periodic-messages queue-size** command sets the maximum number of (S, G) entries carried in a Join/Prune message that is sent every second.

The **undo join-prune periodic-messages queue-size** command restores the default maximum number of (S, G) entries carried in a Join/Prune message that is sent every second.

By default, a Join/Prune message that is sent every second contains 1020 entries.

Format

join-prune periodic-messages queue-size *queue-size*

undo join-prune periodic-messages queue-size

Parameters

Parameter	Description	Value
queue-size	Specifies the maximum number of (S, G) entries carried in a Join/Prune message that is sent every second.	The value is an integer that ranges from 16 to 4096.

Views

PIM-IPv6 view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If the peer device has a low throughput, reduce the length of a queue for periodically sending messages to control the number of (S, G) entries. This setting allows the local device to send Join/Prune messages with a small number of (S, G) entries multiple times, preventing packet loss or route flapping.

Prerequisites

IPv6 multicast routing has been enabled globally using the **multicast ipv6 routing-enable** command in the system view.

Precautions

This command is valid for PIM-SM (IPv6) and PIM-DM (IPv6).

Example

Allow each Join/Prune message that is sent every second to carry a maximum of 2000 (S, G) entries.

```
<HUAWEI> system-view
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] pim-ipv6
[HUAWEI-pim6] join-prune periodic-messages queue-size 2000
```


8.4.42 join-prune triggered-message-cache disable (IPv6)

Function

The **join-prune triggered-message-cache disable** command disables the Join/Prune message package function.

The **undo join-prune triggered-message-cache disable** command enables the Join/Prune message package function.

By default, the Join/Prune message package function is enabled.

Format

join-prune triggered-message-cache disable

undo join-prune triggered-message-cache disable

Parameters

None

Views

PIM-IPv6 view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The system performs more efficiently when sending a package of Join/Prune messages than sending a large number of individual Join/Prune messages. A device sends Join/Prune messages in packages. To disable the package function, run the **join-prune triggered-message-cache disable** command.

Prerequisites

IPv6 multicast routing has been enabled globally using the **multicast ipv6 routing-enable** command in the system view.

Precautions

This command is valid for PIM-SM (IPv6) and PIM-DM (IPv6).

Example

Disable the Join/Prune message package function.

```
<HUAWEI> system-view
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] pim-ipv6
[HUAWEI-pim6] join-prune triggered-message-cache disable
```


8.4.43 neighbor-check (IPv6)

Function

The **neighbor-check** command enables the PIM neighbor check function.

The **undo neighbor-check** command restores the default setting.

By default, the PIM neighbor check function is not enabled.

Format

neighbor-check { **receive** | **send** }

undo neighbor-check { **receive** | **send** }

Parameters

Parameter	Description	Value
receive	Checks whether the Join/Prune and Assert messages are received from a PIM neighbor. If not, these messages are discarded.	-
send	Checks whether the Join/Prune and Assert messages are sent to a PIM neighbor. If not, these messages are not sent.	-

Views

PIM-IPv6 view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

PIM devices send Join/Prune messages to the upstream PIM neighbor to perform join and prune actions and PIM neighbors often exchange Assert messages. To save system resources and protect security of Join/Prune messages and Assert messages, run the **neighbor-check** command to enable the PIM neighbor check function.

Prerequisites

IPv6 multicast routing has been enabled using the **multicast ipv6 routing-enable** command in the system view.

Precautions

You can specify both **receive** and **send** to enable the PIM neighbor check function for the received and sent Join/Prune and Assert messages.

This command is valid for only PIM-SM (IPv6).

Example

In the PIM-IPv6 view, enable the PIM neighbor check function for the received Join/Prune and Assert messages.

```
<HUAWEI> system-view
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] pim-ipv6
[HUAWEI-pim6] neighbor-check receive
```

8.4.44 pim-ipv6

Function

The **pim-ipv6** command displays the PIM-IPv6 view.

The **undo pim-ipv6** command clears the configuration in the PIM-IPv6 view.

Format

pim-ipv6

undo pim-ipv6

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Before performing PIM (IPv6) configurations, run the **pim-ipv6** command to enter the PIM-IPv6 view.

Prerequisites

IPv6 multicast routing has been enabled using the **multicast ipv6 routing-enable** command in the system view.

Precautions

NOTICE

In using the **undo pim-ipv6** command, enter Y or N to confirm the action. This command clears global PIM (IPv6) configurations in the current instance. Use this command with caution.

Example

Enter the PIM-IPv6 view.

```
<HUAWEI> system-view
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] pim-ipv6
[HUAWEI-pim6]
```

8.4.45 pim ipv6 bfd

Function

The **pim ipv6 bfd** command configures PIM BFD (IPv6) parameters on an interface.

The **undo pim ipv6 bfd** command restores default PIM BFD (IPv6) parameters on an interface.

By default, the interval for transmitting BFD packets and interval for receiving BFD packets are 1000 ms, and the BFD detection multiplier is 3.

NOTE

Only the S5720I-SI, S5735-S, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6720S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Format

pim ipv6 bfd { **min-tx-interval** *tx-value* | **min-rx-interval** *rx-value* | **detect-multiplier** *multiplier-value* }*

undo pim ipv6 bfd { **min-tx-interval** | **min-rx-interval** | **detect-multiplier** }*

undo pim ipv6 bfd { **min-tx-interval** *tx-value* | **min-rx-interval** *rx-value* | **detect-multiplier** *multiplier-value* }*

Parameters

Parameter	Description	Value
min-tx-interval *tx-value*	Specifies the interval for sending BFD packets.	The value is an integer that ranges from 100 to 1000, in milliseconds. ● After the **set service-mode enhanced** command is configured on the S5731-H, S5731-S, S5731S-H, and S5731S-S, the value ranges from 3 to 1000. ● After the **set service-mode enhanced-bfd** command is configured on the S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S, the value ranges from 3 to 1000.
min-rx-interval *rx-value*	Specifies the interval for receiving BFD packets.	The value is an integer that ranges from 100 to 1000, in milliseconds. ● After the **set service-mode enhanced** command is configured on the S5731-H, S5731-S, S5731S-H, and S5731S-S, the value ranges from 3 to 1000. ● After the **set service-mode enhanced-bfd** command is configured on the S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S, the value ranges from 3 to 1000.

Parameter	Description	Value
detect-multiplier *multiplier-value*	Specifies the local detection multiplier of BFD packets. • For a stable link, you can set the detection multiplier to a large value to avoid frequent link detection. • For an unstable link, a small detection multiplier may cause BFD session flapping. Therefore, it is recommended that you set the detection multiplier to a large value.	The value is an integer ranging from 3 to 50. The default value is 3.

Views

GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, VLANIF interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If you need to control detection parameters of BFD packets, run the **pim ipv6 bfd** command to configure the sending interval, receiving interval, and local detection multiplier for PIM BFD (IPv6) packets.

The **min-tx-interval**, **min-rx-interval**, and **detect-multiplier** parameters can be configured separately at two ends of a link so that the two ends can send or receive BFD packets at different rates. If there is no special requirement for the detection period and the link is stable, you are advised to configure the same parameter settings for the routing devices that have the same performance and are on the shared network segment.

Prerequisites

IPv6 multicast routing has been enabled globally using the **multicast ipv6 routing-enable** command in the system view.

Configuration Impact

After BFD parameters are configured, PIM (IPv6) provides the address to be detected, the minimum sending interval and receiving interval of PIM BFD (IPv6)

packets, and the local detection multiplier for BFD. The two ends enabled with BFD then negotiate the actual sending interval and receiving interval, and the detection period based on these configured parameters. During the detection phase, BFD notifies the route management (RM) module of the BFD session status and the RM module then notifies PIM (IPv6) of the session status.

If a link fault occurs, BFD quickly notifies the RM of the session status and the RM then notifies PIM (IPv6) of the session status. The PIM (IPv6) protocol deletes the status of the faulty interface, triggers a new DR or Assert election, and restores the forwarding of multicast data to the downstream interface. This shortens the period of multicast traffic interruption caused by the interface fault.

Precautions

To validate PIM BFD (IPv6), ensure that a BFD session has been set up and the session is in the Up state.

The two ends negotiate the actual sending interval and receiving interval, and detection period of BFD packets based on the following negotiation mechanism:

- The formula used to calculate the interval for sending PIM IPv6 BFD packets and the formula used to calculate the interval for receiving PIM IPv6 BFD packets are as follows:
  - Interval for sending PIM IPv6 BFD packets = Max (Local **min-tx-interval**, Remote **min-rx-interval**)
  - Interval for receiving PIM IPv6 BFD packets = Max (Remote **min-tx-interval**, Local **min-rx-interval**)
- The formula used to calculate the detection period is as follows:
  - Detection period = Remote **detect-multiplier** x Max (Remote **min-tx-interval**, Local **min-rx-interval**)

If a large parameter value is set, BFD will take a long time to detect a fault on a link. This may cause packet loss.

Example

Enable PIM BFD (IPv6) on VLANIF 100, and set both the minimum interval for sending BFD packets and the minimum interval for receiving BFD packets to 200 ms and the local detection multiplier to 5.

```
<HUAWEI> system-view
[HUAWEI] bfd
[HUAWEI-bfd] quit
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] ipv6 enable
[HUAWEI-Vlanif100] pim ipv6 sm
[HUAWEI-Vlanif100] pim ipv6 bfd enable
[HUAWEI-Vlanif100] pim ipv6 bfd min-tx-interval 200 min-rx-interval 200 detect-multiplier 5
```

Enable PIM BFD (IPv6) on GE0/0/1, and set both the minimum interval for sending BFD packets and the minimum interval for receiving BFD packets to 200 ms and the local detection multiplier to 5.

```
<HUAWEI> system-view
[HUAWEI] bfd
[HUAWEI-bfd] quit
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
```



```
[HUAWEI-GigabitEthernet0/0/1] ipv6 enable
[HUAWEI-GigabitEthernet0/0/1] pim ipv6 sm
[HUAWEI-GigabitEthernet0/0/1] pim ipv6 bfd enable
[HUAWEI-GigabitEthernet0/0/1] pim ipv6 bfd min-tx-interval 200 min-rx-interval 200 detect-multiplier
5
```

8.4.46 pim ipv6 bfd enable

Function

The **pim ipv6 bfd enable** command enables PIM BFD (IPv6) on an interface.

The **undo pim ipv6 bfd enable** command disables PIM BFD (IPv6) on an interface.

By default, PIM BFD (IPv6) is disabled on an interface.

NOTE

Only the S5720I-SI, S5735-S, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6720S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Format

pim ipv6 bfd enable

undo pim ipv6 bfd enable

Parameters

None

Views

GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, VLANIF interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To minimize the impact of a fault on services and improve network availability, a network device is required to quickly detect a communications fault between adjacent devices so that the upper layer protocol can rectify the fault to ensure normal services.

On a PIM network, changes of link status between PIM neighbors will restart some PIM mechanisms, such as DR election or Assert winner election. For example, when the DR or Assert winner on a shared network segment fails, PIM neighbors on the network segment trigger DR or Assert winner re-election only

when the PIM neighbor relationships time out. Multicast data transmission is interrupted before a new DR or Assert winner is elected. The multicast service interruption time is longer than or equal to the neighbor relationship timeout interval or Assert timer value, and is usually several seconds.

PIM BFD (IPv6) can detect link status changes on a shared network segment in milliseconds, enabling PIM devices to rapidly respond to failures of PIM neighbors. If a PIM BFD (IPv6)-capable interface does not receive any BFD packets from the DR or Assert winner within the detection interval, it considers that the DR or Assert winner has failed. Then BFD rapidly reports the session status to the route management (RM) module, which then reports the link status change to the PIM module. After receiving the notification, the PIM module triggers DR or Assert winner re-election immediately, without waiting for timeout of the neighbor relationship. This mechanism reduces the multicast service interruption time and improves reliability of multicast data transmission.

Pre-configuration Tasks

PIM BFD (IPv6) depends on the BFD protocol. Therefore, you need first to enable BFD globally to validate the PIM BFD (IPv6) function.

IPv6 multicast routing has been enabled globally using the **multicast ipv6 routing-enable** command in the system view.

Before configuring PIM BFD (IPv6), enable PIM-SM (IPv6) in the interface view. If the **undo pim ipv6 sm** command is run, IPv6 PIM-SM is disabled and the PIM BFD (IPv6) function is removed from the interface at the same time.

Example

Enable PIM BFD (IPv6) on VLANIF 100.

```
<HUAWEI> system-view
[HUAWEI] bfd
[HUAWEI-bfd] quit
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] ipv6 enable
[HUAWEI-Vlanif100] pim ipv6 sm
[HUAWEI-Vlanif100] pim ipv6 bfd enable
```

Enable PIM BFD (IPv6) on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] bfd
[HUAWEI-bfd] quit
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] ipv6 enable
[HUAWEI-GigabitEthernet0/0/1] pim ipv6 sm
[HUAWEI-GigabitEthernet0/0/1] pim ipv6 bfd enable
```

8.4.47 pim ipv6 bsr-boundary

Function

The **pim ipv6 bsr-boundary** command configures the BSR boundary of a PIM-SM (IPv6) domain on an interface.

The **undo pim ipv6 bsr-boundary** command restores the default configuration.

By default, the BSR boundary of a PIM-SM (IPv6) domain is not set.

Format

pim ipv6 bsr-boundary

undo pim ipv6 bsr-boundary

Parameters

None

Views

GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, VLANIF interface view, loopback interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

As the management core of the PIM-SM (IPv6) network, the BSR is responsible for sending collected RP-set information to PIM neighbors through Bootstrap messages.

You can divide a large PIM-SM (IPv6) network into multiple PIM-SM (IPv6) domains by configuring the bsr boundary on an interface. Each BSR then serves the local PIM-SM (IPv6) domain.

Prerequisites

IPv6 multicast routing has been enabled globally using the **multicast ipv6 routing-enable** command in the system view.

Configuration Impact

The Bootstrap messages cannot traverse the BSR boundary but other multicast packets can.

Example

Configure the BSR boundary of a PIM-SM (IPv6) domain on VLANIF100.

```
<HUAWEI> system-view
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] ipv6 enable
[HUAWEI-Vlanif100] pim ipv6 bsr-boundary
```

Configure the BSR boundary of a PIM-SM (IPv6) domain on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
```



```
[HUAWEI-GigabitEthernet0/0/1] ipv6 enable
[HUAWEI-GigabitEthernet0/0/1] pim ipv6 bsr-boundary
```

8.4.48 pim ipv6 dm

Function

The **pim ipv6 dm** command enables PIM-DM (IPv6) on an interface.

The **undo pim ipv6 dm** command restores the default configuration.

By default, PIM-DM (IPv6) is disabled on an interface.

Format

pim ipv6 dm

undo pim ipv6 dm

Parameters

None

Views

GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, VLANIF interface view, loopback interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

PIM-DM (IPv6) is a multicast routing protocol in dense mode and applies to small-scale networks with densely-distributed group members.

After PIM-DM (IPv6) is enabled on an interface, the switch can set up the PIM neighbor relationship with the neighboring device. The switch then can process protocol packets received from PIM neighbors.

Prerequisites

IPv6 multicast routing has been enabled using the **multicast ipv6 routing-enable** command in the system view.

Precautions

PIM-DM (IPv6) and PIM-SM (IPv6) cannot be enabled simultaneously on the device.

If PIM-DM (IPv6) and MLD need to be enabled on the same interface, enable PIM-DM (IPv6), and then enable MLD.

Running the **pim ipv6 dm** command failed on the VLANIF interface because Layer 2 multicast querier or report-suppress is enabled for this VLAN.

If both Layer 2 and Layer 3 multicast services are required in a VLAN, enable PIM (IPv6) on the corresponding VLANIF interface first, and then enable MLD snooping in the VLAN. If MLD snooping is enabled in the VLAN first, PIM (IPv6) cannot be enabled on the VLANIF interface.

Example

Enable PIM-DM (IPv6) on VLANIF100.

```
<HUAWEI> system-view
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] ipv6 enable
[HUAWEI-Vlanif100] pim ipv6 dm
```

Enable PIM-DM (IPv6) on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] ipv6 enable
[HUAWEI-GigabitEthernet0/0/1] pim ipv6 dm
```

8.4.49 pim ipv6 hello-option dr-priority

Function

The **pim ipv6 hello-option dr-priority** command sets the priority for the PIM interface that is elected as DR.

The **undo pim ipv6 hello-option dr-priority** command restores the default value of the priority.

By default, the priority for the PIM interface that is elected as DR is 1.

Format

pim ipv6 hello-option dr-priority *priority*

undo pim ipv6 hello-option dr-priority

Parameters

Parameter	Description	Value
priority	Specifies the priority of the PIM interface that is elected as DR.	The value is an integer that ranges from 0 to 4294967295. The greater the value, the higher the priority.

Views

GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, VLANIF interface view, loopback interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On a PIM (IPv6) network, devices on a shared network segment are candidates for the DR. The DR is responsible for the registering of the local multicast source and the joining of the receivers.

The DR is elected based on the priority and the IPv6 address. Switches send Hello messages carrying their priorities to each other, and the one with the highest priority becomes the DR. If the switches have the same priority, the switch with the largest IPv6 address becomes the DR.

If at least one device in the network does not support Hello packets that contain the priority, the device with the largest IPv6 address functions as the DR.

Prerequisites

IPv6 multicast routing has been enabled using the **multicast ipv6 routing-enable** command in the system view.

Precautions

The **pim ipv6 hello-option dr-priority** command has the same function as the **hello-option dr-priority (IPv6)** command in the PIM-IPv6 view. By default, if the **pim ipv6 hello-option dr-priority** command is not used, the value configured in the PIM-IPv6 view is used; otherwise, the value configured in the interface view is used.

Example

Set the priority of VLANIF100 that is elected as DR to 3.

```
<HUAWEI> system-view
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] ipv6 enable
[HUAWEI-Vlanif100] pim ipv6 hello-option dr-priority 3
```

Set the priority of GE0/0/1 that is elected as DR to 3.

```
<HUAWEI> system-view
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] ipv6 enable
[HUAWEI-GigabitEthernet0/0/1] pim ipv6 hello-option dr-priority 3
```

8.4.50 pim ipv6 hello-option holdtime

Function

The **pim ipv6 hello-option holdtime** command sets the timeout period during which the PIM interface waits to receive the Hello message from its neighbor.

The **undo pim ipv6 hello-option holdtime** command restores the default value of the timeout.

By default, the timeout period during which the PIM interface waits to receive the Hello message from its neighbor is 105 seconds.

Format

pim ipv6 hello-option holdtime *interval*

undo pim ipv6 hello-option holdtime

Parameters

Parameter	Description	Value
interval	Specifies the timeout period during which the PIM interface waits to receive Hello messages from its neighbor.	The value is an integer that ranges from 1 to 65535, in seconds.

Views

GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, VLANIF interface view, loopback interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On a PIM (IPv6) network, after a switch receives a Hello message from its PIM neighbor, it starts a timer based on Holdtime value in the Hello message. If the switch does not receive any Hello message from its PIM neighbor when the timer expires, the switch considers the neighbor invalid or unreachable.

The **pim ipv6 hello-option holdtime** command sets the timeout period during which the PIM interface waits to receive the Hello message from its neighbor.

Prerequisites

IPv6 multicast routing has been enabled globally using the **multicast ipv6 routing-enable** command in the system view.

Precautions

The timeout period must be greater than the interval for sending Hello messages, which is set using the **pim ipv6 time hello** command.

The **pim ipv6 hello-option holdtime** command has the same function as the **hello option holdtime (IPv6)** command in the PIM-IPv6 view. By default, if the **pim ipv6 hello-option holdtime** command is not used, the value configured in the PIM-IPv6 view is used; otherwise, the value configured in the interface view is used.

Example

Set the timeout period during which VLANIF100 waits to receive Hello messages from its neighbor to 120 seconds.

```
<HUAWEI> system-view
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] ipv6 enable
[HUAWEI-Vlanif100] pim ipv6 hello-option holdtime 120
```

Set the timeout period during which GE0/0/1 waits to receive Hello messages from its neighbor to 120 seconds.

```
<HUAWEI> system-view
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] ipv6 enable
[HUAWEI-GigabitEthernet0/0/1] pim ipv6 hello-option holdtime 120
```

8.4.51 pim ipv6 hello-option lan-delay

Function

The **pim ipv6 hello-option lan-delay** command sets the delay in transmitting messages in a shared network in the interface view.

The **undo pim ipv6 hello-option lan-delay** command restores the default value of the delay.

By default, the delay in transmitting messages in the shared network is 500 ms.

Format

pim ipv6 hello-option lan-delay *interval*

undo pim ipv6 hello-option lan-delay

Parameters

Parameter	Description	Value
interval	Specifies the delay in transmitting messages in the shared network.	The value is an integer that ranges from 1 to 32767, in milliseconds.

Views

GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, VLANIF interface view, loopback interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Hello messages sent switches carry **lan-delay** and **override-interval** values. The **lan-delay** parameter indicates the delay in transmitting messages in the LAN. If devices on the same link have different **lan-delay** values, the maximum value is used.

When a switch sends a Prune message to the upstream device in the same network segment, the other devices that still request multicast data need to send a Join message to the upstream device within the override-interval period.

The value of the Prune-Pending Timer (PPT) is the sum of **lan-delay** and **override-interval** values and refer to the delay from the current device receiving a Prune message from the downstream interface to performing the prune action. If the switch receives a Join message from the downstream interface before the PPT timer expires, it cancels the prune action.

Prerequisites

IPv6 multicast routing has been enabled using the **multicast ipv6 routing-enable** command in the system view.

Precautions

This command is valid for PIM-SM (IPv6) and PIM-DM (IPv6).

If the prune delay is set too short, the upstream device stops forwarding multicast packets before the downstream device overrides Prune messages of neighbors. Exercise caution when you run this command.

The function of this command in the interface view is the same as that of the **hello-option lan-delay (IPv6)** command in the PIM-IPv6 view. By default, if the configuration on the interface is not performed, the value configured in the PIM-IPv6 view is used; otherwise, the value configured in the interface view is used.

Example

Set the delay in transmitting messages to 200 ms on VLANIF100.

```
<HUAWEI> system-view
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] ipv6 enable
[HUAWEI-Vlanif100] pim ipv6 hello-option lan-delay 200
```

Set the delay in transmitting messages to 200 ms on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] ipv6 enable
[HUAWEI-GigabitEthernet0/0/1] pim ipv6 hello-option lan-delay 200
```

8.4.52 pim ipv6 hello-option neighbor-tracking

Function

The **pim ipv6 hello-option neighbor-tracking** command enables the neighbor tracking function in the interface view.

The **undo pim ipv6 hello-option neighbor-tracking** command restores the default configuration.

By default, the neighbor tracking function is not enabled.

Format

pim ipv6 hello-option neighbor-tracking

undo pim ipv6 hello-option neighbor-tracking

Parameters

None

Views

GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, VLANIF interface view, loopback interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When sending a Hello message, a switch generates a Generation ID and encapsulates it into the message. The Generation ID changes only when the device status changes. In this case, the neighboring device detects the Generation ID change after receiving the Hello message and immediately sends a Join message to the device to update the neighbor relationship. If multiple devices on the shared network segment prepare to send Join messages to the same upstream PIM neighbor, only one device is allowed to send the Join message. After other devices detect the Join message, they do not send Join messages to the upstream neighbor. This means that the upstream neighbor cannot update neighbor relationships with downstream devices after a Generation ID change.

After the neighbor tracking function is enabled, when the device detects Join messages from other devices, the device still sends the Join messages to the same upstream PIM neighbor.

Prerequisites

IPv6 multicast routing has been enabled globally using the **multicast ipv6 routing-enable** command in the system view.

Precautions

This command is valid for only PIM-SM (IPv6).

The neighbor tracking function can be implemented on a shared network segment only when this function is enabled on all devices on the network segment.

The **pim ipv6 hello-option neighbor-tracking** command has the same function as the **hello-option neighbor-tracking (IPv6)** command in the PIM-IPv6 view. By default, if the **pim ipv6 hello-option neighbor-tracking** command is not used, the configuration in the PIM-IPv6 view takes effect; otherwise, the configuration in the interface view takes effect.

Example

Enable the neighbor tracking function on VLANIF100.

```
<HUAWEI> system-view
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] ipv6 enable
[HUAWEI-Vlanif100] pim ipv6 hello-option neighbor-tracking
```

Enable the neighbor tracking function on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] ipv6 enable
[HUAWEI-GigabitEthernet0/0/1] pim ipv6 hello-option neighbor-tracking
```

8.4.53 pim ipv6 hello-option override-interval

Function

The **pim ipv6 hello-option override-interval** command sets the interval carried in Hello messages for overriding the prune action on the interface.

The **undo pim ipv6 hello-option override-interval** command, restores the default configuration.

By default, the interval carried in Hello messages for overriding the prune action on the interface is 2500 milliseconds.

Format

pim ipv6 hello-option override-interval *interval*

undo pim ipv6 hello-option override-interval

Parameters

Parameter	Description	Value
interval	Specifies the interval of overriding the prune action.	The value is an integer that ranges from 1 to 65535, in milliseconds.

Views

GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, VLANIF interface view, loopback interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Hello messages sent from switches carry **lan-delay** and **override-interval** values. The **override-interval** parameter refers to the period during which a downstream switch can override the prune action.

When a switch sends a Prune message to the upstream device in the same network segment, the other devices that still request multicast data need to send a Join message to the upstream device within the override-interval period.

If switches on the same link have different values, the maximum value is used.

The value of PPT is the sum of **lan-delay** and **override-interval** values. When receiving a Prune message from a downstream interface, the switch does not perform the prune action until the PPT expires. If the switch receives a Join message from the downstream interface before the PPT expires, it cancels the Prune action.

Prerequisites

IPv6 multicast routing has been enabled globally using the **multicast ipv6 routing-enable** command in the system view.

Precautions

The **pim ipv6 hello-option override-interval** command has the same function as the **hello-option override-interval (IPv6)** command in the PIM-IPv6 view. By default, if the **pim ipv6 hello-option override-interval** command is not used, the value configured in the PIM-IPv6 view is used; otherwise, the value configured in the interface view is used.

Example

Set the interval for overriding the prune action in Hello messages to 2000 ms on VLANIF100.

```
<HUAWEI> system-view
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] ipv6 enable
[HUAWEI-Vlanif100] pim ipv6 hello-option override-interval 2000
```

Set the interval for overriding the prune action in Hello messages to 2000 ms on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] ipv6 enable
[HUAWEI-GigabitEthernet0/0/1] pim ipv6 hello-option override-interval 2000
```


8.4.54 pim ipv6 holdtime assert

Function

The **pim ipv6 holdtime assert** command sets the timeout period during which a PIM interface keeps the Assert state.

The **undo pim ipv6 holdtime assert** command restores the default value of the timeout.

By default, the timeout period during which a PIM interface keeps the Assert state is 180 seconds.

Format

pim ipv6 holdtime assert *interval*

undo pim ipv6 holdtime assert

Parameters

Parameter	Description	Value
interval	Specifies the timeout period during which a PIM interface keeps the Assert state.	The value is an integer that ranges from 7 to 65535, in seconds.

Views

GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, VLANIF interface view, loopback interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On the shared network segment connected to multiple PIM devices, if the same multicast packets reach these PIM devices and pass the RPF check, multiple copies of the same multicast packets are forwarded to this network segment. In this situation, these PIM routers need to initiate the assert mechanism. The router that wins assert election is responsible for multicast forwarding on the shared network segment. Other devices suppress multicast data forwarding and retain the Assert state for a period of time. After the timer for a PIM interface in the Assert state expires, the device that fails to be elected triggers a new round of election.

Prerequisites

IPv6 multicast routing has been enabled using the **multicast ipv6 routing-enable** command in the system view.

Precautions

This command is valid for PIM-SM (IPv6) and PIM-DM (IPv6).

The **pim ipv6 holdtime assert** command has the same function as the **holdtime assert (IPv6)** command in the PIM-IPv6 view. By default, if the **pim ipv6 holdtime assert** command is not used, the value configured in the PIM-IPv6 view is used; otherwise, the value configured in the interface view is used.

Example

Set the timeout period for VLANIF100 to keep the Assert state to 100s.

```
<HUAWEI> system-view
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] ipv6 enable
[HUAWEI-Vlanif100] pim ipv6 holdtime assert 100
```

Set the timeout period for GE0/0/1 to keep the Assert state to 100s.

```
<HUAWEI> system-view
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] ipv6 enable
[HUAWEI-GigabitEthernet0/0/1] pim ipv6 holdtime assert 100
```

8.4.55 pim ipv6 holdtime join-prune

Function

The **pim ipv6 holdtime join-prune** command sets the holdtime in a Join/Prune message sent by the PIM interface.

The **undo pim ipv6 holdtime join-prune** command restores the default value of the holdtime.

By default, the holdtime in a Join/Prune message sent by the PIM interface is 210 seconds.

Format

pim ipv6 holdtime join-prune *interval*

undo pim ipv6 holdtime join-prune

Parameters

Parameter	Description	Value
interval	Specifies the value of holdtime in a Join/Prune message sent by the PIM interface.	The value is an integer that ranges from 1 to 65535, in seconds.

Views

GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, VLANIF interface view, loopback interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After receiving a Join/Prune message from the downstream device, the switch starts the hold timer. If this message carries group-join information and the switch does not receive subsequent Join/Prune messages from the downstream device when the timer expires, it suppresses multicast data forwarding to downstream interfaces of the specified group. If Join/Prune message carries group-prune information, the switch resumes multicast data forwarding to downstream interfaces when the hold timer expires.

Prerequisites

IPv6 multicast routing has been enabled using the **multicast ipv6 routing-enable** command in the system view.

Precautions

The **pim ipv6 holdtime join-prune** command has the same function as the **holdtime join-prune (IPv6)** command in the PIM-IPv6 view. By default, if the **pim ipv6 holdtime join-prune** command is not used, the value configured in the PIM view is used; otherwise, the value configured in the interface view is used.

Example

Set the holdtime in a Join/Prune message sent by VLANIF100 to 280 seconds.

```
<HUAWEI> system-view
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] ipv6 enable
[HUAWEI-Vlanif100] pim ipv6 holdtime join-prune 280
```

Set the holdtime in a Join/Prune message sent by GE0/0/1 to 280 seconds.

```
<HUAWEI> system-view
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] ipv6 enable
[HUAWEI-GigabitEthernet0/0/1] pim ipv6 holdtime join-prune 280
```

8.4.56 pim ipv6 join-policy

Function

The **pim ipv6 join-policy** command enables the system to filter join information in Join/Prune messages.

The **undo pim ipv6 join-policy** command restores the default setting.

By default, join information in Join/Prune message is not filtered.

Format

pim ipv6 join-policy { **asm** *basic-acl6-number* | **ssm** *advanced-acl6-number* | *advanced-acl6-number* }

undo pim ipv6 join-policy [**asm** | **ssm**]

Parameters

Parameter	Description	Value
asm	Filters join information, with the group address in the ASM group address range.	-
basic-acl6-number	Specifies the basic ACL number.	The value is an integer that ranges from 2000 to 2999.
ssm	Filters join messages, with the group addresses within the SSM group address range and specified source address.	-
advanced-acl6-number	Specifies the advanced ACL number.	The value is an integer that ranges from 3000 to 3999.

Views

GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, VLANIF interface view, loopback interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To prevent unauthorized users from joining multicast groups on the PIM-SM (IPv6) network by filtering join information in Join/Prune messages, run the **pim ipv6 join-policy** command.

Prerequisites

IPv6 multicast routing has been enabled globally using the **multicast ipv6 routing-enable** command in the system view.

Configuration Impact

This command is valid for only IPv6 PIM-SM.

The **pim ipv6 join-policy** command and the **acl ipv6 (system view)** command are used together.

- If **asm** is specified, you can set the multicast group address range of join information in the basic ACL6 view by specifying the **source** parameter in the **rule (basic ACL6 view)** command.
- If **ssm** is specified, you can set the source address range and multicast group address range of join information in the advanced ACL6 view by respectively specifying the **source** parameter and **destination** parameter in the **rule (advanced ACL6 view)** command.

You must run the **multicast ipv6 routing-enable** command to enable the multicast function before using the command.

Example

Configure VLANIF100 to accept the join information with the group address FF25::1.

```
<HUAWEI> system-view
[HUAWEI] acl ipv6 number 2001
[HUAWEI-acl6-basic-2001] rule permit source ff25::1 128
[HUAWEI-acl6-basic-2001] quit
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] ipv6 enable
[HUAWEI-Vlanif100] pim ipv6 join-policy asm 2001
```

Configure GE0/0/1 to accept the join information with the group address FF25::1.

```
<HUAWEI> system-view
[HUAWEI] acl ipv6 number 2001
[HUAWEI-acl6-basic-2001] rule permit source ff25::1 128
[HUAWEI-acl6-basic-2001] quit
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] ipv6 enable
[HUAWEI-GigabitEthernet0/0/1] pim ipv6 join-policy asm 2001
```

8.4.57 pim ipv6 neighbor-policy

Function

The **pim ipv6 neighbor-policy** command configures a policy for filtering PIM neighbors on an interface.

The **undo pim ipv6 neighbor-policy** command restores the default setting.

By default, PIM neighbors on the interface are not filtered.

Format

pim ipv6 neighbor-policy *basic-acl6-number*

undo pim ipv6 neighbor-policy

Parameters

Parameter	Description	Value
basic-acl6-number	Specifies the basic ACL number.	The value is an integer that ranges from 2000 to 2999.

Views

GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, VLANIF interface view, loopback interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To prevent unauthorized neighbors from being involved in the PIM protocol, run the **pim ipv6 neighbor-policy** command to configure a policy for filtering PIM neighbors and set the address range of PIM neighbors. The switch sets up neighbor relationships with the addresses matching the filtering rules and deletes the neighbors that do not match the filtering rules.

Prerequisites

IPv6 multicast routing has been enabled globally using the **multicast ipv6 routing-enable** command in the system view.

Configuration Impact

The **pim ipv6 neighbor-policy** command and the **acl ipv6** command are used together. In the ACL view, set the address range of PIM neighbors by specifying **source** in the **rule** command.

Precautions

This command is valid for both PIM-DM (IPv6) and PIM-SM (IPv6).

When configuring the neighbor filtering function on the interface, you must also configure the neighbor filtering function correspondingly on the PIM neighbor of the interface.

If the IPv6 address of a PIM neighbor that has established a neighbor relationship with the device is not in the configured range of valid neighbor IPv6 addresses, the device will no longer receive Hello messages from this PIM neighbor. When the holdtime of Hello messages expires, the neighbor relationship between the PIM device and the device is terminated.

Example

Configure VLANIF100 to set up the PIM neighbor relationship with the switch of the address FC00:0:0:2000::1.

```
<HUAWEI> system-view
[HUAWEI] acl ipv6 number 2001
[HUAWEI-acl6-basic-2001] rule permit source fc00:0:0:2000::1 128
[HUAWEI-acl6-basic-2001] quit
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] ipv6 enable
[HUAWEI-Vlanif100] pim ipv6 neighbor-policy 2001
```

Configure GE0/0/1 to set up the PIM neighbor relationship with the switch of the address FC00:0:0:2000::1.

```
<HUAWEI> system-view
[HUAWEI] acl ipv6 number 2001
[HUAWEI-acl6-basic-2001] rule permit source fc00:0:0:2000::1 128
[HUAWEI-acl6-basic-2001] quit
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] ipv6 enable
[HUAWEI-GigabitEthernet0/0/1] pim ipv6 neighbor-policy 2001
```

8.4.58 pim ipv6 require-genid

Function

The **pim ipv6 require-genid** command configures a PIM interface to reject the Hello messages without the Generation ID.

The **undo pim ipv6 require-genid** command restores the default configuration.

By default, a PIM interface is allowed to receive the Hello messages without the Generation ID.

Format

pim ipv6 require-genid

undo pim ipv6 require-genid

Parameters

None

Views

GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, VLANIF interface view, loopback interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After an interface is enabled with PIM, the switch generates a random number as the Generation ID of the Hello message. If the device status is updated, the switch generates a new Generation ID. When the switch finds that the Hello message received from a PIM neighbor contains a different Generation ID, it considers that the status of the PIM neighbor has changed.

To ensure that connected PIM neighbors work properly, run the **pim ipv6 require-genid** command to configure a PIM interface to reject the Hello messages without the Generation ID.

Prerequisites

IPv6 multicast routing has been enabled globally using the **multicast ipv6 routing-enable** command in the system view.

Precautions

This command is valid for both PIM-DM (IPv6) and PIM-SM (IPv6).

Example

Configure VLANIF100 to reject the Hello messages without the Generation ID.

```
<HUAWEI> system-view
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] ipv6 enable
[HUAWEI-Vlanif100] pim ipv6 require-genid
```

Configure GE0/0/1 to reject the Hello messages without the Generation ID.

```
<HUAWEI> system-view
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] ipv6 enable
[HUAWEI-GigabitEthernet0/0/1] pim ipv6 require-genid
```

8.4.59 pim ipv6 silent

Function

The **pim ipv6 silent** command enables the PIM silent (IPv6) function on an interface.

The **undo pim ipv6 silent** command cancels the PIM silent (IPv6) function on an interface.

By default, the PIM silent (IPv6) function is disabled on an interface.

Format

pim ipv6 silent

undo pim ipv6 silent

Parameters

None

Views

GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, VLANIF interface view, loopback interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To protect the switch against pseudo PIM Hello (IPv6) messages sent from malicious hosts, configure the **pim ipv6 silent** command on the interface directly connected to the host network segment to set the interface to PIM silent (IPv6) mode. Then the interface cannot receive or forward any PIM (IPv6) packet, and all PIM (IPv6) neighbors and PIM (IPv6) state machines on this interface are deleted. This interface becomes the DR, but the MLD function on the interface is not affected.

The PIM silent (IPv6) function applies only to the interface directly connected to a host network segment, and only one PIM switch can be connected to this network segment.

Prerequisites

IPv6 multicast routing has been enabled using the **multicast ipv6 routing-enable** command in the system view.

Precautions

Running the **pim ipv6 silent** command failed on the VLANIF interface because Layer 2 multicast querier or report-suppress is enabled for this VLAN.

If PIM BFD (IPv6) function is enabled on the interface, this command cannot be configured.

This command and **pim ipv6 timer dr-switch-delay** command are mutually exclusive.

NOTICE

After you run this command on an interface, the interface no longer receives or sends any PIM (IPv6) packets and other PIM (IPv6) functions on the interface become invalid. Confirm your action before using this command.

If a host network segment is connected to multiple switches and PIM silent (IPv6) is enabled on multiple interfaces, all these interfaces become static DRs. This causes multicast forwarding failures.

Example

Configure the PIM silent (IPv6) function on VLANIF100.

```
<HUAWEI> system-view
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] ipv6 enable
[HUAWEI-Vlanif100] pim ipv6 silent
```

Configure the PIM silent (IPv6) function on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] ipv6 enable
[HUAWEI-GigabitEthernet0/0/1] pim ipv6 silent
```

8.4.60 pim ipv6 sm

Function

The **pim ipv6 sm** command enables PIM-SM (IPv6) on an interface.

The **undo pim ipv6 sm** command disables PIM-SM (IPv6).

By default, PIM-SM (IPv6) is disabled on an interface.

Format

pim ipv6 sm

undo pim ipv6 sm

Parameters

None

Views

GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, VLANIF interface view, loopback interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After PIM-SM (IPv6) is enabled on interfaces, devices can set up PIM neighbor relationships with each other and process protocol packets received from PIM neighbors.

Prerequisites

IPv6 multicast routing has been enabled using the **multicast ipv6 routing-enable** command in the system view.

Precautions

PIM-DM (IPv6) and PIM-SM (IPv6) cannot be enabled simultaneously on the device.

If PIM-SM (IPv6) and MLD need to be enabled on the same interface, enable PIM-SM (IPv6), and then enable MLD.

Running the **pim ipv6 sm** command failed on the VLANIF interface because Layer 2 multicast querier or report-suppress is enabled for this VLAN.

If both Layer 2 and Layer 3 multicast services are required in a VLAN, enable PIM (IPv6) on the corresponding VLANIF interface first, and then enable MLD snooping in the VLAN. If MLD snooping is enabled in the VLAN first, PIM (IPv6) cannot be enabled on the VLANIF interface.

Example

Enable PIM-SM (IPv6) on VLANIF100.

```
<HUAWEI> system-view
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] ipv6 enable
[HUAWEI-Vlanif100] pim ipv6 sm
```

Enable PIM-SM (IPv6) on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] ipv6 enable
[HUAWEI-GigabitEthernet0/0/1] pim ipv6 sm
```

8.4.61 pim ipv6 state-refresh-capable

Function

The **pim ipv6 state-refresh-capable** command enables PIM-DM (IPv6) State-Refresh on an interface.

The **undo pim ipv6 state-refresh-capable** command disables PIM-DM (IPv6) State-Refresh.

By default, PIM-DM (IPv6) State-Refresh is enabled.

Format

pim ipv6 state-refresh-capable

undo pim ipv6 state-refresh-capable

Parameters

None

Views

GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, VLANIF interface view, loopback interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

PIM-DM (IPv6) State-Refresh is implemented by periodically sending State-Refresh messages in the network. After receiving a State-Refresh message, the switch in the pruned state resets the prune-status timer, preventing the downstream interface from forwarding packets.

After PIM-DM (IPv6) state-refresh is disabled, the interface starts to forward multicast data when the prune timer expires. The downstream routers that do not require the data send Prune messages. The process repeats and wastes a lot of network resources. Enabling PIM-DM (IPv6) State-Refresh can reduce traffic on the network.

Prerequisites

IPv6 multicast routing has been enabled using the **multicast ipv6 routing-enable** command in the system view.

Precautions

This command is valid for only PIM-DM (IPv6).

Example

Disable PIM-DM (IPv6) State-Refresh on VLANIF100.

```
<HUAWEI> system-view
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] ipv6 enable
[HUAWEI-Vlanif100] undo pim ipv6 state-refresh-capable
```

Disable PIM-DM (IPv6) State-Refresh on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] ipv6 enable
[HUAWEI-GigabitEthernet0/0/1] undo pim ipv6 state-refresh-capable
```

8.4.62 pim ipv6 timer dr-switch-delay

Function

The **pim ipv6 timer dr-switch-delay** command enables PIM DR switching delay and configures the delay on an interface. When the interface changed from a DR to a non-DR, the interface continues to forward data before the delay expires.

The **undo pim ipv6 timer dr-switch-delay** command disables PIM DR switching delay on the interface.

By default, when the interface changes from a DR to a non-DR, the interface stops forwarding data immediately.

Format

pim ipv6 timer dr-switch-delay *interval*

undo pim ipv6 timer dr-switch-delay

Parameters

Parameter	Description	Value
interval	Specifies the delay.	The value is an integer that ranges from 10 to 3600, in seconds.

Views

GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, VLANIF interface view, loopback interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If the DR on a shared network segment becomes the non-DR, original multicast forwarding entries will be deleted immediately, causing multicast data interruption in a short time. To solve the problem, set the DR switching delay. Original multicast forwarding entries still take effect until the delay is reached.

Prerequisites

IPv6 multicast routing has been enabled using the **multicast ipv6 routing-enable** command in the system view.

Precautions

This command is valid for only PIM-SM (IPv6).

This command and **pim ipv6 silent** command are mutually exclusive.

Example

Enable PIM DR switching delay on VLANIF100 and set the delay to 20 seconds.

```
<HUAWEI> system-view
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] interface vlanif 100
```



```
[HUAWEI-Vlanif100] ipv6 enable
[HUAWEI-Vlanif100] pim ipv6 timer dr-switch-delay 20
```

Enable PIM DR switching delay on GE0/0/1 and set the delay to 20 seconds.

```
<HUAWEI> system-view
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] ipv6 enable
[HUAWEI-GigabitEthernet0/0/1] pim ipv6 timer dr-switch-delay 20
```

8.4.63 pim ipv6 timer graft-retry

Function

The **pim ipv6 timer graft-retry** command sets the interval for retransmitting Graft messages on an interface.

The **undo pim ipv6 timer graft-retry** command restores the default value of the interval.

By default, the interval for retransmitting Graft messages on an interface is 3 seconds.

Format

pim ipv6 timer graft-retry *interval*

undo pim ipv6 timer graft-retry

Parameters

Parameter	Description	Value
interval	Specifies the interval of retransmitting Graft messages.	The value is an integer that ranges from 1 to 65535, in seconds.

Views

GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, VLANIF interface view, loopback interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In PIM-DM (IPv6) mode, when a member joins a pruned group, the switch sends a Graft message and waits to receive an ACK message from the upstream switch. If the downstream switch does not receive the ACK message in the period configured through the command, the switch resends the Graft message until the switch receives the ACK message from the upstream switch.

Prerequisites

IPv6 multicast routing has been enabled using the **multicast ipv6 routing-enable** command in the system view.

Precautions

This command is valid for only PIM-DM (IPv6).

Example

Set the interval for retransmitting Graft messages to 80s on VLANIF100.

```
<HUAWEI> system-view
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] ipv6 enable
[HUAWEI-Vlanif100] pim ipv6 timer graft-retry 80
```

Set the interval for retransmitting Graft messages to 80s on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] ipv6 enable
[HUAWEI-GigabitEthernet0/0/1] pim ipv6 timer graft-retry 80
```

8.4.64 pim ipv6 timer hello

Function

The **pim ipv6 timer hello** command sets the interval for sending Hello messages on an interface.

The **undo pim ipv6 timer hello** command restores the default value of the interval.

By default, the interval for sending Hello messages on an interface is 30 seconds.

Format

pim ipv6 timer hello *interval*

undo pim ipv6 timer hello

Parameters

Parameter	Description	Value
interval	Specifies the interval for sending Hello messages.	The value is an integer that ranges from 1 to 18000, in seconds.

Views

GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, VLANIF interface view, loopback interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

PIM devices periodically send Hello messages to maintain PIM neighbor relationships. You can run the **pim ipv6 timer hello** command to set the interval for sending Hello messages.

Prerequisites

IPv6 multicast routing has been enabled globally using the **multicast ipv6 routing-enable** command in the system view.

Precautions

This command is valid for both PIM-DM (IPv6) and PIM-SM (IPv6).

The interval for sending Hello messages must be shorter than the timeout period of PIM neighbors. You can run the **pim ipv6 hello-option holdtime** command to set the timeout period of PIM neighbors.

The configuration is the same as the **timer hello (IPv6)** command in the PIM-IPv6 view. The configuration in the interface view takes precedence over the configuration in the PIM-IPv6 view. The value configured in the PIM-IPv6 view is used if no value is configured on the interface.

Example

Set the interval for sending Hello messages to 40 seconds on VLANIF100.

```
<HUAWEI> system-view
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] ipv6 enable
[HUAWEI-Vlanif100] pim ipv6 timer hello 40
```

Set the interval for sending Hello messages to 40 seconds on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] ipv6 enable
[HUAWEI-GigabitEthernet0/0/1] pim ipv6 timer hello 40
```

8.4.65 pim ipv6 timer join-prune

Function

The **pim ipv6 timer join-prune** command sets the interval for periodically sending Join/Prune messages to the upstream device.

The **undo pim ipv6 timer join-prune** command restores the default interval.

By default, the interval for periodically sending Join/Prune messages to the upstream device is 60 seconds.

Format

pim ipv6 timer join-prune *interval*

undo pim ipv6 timer join-prune

Parameters

Parameter	Description	Value
interval	Specifies the interval at which Join/Prune messages are sent.	The value is an integer that ranges from 1 to 18000, in seconds.

Views

GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, VLANIF interface view, loopback interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The device sends join information to the upstream device, requesting the upstream device to forward multicast data. The device sends prune information to the upstream device, requesting the upstream device to stop forwarding multicast data. Join information and prune information are encapsulated in Join/Prune messages. The device periodically sends Join/Prune messages to the upstream device to update the forwarding status.

Prerequisites

IPv6 multicast routing has been enabled globally using the **multicast ipv6 routing-enable** command in the system view.

Precautions

This command is valid for both PIM-DM (IPv6) and PIM-SM (IPv6).

The interval configured through this command must be shorter than the interval configured through the **pim ipv6 holdtime join-prune** command. The interval at which Join or Prune messages are sent must be shorter than the holdtime carried in Join/Prune messages.

The configuration is the same as that of the **timer join-prune (IPv6)** command in the PIM-IPv6 view. The system prefers the configuration in the interface view. The value configured in the PIM-IPv6 view is used if no value is configured on the interface.

Example

Set the interval for sending Join or Prune messages to 80 seconds on VLANIF100.

```
<HUAWEI> system-view
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] ipv6 enable
[HUAWEI-Vlanif100] pim ipv6 timer join-prune 80
```

Set the interval for sending Join or Prune messages to 80 seconds on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] ipv6 enable
[HUAWEI-GigabitEthernet0/0/1] pim ipv6 timer join-prune 80
```

8.4.66 pim ipv6 triggered-hello-delay

Function

The **pim ipv6 triggered-hello-delay** command sets the maximum delay for triggering Hello messages.

The **undo pim ipv6 triggered-hello-delay** command restores the default maximum delay.

By default, the maximum delay for triggering Hello messages is 5 seconds.

Format

pim ipv6 triggered-hello-delay *interval*

undo pim ipv6 triggered-hello-delay

Parameters

Parameter	Description	Value
interval	Specifies the maximum delay for triggering Hello messages.	The value is an integer that ranges from 1 to 5, in seconds.

Views

GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, VLANIF interface view, loopback interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Conflicts will occur if multiple PIM devices sending Hello message at the same time. To avoid such conflicts, when a PIM device detects Hello messages on the network, it waits for a random delay that is smaller than the value configured using this command before sending a Hello message.

To avoid the conflict caused by multiple PIM devices sending Hello message at the same time, the PIM device automatically selects a random number smaller than the configured value as the delay. When detecting Hello messages in the network, the PIM device sends Hello message after the delay.

Prerequisites

IPv6 multicast routing has been enabled globally using the **multicast ipv6 routing-enable** command in the system view.

Example

Set the maximum delay for triggering the Hello message to 3 seconds.

```
<HUAWEI> system-view
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] ipv6 enable
[HUAWEI-Vlanif100] pim ipv6 triggered-hello-delay 3
```

Set the maximum delay for triggering the Hello message to 3 seconds.

```
<HUAWEI> system-view
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] ipv6 enable
[HUAWEI-GigabitEthernet0/0/1] pim ipv6 triggered-hello-delay 3
```

8.4.67 probe-interval (IPv6)

Function

The **probe-interval** command sets the interval for a switch to send Probe messages (null Register message) to the RP.

The **undo probe-interval** command restores the default value of the interval.

By default, the interval for a switch to send Probe messages to the RP is 5 seconds.

Format

probe-interval *interval*

undo probe-interval

Parameters

Parameter	Description	Value
interval	Specifies the interval for sending Probe messages to RP.	The value is an integer that ranges from 1 to 1799, in seconds.

Views

PIM-IPv6 view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When receiving a Register-Stop message sent by the RP, the DR at the source side stops sending Register messages and enters the register suppression state.

During the register suppression, the DR at the source side sends Probe messages to notify the RP that the multicast source is still in the Active state. After the register suppression times out, the DR at the source side starts to send Register messages.

Prerequisites

IPv6 multicast routing has been enabled globally using the **multicast ipv6 routing-enable** command in the system view.

Precautions

This command is valid for only PIM-SM (IPv6).

The interval set using the **probe-interval** command must be less than half the interval set using the **register-suppression-timeout (IPv6)** command.

Example

In the PIM-IPv6 view, set the interval for sending Probe messages to RP to 6 seconds.

```
<HUAWEI> system-view
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] pim-ipv6
[HUAWEI-pim6] probe-interval 6
```

8.4.68 register-policy (IPv6)

Function

The **register-policy** command sets the rules used by an RP to filter Register messages.

The **undo register-policy** command restores the default setting.

By default, the rules for filtering Register messages are not configured.

Format

register-policy *advanced-acl6-number*

undo register-policy

Parameters

Parameter	Description	Value
advanced-acl6-number	Specifies the number of the advanced ACL that defines the rules for filtering packets based on source addresses or group addresses.	The value is an integer that ranges from 3000 to 3999.

Views

PIM-IPv6 view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To prevent the attack of invalid Register messages, you can configure devices to receive or deny Register messages according to the packet filtering rules.

If the ACL rejects an (S, G) entry contained in a Register message or the ACL does not filter this entry, the RP sends a Register-Stop message to the DR on the source side to stop the registration of this multicast data stream.

The **register-policy** command and the **acl ipv6** command are used together. In the ACL6 view, you can set the multicast source address range by specifying the **source** parameter in the **rule** command, and set the multicast group address range by specifying the **destination** parameter in the **rule** command.

The configurations of the IPv6 Named ACL and the advanced ACL are the same, and can implement filtering of both source addresses and multicast group addresses. The Named ACL can also be configured with the **time-range** parameter.

Prerequisites

IPv6 multicast routing has been enabled globally using the **multicast ipv6 routing-enable** command in the system view.

Precautions

NOTICE

When the **register-policy** command is used on the RP, only Register messages matching the rule of the ACL are received by the RP. If an undefined ACL is specified, the RP denies all Register messages.

This command is valid for only PIM-SM (IPv6).

The **register-policy** command takes effect for only subsequently received Register messages. The multicast entries that have been registered successfully are not deleted and can still be used for multicast data forwarding.

Example

Configure the RP to receive Register packets sent by the multicast source on the network segment FC00:0:0:2001::2/64 to the multicast group FF02:13::/64.

```
<HUAWEI> system-view
[HUAWEI] acl ipv6 3000
[HUAWEI-acl6-adv-3000] rule permit ipv6 source fc00:0:0:2001::2 64 destination ff02:13:: 64
[HUAWEI-acl6-adv-3000] quit
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] pim-ipv6
[HUAWEI-pim6] register-policy 3000
```

8.4.69 register-source (IPv6)

Function

The **register-source** command specifies the source IPv6 address used by the source's DR to send Register messages.

The **undo register-source** command restores the default setting.

By default, the source IPv6 address used by the source's DR to send Register messages is not specified.

Format

register-source *ipv6-address*

undo register-source

Parameters

Parameter	Description	Value
ipv6-address	Specifies the global IPv6 unicast address of the registered source.	-

Views

PIM-IPv6 view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the source IPv6 address for sending Register messages is no longer the only IPv6 address in the network for the RP device or the source IPv6 address is filtered

out, errors occur in the registration process and extra traffic occupies bandwidth on the network. In this case, use the **register-source** command to specify an appropriate interface as the source IPv6 address for sending Register messages. Using the loopback address of the source's DR as the source IPv6 address is recommended.

Prerequisites

IPv6 multicast routing has been enabled globally using the **multicast ipv6 routing-enable** command in the system view.

Before specifying the source IPv6 unicast address for sending Register messages, enable PIM-SM.

Precautions

The command is effective only when the specified interface is in Up state.

Example

Specify the source IPv6 address used by the source's DR to send Register message as FC00:0:0:1101::1.

```
<HUAWEI> system-view
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] pim-ipv6
[HUAWEI-pim6] register-source fc00:0:0:1101::1
```

8.4.70 register-suppression-timeout (IPv6)

Function

The **register-suppression-timeout** command sets the timeout period during which a switch keeps the register suppression state.

The **undo register-suppression-timeout** command restores the default timeout period.

By default, a switch keeps the register suppression state for 60 seconds.

Format

register-suppression-timeout *interval*

undo register-suppression-timeout

Parameters

Parameter	Description	Value
interval	Specifies the timeout period during which the switch keeps the register suppression state.	The value is an integer that ranges from 11 to 3600, in seconds.

Views

PIM-IPv6 view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After receiving a Register-Stop message from the RP, the switch immediately stops sending Register messages and enters the register suppression state.

The **register-suppression-timeout** command determines how long the switch keeps the register suppression state. When the timeout period expires, the switch (source DR) starts to send Register messages to the RP.

Prerequisites

IPv6 multicast routing has been enabled globally using the **multicast ipv6 routing-enable** command in the system view.

Precautions

This command is valid only for PIM-SM (IPv6).

If the timeout period is too short, the RP receives burst multicast data more frequently. If the timeout period is too long, there will be a long delay for a new receiver to join a group when an (S, G) entry on the RP times out.

You can use the **probe-interval (IPv6)** command to configure the switch to send null Register messages before the suppression timer times out. This configuration reduces burst Register messages and shortens the timeout period to reduce the delay for a new receiver to join a group.

Example

In the PIM-IPv6 view, set the timeout period during which the switch keeps the register suppression state to 70 seconds.

```
<HUAWEI> system-view
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] pim-ipv6
[HUAWEI-pim6] register-suppression-timeout 70
```

8.4.71 reset pim ipv6 control-message counters

Function

The **reset pim ipv6 control-message counters** command resets the statistics about PIM (IPv6) control messages.

Format

reset pim ipv6 control-message counters [**interface** *interface-type interface-number*]

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Specifies the name and the number of an interface. It is used to reset the statistics about PIM (IPv6) control messages on a specified interface.	-

Views

User view

Default Level

3: Management level

Usage Guidelines

If an interface with PIM (IPv6) enabled has been forwarding multicast packets for a long time, the switch stores statistics on a large number of control messages. You can run this command to reset statistics on control messages.

Example

Reset the statistics about PIM (IPv6) control messages on all interfaces.

```
<HUAWEI> reset pim ipv6 control-message counters
```

8.4.72 reset pim ipv6 routing-table

Function

The **reset pim ipv6 routing-table** command clears PIM status of the specified downstream interface of a specified PIM (IPv6) entry.

Format

reset pim ipv6 routing-table group *ipv6-group-address* **mask** *ipv6-group-mask-length* **source** *ipv6-source-address* **interface** *interface-type interface-number*

Parameters

Parameter	Description	Value
group *ipv6-group-address*	Specifies the group address of an IPv6 PIM entry.	The address is a 32-digit hexadecimal number, in the format X:X:X:X:X:X:X:X. An IPv6 multicast address starts with FF.

Parameter	Description	Value
mask *ipv6-group-mask-length*	Specifies the mask length of an IPv6 multicast group address.	The value is an integer that ranges from 0 to 128.
source *ipv6-source-address*	Specifies the source address of an IPv6 PIM entry.	The address is a 32-digit hexadecimal number, in the format X:X:X:X:X:X:X:X.
interface *interface-type interface-number*	Specifies the type and number of an interface.	-

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

The **reset pim ipv6 routing-table** command clears PIM status of the specified downstream interface of a specified PIM entry.

Configuration Impact

Using this command can clear the PIM status of the specified interface in a specified PIM entry. The command cannot be used to clear the MLD and static group join status on a specified interface.

Precautions

This command is valid for only PIM-SM (IPv6).

NOTICE

Clearing PIM status of the downstream interfaces can trigger sending of Join/Prune messages, which causes multicast service interruption.

Example

Clear PIM status of the downstream interface VLANIF100 of the (S, G) entry (FC00:0:0:2001::4,FF25::1).

```
<HUAWEI> reset pim ipv6 routing-table group ff25::1 mask 128 source fc00:0:0:2001::4 interface vlanif 100
```


8.4.73 source-lifetime (IPv6)

Function

The **source-lifetime** command specifies the timeout period of (S, G) entries on the switch.

The **undo source-lifetime** command restores the default value of the timeout period.

By default, the timeout period is 210 seconds.

Format

source-lifetime { *interval* | **infinity** } [**group-policy** *acl6-number*]

undo source-lifetime

undo source-lifetime { *interval* | **infinity** } [**group-policy** *acl6-number*]

Parameters

Parameter	Description	Value
interval	Specifies the timeout period of (S, G) entries on the switch.	The value is an integer that ranges from 60 to 65535, in seconds.
infinity	Indicates that (S, G) entries on the switch will never age out.	-
group-policy	Specifies a group policy to determine to which the configured timeout period takes effect.	-
acl6-number	Specifies the number of a basic or advanced ACL.	The value is an integer that ranges from 2000 to 3999.

Views

PIM-IPv6 view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A switch creates a timer for each (S, G) entry. The **source-lifetime** command is used to set the value of the timer. After receiving a multicast packet from S, the interface resets the timer. If the timer times out, the (S, G) entry is considered invalid.

- If you configure **source-lifetime** *interval*, the configured timeout period applies to all (S, G) entries.
- If you configure **source-lifetime** *interval* { **group-policy** *acl6-number* }:
  - If you specify an advanced ACL name in the command, the configured timeout period applies to the (S, G) entries in which the source and group addresses are permitted by the specified ACL.
  - If you specify a basic ACL number in the command, the configured timeout period applies to the (S, G) entries in which the source addresses are permitted by the specified ACL.
  - If you specify an advanced ACL number in the command, the configured timeout period applies to the (S, G) entries in which the source and group addresses are permitted by the specified ACL.
- If you configure **source-lifetime infinity**, all (S, G) entries will never age out.
- If you configure **source-lifetime infinity** { **group-policy** *acl6-number* }:
  - If you specify an advanced ACL name in the command, the (S, G) entries in which the source and group addresses are permitted by the specified ACL will never age out.
  - If you specify a basic ACL number in the command, the (S, G) entries in which the source addresses are permitted by the specified ACL will never age out.
  - If you specify an advanced ACL number in the command, the (S, G) entries in which the source and group addresses are permitted by the specified ACL will never age out.

If you run this command multiple times for the same range of multicast forwarding entries and specify *interval* and **infinity** respectively in the commands, **infinity** takes precedence over *interval*.

Prerequisites

IPv6 multicast routing has been enabled using the **multicast ipv6 routing-enable** command in the system view.

Precautions

This command is valid for both PIM-DM (IPv6) and PIM-SM (IPv6).

Example

Set the timeout period of (S, G) entries on the switch to 200 seconds.

```
<HUAWEI> system-view
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] pim-ipv6
[HUAWEI-pim6] source-lifetime 200
```

8.4.74 source-policy (IPv6)

Function

The **source-policy** command configures the switch to filter received multicast data packets based on source addresses or source/group addresses.

The **undo source-policy** command deletes the configuration.

By default, a switch does not filter received multicast data packets based on source addresses or source/group addresses.

Format

source-policy *acl6-number*

undo source-policy

Parameters

Parameter	Description	Value
acl6-number	Specifies number of the basic or advanced ACL.	The value is an integer that ranges from 2000 to 3999.

Views

PIM-IPv6 view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To prevent unauthorized source information from being advertised on the PIM network, run the **source-policy** command to configure the switch to filter received multicast data packets based on source addresses or source/group addresses.

Prerequisites

IPv6 multicast routing has been enabled globally using the **multicast ipv6 routing-enable** command in the system view.

Configuration Impact

For the numbered ACL, the **source-policy** command and the **acl ipv6acl ipv6** command are used together.

- In the basic ACL6 view, you can set the source address range of multicast packets by specifying the **source** parameter in the **rule** command.
- In the advanced ACL6 view, you can set the source address range of multicast packets by specifying the **source** parameter in the **rule** command, and set the multicast group IPv6 address range by specifying the **destination** parameter in the **rule** command.

The configurations of the named ACL and advanced ACL are the same, and can filter both source addresses and group addresses. A named ACL can also be configured with the **time-range** parameter.

Precautions

This command is valid for both PIM-DM (IPv6) and PIM-SM (IPv6).

Example

In the public network instance, configure the switch to receive multicast data packets with the source address of FC00:0:0:3121::1 and to discard those with the source address of FC00:0:0:3121::2.

```
<HUAWEI> system-view
[HUAWEI] acl ipv6 number 2001
[HUAWEI-acl6-basic-2001] rule permit source fc00:0:0:3121::1 128
[HUAWEI-acl6-basic-2001] rule deny source fc00:0:0:3121::2 128
[HUAWEI-acl6-basic-2001] quit
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] pim-ipv6
[HUAWEI-pim6] source-policy 2001
```

8.4.75 spt-switch-threshold (IPv6)

Function

The **spt-switch-threshold** command sets the rate threshold of the multicast packets when the DR at the member side joins the SPT.

The **undo spt-switch-threshold** command restores the default value.

By default, the system performs SPT switchover on receiving the first multicast data packet through the RPT.

Format

spt-switch-threshold { *traffic-rate* | **infinity** } [**group-policy** { *basic-acl6-number* } [**order** *order-value*]]

undo spt-switch-threshold [*traffic-rate* | **infinity**] [**group-policy** { *basic-acl6-number* }]

Parameters

Parameter	Description	Value
traffic-rate	Specifies the threshold rate for the switchover from the RPT to the SPT. **NOTE** Setting this parameter may affect operation of multicast services. You are advised to use the default triggering condition. That is, an SPT switchover is triggered immediately after the first multicast data packet is received from the RPT. The default triggering condition can reduce the number of multicast packets forwarded on the RPT.	The value is an integer that ranges from 1 to 4194304, in kbit/s.
infinity	Indicates that the SPT switchover is never enabled.	-

Parameter	Description	Value
basic-acl6-number	Specifies an entry of the group-policy list. It works with the multicast group that matches *basic-acl6-number* to enable the threshold. *basic-acl6-number* specifies the number of the basic ACL that defines the range of multicast groups.	If the parameter is not set, the threshold is applied to all multicast groups. The value ranges from 2000 to 2999.
order *order-value*	Adjusts the order of the ACLs in the group-policy list. If a group matches multiple ACLs, the threshold is selected in the order specified by *order-value*. *order-value* specifies the updated number.	The value is an integer. The value is any value other than original one in the current group-policy list. If the parameter is not set, the order of the ACLs in the group-policy list does not change.

Views

PIM-IPv6 view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The source's DR encapsulates multicast packets in a Register message, and then transmits the unicast Register message to the RP. Then, the RP decapsulates the Register message and forwards the multicast packets to the receivers along the RPT. By default, when the RP or receiver's DR receives the first multicast packet, it initiates an SPT switchover to the source.

After the **spt-switch-threshold** command is executed on the receiver's DR, the receiver's DR periodically checks the forwarding rate of multicast packets. When the forwarding rate exceeds the threshold, the receiver's DR sends a Join messages to the source, triggering the SPT switchover.

Prerequisites

IPv6 multicast routing has been enabled globally using the **multicast ipv6 routing-enable** command in the system view.

Configuration Impact

If this command is used several times for the same group, the first matched command takes effect.

This command is valid to all devices that may function as the DR at the member side, but is invalid to RPs.

Precautions

This command is valid for only PIM-SM (IPv6).

Example

Set the threshold to 4 kbit/s. If the transmission rate of packets from the source to the multicast group is higher than the threshold, the switch switches packets to the SPT towards the source.

```
<HUAWEI> system-view
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] pim-ipv6
[HUAWEI-pim6] spt-switch-threshold 4
```

Add a group-policy: the ACL number, rate threshold, and order of the group-policy are 2010, 100 kbit/s, and 1 respectively.

```
<HUAWEI> system-view
[HUAWEI] acl ipv6 2010
[HUAWEI-acl6-basic-2010] rule permit source ff02:: 96
[HUAWEI-acl6-basic-2010] quit
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] pim-ipv6
[HUAWEI-pim6] spt-switch-threshold 100 group-policy 2010 order 1
```

8.4.76 ssm-policy (IPv6)

Function

The **ssm-policy** command sets the range of SSM group addresses.

The **undo ssm-policy** command restores the default configuration.

By default, the range of IPv6 SSM group addresses is FF3x::/32. (The value of x ranges from 0 to F.)

Format

ssm-policy *basic-acl6-number*

undo ssm-policy

Parameters

Parameter	Description	Value
basic-acl6-number	Specifies the number of the basic ACL that defines the range of SSM group addresses.	The value is an integer that ranges from 2000 to 2999.

Views

PIM-IPv6 view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

By default, the SSM group address range is FF3x::/32. The value of x ranges from 0 to F. You can run the **ssm-policy** command to specify the range of PIM SSM group addresses. All the PIM-SM (IPv6) interfaces consider that PIM SSM is enabled on all the multicast groups in the specified address range. The specified SSM group address range can exceed the default group address range.

Prerequisites

IPv6 multicast routing has been enabled using the **multicast ipv6 routing-enable** command in the system view.

Precautions

If Multicast Listener Discovery version 2 (MLDv2) is used to add an (S, G) entry, this command does not take effect.

The **ssm-policy** command and the **acl ipv6acl ipv6** command are used together.

- For the numbered ACL6, in the ACL6 view, you can set the IPv6 address range of SSM multicast groups by specifying the **source** parameter in the **rule (basic ACL6 view)** command.
- For the named ACL6, in the ACL6 view, when the **rule (basic ACL6 view)** command is used to configure a filtering rule, the filtering rule is effective only with the multicast group address range that is specified by the **destination** parameter and with the time period that is specified by the **time-range** parameter.

This command is valid for only PIM-SM (IPv6).

Example

Set the range of PIM SSM multicast addresses to FF31:0:8192::/96.

```
<HUAWEI> system-view
[HUAWEI] acl ipv6 2000
[HUAWEI-acl6-basic-2000] rule permit source ff31:0:8192:: 96
[HUAWEI-acl6-basic-2000] quit
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] pim-ipv6
[HUAWEI-pim6] ssm-policy 2000
```

8.4.77 state-refresh-interval (IPv6)

Function

The **state-refresh-interval** command sets the interval for sending PIM State-Refresh messages.

The **undo state-refresh-interval** command restores the default value of the interval.

By default, the interval for sending PIM State-Refresh messages is 60 seconds.

Format

state-refresh-interval *interval*

undo state-refresh-interval

Parameters

Parameter	Description	Value
interval	Specifies the interval for sending PIM State-Refresh messages.	The value is an integer that ranges from 1 to 255, in seconds.

Views

PIM-IPv6 view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On the PIM-DM (IPv6) network, the device periodically sends State-Refresh messages to update the timeout interval of the prune timer on the downstream device. By doing this, the interface that has no multicast requirements retains in prune state.

Prerequisites

IPv6 multicast routing has been enabled using the **multicast ipv6 routing-enable** command in the system view.

Precautions

This command is valid for only PIM-DM (IPv6).

To prevent a pruned interface from forwarding packets when the Prune status times out, the interval for sending State-Refresh messages is shorter than the period for keeping the Prune status.

You can run the **holdtime join-prune (IPv6)** command to set the period during which the device keeps the Prune status.

This command takes effect only when it is run on the routers directly connected to the source.

Example

Set the interval for sending PIM State-Refresh messages to 70s.

```
<HUAWEI> system-view
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] pim-ipv6
[HUAWEI-pim6] state-refresh-interval 70
```


8.4.78 state-refresh-rate-limit (IPv6)

Function

The **state-refresh-rate-limit** command sets the minimum period to wait before receiving the next PIM State-Refresh message.

The **undo state-refresh-rate-limit** command restores the default value.

By default, the minimum period to wait to receive the next PIM State-Refresh message is 30 seconds.

Format

state-refresh-rate-limit *interval*

undo state-refresh-rate-limit

Parameters

Parameter	Description	Value
interval	Specifies the minimum period for waiting to receive the next PIM State-Refresh message.	The value is an integer that ranges from 1 to 65535, in seconds.

Views

PIM-IPv6 view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A switch can receive multiple PIM State-Refresh messages in a short period. Some of the messages are the same. To avoid duplicate messages, you can run the **state-refresh-rate-limit** command to set the period to wait to receive the next State-Refresh message.

- Before the State-Refresh timer times out, the switch discards the received duplicate State-Refresh messages.
- After the State-Refresh timer times out, the switch can receive the next State-Refresh message.

Prerequisites

IPv6 multicast routing has been enabled using the **multicast ipv6 routing-enable** command in the system view.

Precautions

This command is valid for only PIM-DM (IPv6).

Example

Set the minimum period to wait to receive the next PIM State-Refresh message to 45s.

```
<HUAWEI> system-view
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] pim-ipv6
[HUAWEI-pim6] state-refresh-rate-limit 45
```

8.4.79 state-refresh-ttl (IPv6)

Function

The **state-refresh-ttl** command sets the TTL value for sending PIM State-Refresh messages.

The **undo state-refresh-ttl** command restores the default value of the TTL.

By default, the TTL value for sending PIM State-Refresh messages is 255.

Format

state-refresh-ttl *ttl-value*

undo state-refresh-ttl

Parameters

Parameter	Description	Value
ttl-value	Specifies the minimum TTL value of the PIM state refresh message sent by an interface.	The value is an integer that ranges from 1 to 255.

Views

PIM-IPv6 view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After receiving a State-Refresh message, the switch decreases the value of the TTL in the message by 1, and then sends the message to the downstream switch until the value of the TTL becomes 0. If the scale of the network is small, the message is delivered in a loop.

You can use the **state-refresh-ttl** command to set the value of the TTL according to the scale of the network.

Prerequisites

IPv6 multicast routing has been enabled using the **multicast ipv6 routing-enable** command in the system view.

Precautions

This command is valid for only PIM-DM (IPv6).

This command takes effect only when it is run on the routers directly connected to the source.

Example

Set the TTL value for sending PIM State-Refresh messages to 45.

```
<HUAWEI> system-view
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] pim-ipv6
[HUAWEI-pim6] state-refresh-ttl 45
```

8.4.80 static-rp (IPv6)

Function

The **static-rp** command configures a static RP.

The **undo static-rp** command restores the default configuration.

By default, no static RP is configured.

Format

static-rp *rp-address* [*basic-acl6-number*] [**preferred**]

undo static-rp *rp-address*

Parameters

Parameter	Description	Value
rp-address	Specifies address of a static RP.	The address is a 32-digit hexadecimal number, in the format X:X:X:X:X:X:X:X.
basic-acl6-number	Specifies the basic ACL that is used to control the range of multicast groups served by a static RP.	The value is an integer that ranges from 2000 to 2999.
preferred	Indicates that the static RP is preferred.	-

Views

PIM-IPv6 view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When only one RP exists in the network, you can manually configure a static RP rather than a dynamic RP. This can reduce bandwidth used to exchange information between the C-RP and the BSR.

Prerequisites

IPv6 multicast routing has been enabled globally using the **multicast ipv6 routing-enable** command in the system view.

Configuration Impact

If the address of the static RP is the address of an interface in the Up state on the local host, the local host acts as the static RP. PIM (IPv6) does not need to be enabled on the interface of the static RP.

If no ACL number is specified in the command, the static RP serves all the multicast groups. If an ACL is specified but the ACL does not contain any rules, the static RP serves all the multicast groups. If the specified ACL has rules configured, the static RP serves only the multicast groups permitted by the ACL.

If the command used to configure the static RP does not contain **preferred**, devices apply BSR mechanism to elect a dynamic RP. If the dynamic RP is not configured in the network or the dynamic RP is invalid, the static RP becomes valid. If the command used to configure static RP contains **preferred**, the static RP is preferred.

If this command is used many times, multiple static RPs are configured. In the case that multiple static RPs serve a group, the RP with the largest IPv6 address is selected to serve the group. If *rp-address* of the RPs is identical, the latest RP replaces the previous one.

Precautions

The **static-rp** command and the **acl ipv6** command are used together. In the ACL6 view, when the **rule** command is used to configure a filtering rule, you can set the address range of multicast groups that are served by the static RP by specifying the **source** parameter in the **rule** command. The filtering rule is effective only with the **source** parameter and the time period specified by the **time-range** parameter.

NOTE

Up to 50 static RPs can be configured by using this command repeatedly, but the same ACL cannot correspond to multiple static RPs. If the ACL is not referenced, only one static RP can be configured.

To make the static RP work normally, run the **static-rp** command on all devices in the PIM-SM (IPv6) domain.

Example

Configure the switch with the address of FC00:0:0:1111::1111 as the static RP in the PIM-SM (IPv6) domain.

```
<HUAWEI> system-view
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] pim-ipv6
[HUAWEI-pim6] static-rp fc00:0:0:1111::1111
```

8.4.81 timer hello (IPv6)

Function

The **timer hello** command sets the interval at which the PIM switch sends Hello messages.

The **undo timer hello** command restores the default interval.

By default, the interval at which the PIM switch sends Hello messages is 30 seconds.

Format

timer hello *interval*

undo timer hello

Parameters

Parameter	Description	Value
interval	Specifies the interval at which Hello messages are sent.	The value is an integer that ranges from 1 to 18000, in seconds.

Views

PIM-IPv6 view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

PIM devices periodically send Hello messages to maintain PIM neighbor relationships. You can run the **pim ipv6 timer hello** command to set the interval for sending Hello messages.

Prerequisites

IPv6 multicast routing has been enabled globally using the **multicast ipv6 routing-enable** command in the system view.

Configuration Impact

This command is valid for both PIM-DM (IPv6) and PIM-SM (IPv6).

The interval at which the PIM device sends Hello messages should be less than the timeout period of the PIM neighbor. You can run the **hello-option holdtime (IPv6)** command to set the timeout period of PIM neighbors.

The **timer hello** command has the same function as the **pim ipv6 timer hello** command in the interface view. By default, if the **pim ipv6 timer hello** command is not used, the value configured in the PIM view is used; otherwise, the value configured in the interface view is used.

Example

Set the interval at which PIM Hello messages are sent to 40s.

```
<HUAWEI> system-view
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] pim-ipv6
[HUAWEI-pim6] timer hello 40
```

8.4.82 timer join-prune (IPv6)

Function

The **timer join-prune** command configures the interval at which Join/Prune messages are sent to an upstream device.

The **undo timer join-prune** command restores the default interval.

By default, the interval at which Join/Prune messages are sent to an upstream device is 60 seconds.

Format

timer join-prune *interval*

undo timer join-prune

Parameters

Parameter	Description	Value
interval	Specifies the interval for sending Join/Prune messages.	The value is an integer that ranges from 1 to 18000, in seconds.

Views

PIM-IPv6 view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The switch sends join information to the upstream device, requesting the upstream device to forward multicast data. The switch sends prune information to the upstream device, requesting the upstream device to stop forwarding multicast data. Join information and prune information are encapsulated in Join/Prune messages. The PIM switch periodically sends Join/Prune messages to the upstream switch to update the forwarding status.

Prerequisites

IPv6 multicast routing has been enabled globally using the **multicast ipv6 routing-enable** command in the system view.

Precautions

This command is valid for both PIM-DM (IPv6) and PIM-SM (IPv6).

The interval configured using the **timer join-prune** command must be shorter than the interval configured using the **holdtime join-prune (IPv6)** command.

The **timer join-prune** command has the same function as the **pim ipv6 timer join-prune** command in the interface view. By default, if the **pim ipv6 timer join-prune** command is not used, the value configured in the PIM view is used; otherwise, the value configured in the interface view is used.

Example

Set the interval at which Join/Prune messages are sent to 80s.

```
<HUAWEI> system-view
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] pim-ipv6
[HUAWEI-pim6] timer join-prune 80
```

8.4.83 timer spt-switch (IPv6)

Function

The **timer spt-switch** command sets the interval for checking whether the rate for transmitting multicast data exceeds the threshold before the switchover from the RPT to the SPT.

The **undo timer spt-switch** command restores the default value of the interval.

By default, the interval for checking whether the rate for transmitting multicast data exceeds the threshold before the switchover from the RPT to the SPT is 15 seconds.

Format

timer spt-switch *interval*

undo timer spt-switch

Parameters

Parameter	Description	Value
interval	Specifies the interval for checking whether the rate for transmitting multicast data exceeds the threshold before the switchover from RPT to SPT.	The value is an integer that ranges from 15 to 65535, in seconds.

Views

PIM-IPv6 view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can run the **timer spt-switch** command to set the interval for checking whether the rate for transmitting multicast data exceeds the threshold.

Prerequisites

IPv6 multicast routing has been enabled using the **multicast ipv6 routing-enable** command in the system view.

Precautions

This command is valid for only PIM-SM (IPv6).

Before running this command, you must set the threshold for SPT switchover by using the **spt-switch-threshold (IPv6)** command; otherwise, the **timer spt-switch** command takes no effect.

Example

Set the interval for checking the rate for transmitting the multicast data before the switchover from RPT to SPT to 30 seconds.

```
<HUAWEI> system-view
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] pim-ipv6
[HUAWEI-pim6] timer spt-switch 30
```

8.5 MSDP Configuration Commands

8.5.1 Command Support

Product	Support
S1700	Not supported.
S300	Supported.
S500	Supported.
S2700	Supported.
S5700	Supported except S5731-L and S5731S-L.
S6700	Supported.

NOTE

Only S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support the MSDP multi-instance feature.

8.5.2 cache-sa-enable

Function

The **cache-sa-enable** command enables the SA cache function on a switch. After receiving an SA message, the switch caches (S, G) information carried in the SA message.

The **cache-sa-disable** command disables the SA cache function.

The **undo cache-sa-enable** command disables the SA cache function.

By default, the SA cache function is enabled on a switch.

Format

cache-sa-enable

cache-sa-disable

undo cache-sa-enable

Parameters

None

Views

MSDP view of the public network instance or MSDP view of the VPN instance

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A switch enabled with the SA cache function locally saves (S, G) information carried in the received SA messages. When the switch receives requests for receiving multicast data, it directly obtains (S, G) information from the SA cache.

A switch no longer saves (S, G) information carried in the received SA messages locally after the **undo cache-sa-enable** or the **cache-sa-disable** command is run to disable the SA cache function. When the switch receives requests for receiving multicast data, it must wait for the SA messages sent by the MSDP peer in the next sending period. This may result in a delay in receiving multicast data.

Prerequisites

MSDP has been enabled using the **msdp** command.

Configuration Impact

When an RP receives a new (*, G) Join message,

- If the SA cache function is enabled, the RP searches the SA cache for the (S, G) information.
  - If the SA cache contains related (S, G) information, the RP directly joins the SPT with the root being S.
  - If the SA cache does not contain related (S, G) information, the RP does not process the received Join message.
- If the SA cache function is disabled, the RP processes the message in one of the following ways:
  - If the sending of SA Request messages is enabled, the RP sends an SA Request message to the specified MSDP peer and waits for the response.
  - If the sending of SA Request messages is disabled, the RP must wait for the SA message sent by the MSDP peer in the next sending period.

Precautions

The **cache-sa-disable** and **undo cache-sa-enable** commands' configurations are both **undo cache-sa-enable** in the configuration file.

Example

Disable the SA cache function on the switch.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] msdp
[HUAWEI-msdp] undo cache-sa-enable
```


8.5.3 display default-parameter msdp

Function

The **display default-parameter msdp** command displays default configurations about MSDP.

Format

display default-parameter msdp

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

This command still displays the default configurations even after the MSDP parameters are changed. You can use this command to check the consistency of default configurations about MSDP parameters on MSDP peers.

Example

Display default configurations about MSDP.

```
<HUAWEI> display default-parameter msdp
  MSDP View Default Configurations:
  ---------------------------------
  Cache-sa-enable: enabled
  Msdp description:
  Encap-data-enable: disabled
  Request-sa-enable: disabled
  Sa-request-policy: disabled
  Sa-policy: disabled
  Connect-retry-period: 30 s
  Minimum TTL: 0
```

Table 8-72 Description of the **display default-parameter msdp** command output

Item	Description
MSDP View Default Configurations	Default configurations in the MSDP view.

Item	Description
Cache-sa-enable	Whether SA cache is enabled. By default, SA cache is enabled. This parameter is configured using the **cache-sa-enable** command.
Msdp description	Whether MSDP peer description is configured. By default, no description is configured for an MSDP peer. This parameter is configured using the **peer description (MSDP)** command.
Encap-data-enable	Whether encapsulating multicast data packets into the SA message is enabled. By default, an SA message does not encapsulate any multicast packet. This parameter is configured using the **encap-data-enable** command.
Request-sa-enable	Whether sending an SA Request message immediately when a Join message is received. By default, when receiving a Join message, the switch waits for the SA message in the next period instead of sending an SA Request message to its MSDP peer. This parameter is configured using the **peer request-sa-enable** command.
Sa-request-policy	Whether the filtering rule for responding to the SA Request message is configured. By default, the switch is not configured with any filtering rule for responding to the SA Request message and responds to all SA Request messages from all MSDP peers. This parameter is configured using the **peer sa-request-policy** command.
Sa-policy	Whether the filtering rule for receiving or forwarding the SA message is configured. By default, the switch does not filter the received or forwarded SA messages. This parameter is configured using the **peer sa-policy** command.

Item	Description
Connect-retry-period	Interval for retrying to set up a TCP connection between MSDP peers. By default, the interval for retrying to set up an MSDP peer relationship is 30 seconds. This parameter is configured using the **timer retry** command.
Minimum TTL	TTL value of SA messages that are encapsulated with multicast data. By default, the TTL value of SA messages that are encapsulated with multicast data is 0. This parameter is configured using the **peer minimum-ttl** command.

8.5.4 display msdp brief

Function

The **display msdp brief** command displays summary information about the status of MSDP peers.

Format

display msdp [**vpn-instance** *vpn-instance-name* | **all-instance**] **brief** [**state** { **connect** | **down** | **listen** | **shutdown** | **up** }]

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Specifies a VPN instance. *vpn-instance-name* specifies the name of the VPN instance.	The value must be an existing VPN instance name.
all-instance	Indicates all the instances. If **vpn-instance** or **all-instance** is not specified, only the public network instance is displayed.	-
state	Displays summary information about the MSDP peers in specified status.	-
connect	Indicates the MSDP peers in Connect state.	-

Parameter	Description	Value
down	Indicates the MSDP peers in Down state.	-
listen	Indicates the MSDP peers in Listen state.	-
shutdown	Indicates the MSDP peers in Shutdown state.	-
up	Indicates the MSDP peers in Up state.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

After MSDP peers establish a TCP connection, the **display msdp brief** command can be used to display the brief information about the remote MSDP peer, such as the address, AS number, the number of (S, G) entries, and the status of the TCP connection.

Precautions

This command displays summary information about the status of MSDP peers only when the MSDP peer has been configured.

MSDP specifies that the peer with the higher IP address acts as the server and listens at port 639. The peer with the lower IP address acts as client and enables the connection. If the connection fails, the client enables the connection again.

Example

Display summary information about MSDP peers.

```
<HUAWEI> display msdp brief
MSDP Peer Brief Information
 Configured   Up          Listen      Connect     Shutdown     Down
 2            2           0           0           0            0

 Peer's Address     State     Up/Down time    AS     SA Count   Reset Count
 192.168.3.2        Up        01:07:08        ?      8          0
 192.168.5.1        Up        00:16:39        ?      13         0
```


Table 8-73 Description of the **display msdp brief** command output

Item	Description
MSDP Peer Brief Information	summary information about MSDP peers.
Configured	Total number of configured MSDP peers.
Up	Number of MSDP peers in Up state.
Listen	Number of MSDP peers in Listen state.
Connect	Number of MSDP peers in Connect state.
Shutdown	Number of MSDP peers in Shutdown state.
Down	Number of MSDP peers in Down state.
Peer's Address	Address of the peer. This parameter is configured using the **peer connect-interface (MSDP)** command.
State	Status of the MSDP session. • Up: The connection is set up and is in Up state. • Listen: The local device acts as the server and is in Listen state. The connection is not set up. • Connect: The local device acts as the client and is in Connect state. The connection is not set up. • Shutdown: The MSDP peer is in Shutdown state. • Down: The connection fails.
Up/Down time	Time when the session becomes Up or Down. The time format is as follows: • Time that is shorter than or equal to 24 hours: hour: minute: second. • Time that is longer than 24 hours but shorter than or equal to one week: day: hour. • Time that is longer than one week: week: day.
AS	The AS number of the MSDP peer. A question mark (?) indicates that the AS number cannot be obtained.
SA Count	Number of (S, G) entries in the SA cache.
Reset Count	Resetting times, including the resetting because the Notification message is received or Holdtimer times out.

8.5.5 display msdp control-message counters

Function

The **display msdp control-message counters** command displays statistics about MSDP messages.

Format

display msdp control-message counters [**peer** *peer-address* | **message-type** { **source-active** | **sa-request** | **sa-response** | **keepalive** | **notification** | **traceroute-request** | **traceroute-reply** | **data-packets** | **unknown-type** }] *

Parameters

Parameter	Description	Value
peer *peer-address*	Specifies IP address of MSDP peer. If **peer** *peer-address* is specified, only statistics about the MSDP messages received, sent, and discarded on a specified MSDP peer are displayed.	The value is in dotted decimal notation.
message-type	Specifies MSDP message types. If **message-type** is specified, only statistics about the MSDP messages received, sent, and discarded of a specified type are displayed.	-
source-active	Displays the statistics about Source-Active messages on the interface.	-
sa-request	Displays the statistics about Source-Active Request messages on the interface.	-
sa-response	Displays the statistics about Source-Active Response messages on the interface.	-
keepalive	Displays the statistics about KeepAlive messages on the interface.	-
notification	Displays the statistics about Notification messages on the interface.	-
traceroute-request	Displays the statistics about Traceroute Request messages on the interface.	-
traceroute-reply	Displays the statistics about Traceroute Reply messages on the interface.	-
data-packets	Displays the statistics about data packets on the interface.	-

Parameter	Description	Value
unknown-type	Displays the statistics about unknown type messages on the interface.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

This command helps you learn MSDP running status by displaying statistics about received, sent, and discarded MSDP messages.

Precautions

This command displays statistics about MSDP messages only when the MSDP peer has been configured.

Example

Display statistics about the MSDP messages that are received, sent, and discarded by the peer 192.168.3.3.

```
<HUAWEI> display msdp control-message counters peer 192.168.3.3
 MSDP message counters for peer: 192.168.3.3
                      Received        Sent            Invalid
 Source-Active          0             0               0
 Source-Active Request  0             0               0
 Source-Active Response 0             0               0
 KeepAlive              48            49              0
 Notification           0             1               0
 Traceroute Request     0             -               -
 Traceroute Reply       0             -               -
 Data Packets           0             0               0
 Unknown Type           1             -               1
```

Table 8-74 Description of the **display msdp control-message counters peer 192.168.3.3** command output

Item	Description
MSDP message counters for peer	IP addresses of MSDP peers.
Received	Number of received messages.
Sent	Number of sent messages.
Invalid	Number of invalid messages.

Item	Description
Source-Active	Source-Active message: carries multiple (S, G) entries and is transmitted among several RPs; encapsulates PIM-SM multicast data.
Source-Active Request	Source-Active Request message: requests (S, G) list of a specified group G to reduce the delay in joining the group.
Source-Active Response	Source-Active Response message: responds to SA request messages.
KeepAlive	Keepalive message: maintains MSDP peer connections. Keepalive packets are sent only when no other protocol packets are exchanged between MSDP peers.
Notification	Notification message.
Traceroute Request	Traceroute Request message: traces and detects the RPF path along which SA messages are transmitted.
Traceroute Reply	Traceroute Reply message: traces and detects the RPF path along which SA messages are transmitted.
Data Packets	Data packets.
Unknown Type	Unknown type message.

8.5.6 display msdp invalid-packet

Function

The **display msdp invalid-packet** command displays statistics about invalid MSDP messages received by a device and details of these messages.

Format

display msdp [**vpn-instance** *vpn-instance-name* | **all-instance**] **invalid-packet** [**peer** *peer-address* | **message-type** { **keepalive** | **notification** | **sa-request** | **sa-response** | **source-active** }] *

display msdp invalid-packet [*packet-number*] **verbose**

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Specifies a VPN instance. *vpn-instance-name* specifies the name of the VPN instance.	The value must be an existing VPN instance name.
all-instance	Displays statistics about invalid MSDP messages received in all VPN instances. If **vpn-instance** or **all-instance** is not specified, only the public network instance is displayed.	-
peer *peer-address*	Displays statistics about invalid MSDP messages received from a specified peer. *peer-address* specifies an MSDP peer address.	The address is in dotted decimal notation.
message-type	Displays statistics about invalid MSDP messages of a specific type.	-
keepalive	Displays statistics about invalid Keepalive messages.	-
notification	Displays statistics about invalid Notification messages.	-
sa-request	Displays statistics about invalid Source-Active Request messages.	-
sa-response	Displays statistics about invalid Source-Active Response messages.	-
source-active	Displays statistics about invalid Source-Active messages.	-
packet-number	Displays details about a specified number of invalid MSDP messages recently received. If this parameter is not specified, details about all invalid MSDP messages.	The value is an integer that ranges from 1 to 100.
verbose	Displays details about invalid MSDP messages.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display msdp invalid-packet** command to view statistics and details of invalid MSDP messages for fault location and rectification.

If MSDP peer relationships fail to be set up on a multicast network, you can run the **display msdp invalid-packet** command first to check whether devices have received invalid MSDP messages. If the command output contains statistics about invalid MSDP messages, run the **display msdp invalid-packet** [*packet-number*] **verbose** command to view details of invalid MSDP messages to locate the fault.

You can run the following related commands to view information about specific invalid MSDP messages:

- Run the **display msdp** [**vpn-instance** *vpn-instance-name* | **all-instance**] **invalid-packet** command to view statistics about invalid MSDP messages received in a specified VPN instance or in all VPN instances.
- Run the **display msdp invalid-packet peer** *peer-address* command to view statistics about invalid MSDP messages received from a specified peer.
- Run the **display msdp invalid-packet** *packet-number* **verbose** command to view details of invalid MSDP messages recently received. Currently, details of a maximum of 100 invalid MSDP messages can be displayed.

Example

Display statistics about invalid MSDP messages received by a device.

```
<HUAWEI> display msdp invalid-packet peer 192.168.1.1

            Statistics of invalid packets for public net:
------------------------------------------------------------------------
MSDP SA invalid packet:
Fault Length           : 0          Bad Length-x           : 0
Bad Sprefix            : 0          Invalid Multicast Group : 0
Invalid Multicast Source: 0         Bad Encap Data         : 0
Illegal RP Addr        : 0          RP Loop                : 0

MSDP SA Response invalid packet:
Fault Length           : 0          Bad Length-x           : 0
Bad Sprefix            : 0          Invalid Multicast Group : 0
Invalid Multicast Source: 0         Illegal RP Addr        : 0
RP Loop                : 0

MSDP SA Request invalid packet:
Fault Length           : 0          Invalid Multicast Group : 0

MSDP Keep Alive invalid packet:
Fault Length           : 0

MSDP Notification invalid packet:
Fault Length           : 0
------------------------------------------------------------------------
```

Table 8-75 Description of the **display msdp invalid-packet peer 192.168.1.1** command output

Item	Description
Statistics of invalid packets for public net	Statistics about invalid MSDP messages in the public network instance.

Item	Description
MSDP SA invalid packet	Invalid Source-Active messages.
Fault Length	Messages with invalid lengths.
Bad Length-x	Messages with invalid Length-x fields.
Bad Sprefix	Messages with invalid Sprefix fields.
Invalid Multicast Group	Messages with invalid multicast group addresses.
Invalid Multicast Source	Messages with invalid multicast source addresses.
Bad Encap Data	Messages with invalid data encapsulated.
Illegal RP Addr	Messages with illegal Rendezvous Point addresses.
RP Loop	Messages whose Rendezvous Point addresses are local addresses.
MSDP SA Response invalid packet	Invalid Source-Active Response messages.
MSDP SA Request invalid packet	Invalid Source-Active Request messages.
MSDP Keep Alive invalid packet	Invalid Keepalive messages.
MSDP Notification invalid packet	Invalid Notification messages.

Display details of a specific invalid MSDP message recently received.

```
<HUAWEI> display msdp invalid-packet 1 verbose
      Detailed information of invalid packets
------------------------------------------------------
Packet information (Index 1):
------------------------------------------------------
Peer              :  10.2.2.2
Time              :  2010-6-9 11:25:46 UTC-08:00
Message Length    :  22
Invalid Type      :  Invalid Addr List
0000: 00 01 00 02 00 69 00 13 00 04 00 00 00 64 00 02
0010: 00 04 81 f4 09 c4
------------------------------------------------------
```

Table 8-76 Description of the **display msdp invalid-packet 1 verbose** command output

Item	Description
Detailed information of invalid packets	Details about invalid MSDP messages.

Item	Description
Packet information (Index 1)	Sequence number of the invalid MSDP message (numbered in the opposite order that the message is received, for example, the index of the last received message is 1, the index of the last but one message is 2, and so on).
Peer	IP address of the peer that sends the invalid MSDP message.
Time	Time when the invalid MSDP message is received, in any of the following formats: ● YYYY-MM-DD HH:MM:SS ● YYYY-MM-DD HH:MM:SS UTC±HH:MM DST ● YYYY-MM-DD HH:MM:SS UTC±HH:MM ● YYYY-MM-DD HH:MM:SS DST UTC±HH:MM indicates that a time zone is configured through the **clock timezone** command; DST indicates that the daylight saving time is configured through **clock daylight-saving-time** command.
Message Length	Length of the invalid MSDP message.
Invalid Type	Type of the invalid MSDP message.
0000: 00 01 00 02 00 69 00 13 00 04 00 00 00 64 00 02 0010: 00 04 81 f4 09 c4	Contents of the invalid MSDP message.

8.5.7 display msdp peer-status

Function

The **display msdp peer-status** command displays the detailed information about MSDP peers.

Format

display msdp [**vpn-instance** *vpn-instance-name* | **all-instance**] **peer-status** [*peer-address*]

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Specifies a VPN instance. *vpn-instance-name* specifies the name of the VPN instance.	The value must be an existing VPN instance name.
all-instance	Indicates all the instances. If **vpn-instance** or **all-instance** is not specified, only the public network instance is displayed.	-
peer-address	Specifies the address of a remote MSDP peer. If this parameter is not specified, information about all the MSDP peers in the instance is displayed.	The address is in dotted decimal notation.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

After MSDP peers establish a TCP connection, the **display msdp peer-status** command can be used to display the detailed information about a specified MSDP peer, such as the interface status, interface configuration, policy for filtering messages, and number of messages.

Precautions

This command displays the detailed information about a specified MSDP peer only when the MSDP peer has been configured.

Example

Display the detailed information about the MSDP peer 10.110.11.11.

```
<HUAWEI> display msdp peer-status 10.110.11.11
  MSDP Peer 10.110.11.11, AS 100
  Description:
  Information about connection status:
    State: Up
    Up/down time: 14:41:08
    Resets: 0
    Connection interface: LoopBack0 (10.110.11.22)
    Number of sent/received messages: 867/947
    Number of discarded output messages: 0
    Elapsed time since last connection or counters clear: 14:42:40
```



```
Information about (Source, Group)-based SA filtering policy:
  Import policy: none
  Export policy: none
  Local Export policy: none
Information about SA-Requests:
  Policy to accept SA-Request messages: none
  Sending SA-Requests status: disable
Minimum TTL to forward SA with encapsulated data: 0
SAs learned from this peer: 0, SA-cache maximum for the peer: none
Input queue size: 0, Output queue size: 0
Counters for MSDP message:
  Count of RPF check failure: 0
  Incoming/outgoing SA messages: 0/0
  Incoming/outgoing SA requests: 0/0
  Incoming/outgoing SA responses: 0/0
  Incoming/outgoing data packets: 0/0
Peer authentication: unconfigured
Peer authentication type: none
```

Table 8-77 Description of the **display msdp peer-status** command output

Item	Description
MSDP Peer	Address of the peer. This parameter is configured using the **peer connect-interface (MSDP)** command.
AS	AS number of the MSDP peer. A question mark (?) indicates that the AS number cannot be obtained.
Description	Description of the verbose information.
Information about connection status	Information of connection status.
State	Status of the MSDP session. • Up: The connection is set up and is in the Up state. • Listen: The local device acts as the server. The connection is not set up. • Connect: The local device acts as the client. The connection is not set up. • Shutdown: The MSDP peer is in Shutdown state. • Down: The connection fails.
Up/down time	Time when the session becomes Up or Down. The time format is as follows: • Time that is shorter than or equal to 24 hours: hour: minute: second. • Time that is longer than 24 hours but shorter than or equal to one week: day: hour. • Time that is longer than one week: week: day.
Resets	Resetting times.

Item	Description
Connection interface	Address of a connect-interface that is used to set up the TCP connection with the peer address. This parameter is configured using the **peer connect-interface (MSDP)** command.
Number of sent/ received messages	Number of MSDP messages received or sent through the connection.
Number of discarded output messages	Number of discarded messages.
Elapsed time since last connection or counters clear	Time that elapsed since the MSDP peer resetting count and control packet statistics were reset.
Information about (Source, Group)-based SA filtering policy	• Import policy: is used to receive the filtering list of the SA messages of a specified MSDP peer. You can configure the policy using the **peer sa-policy import** command. • Export policy: is used to forward the filtering list of the SA messages of a specified MSDP peer. You can configure the policy using the **peer sa-policy export** command. • Local Export policy: is used to send the policy of locally created SA messages tof a specified MSDP peer. You can configure the policy using the **peer sa-policy local-export** command. By default, a device accepts all SA messages from MSDP peers, sends all locally created SA messages to MSDP peers, and forwards all SA messages to MSDP peers.
Information about SA-Requests	• Policy to accept SA-Request messages: restricts the SA request messages received from an MSDP peer by the switch. By default, the switch receives all the SA Request messages sent by the MSDP peer. The item is expressed by none. You can set the policy using the **peer sa-request-policy** command. • Sending SA-Requests status: enables or disables the switch to send SA request messages to a specified MSDP peer when the switch receives a Join message. By default, when receiving a Join message, the switch does not send the SA Request message to its MSDP peers, but waits for the next SA message. You can configure the switch to send SA Request messages using the **peer request-sa-enable** command.

Item	Description
Minimum TTL to forward SA with encapsulated data	If the SA message received is encapsulated with the multicast data packet, the switch forwards the SA message to other peers only when the TTL of the packet is not smaller than the minimum TTL. You can configure the function using the **peer minimum-ttl** command.
SAs learned from this peer	SA messages that pass through the MSDP peer and the number of SA entries in the cache.
SA-cache maximum for the peer	Maximum number of (S, G) entries in the cache when the switch receives the SA message from an MSDP peer. You can configure the maximum number of (S, G) entries in the cache using the **peer sa-cache-maximum** command.
Input queue size	Length of the data in the input cache.
Output queue size	Length of the data in the output cache.
Counters for MSDP message	Number of MSDP messages. ● Count of RPF check failure: indicates the number of SA messages discarded because of the RPF check failure. ● Incoming/outgoing SA messages: indicates the number of sent or received SA messages. ● Incoming/outgoing SA requests: indicates the number of sent or received SA-Request messages. ● Incoming/outgoing SA responses: indicates the number of sent or received SA-Response messages. ● Incoming/outgoing data packets: indicates the number of sent or received SA messages that are encapsulated with multicast data packets.
Peer authentication	Whether MSDP authentication is configured.
Peer authentication type	MSDP authentication modes, including: ● none: indicates authentication is not configured. ● MD5: indicates MD5 authentication. This parameter is configured using the **peer password (MSDP)** command. ● Keychain: indicates Keychain authentication. This parameter is configured using the **peer keychain (MSDP)** command.

8.5.8 display msdp rpf-peer

Function

The **display msdp rpf-peer** command displays information about all RPF peers of a specific source RP address, including RPF peer selection rules and RPF route types.

Format

display msdp [**vpn-instance** *vpn-instance-name* | **all-instance**] **rpf-peer original-rp** *original-rp-address*

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Specifies a VPN instance. *vpn-instance-name* specifies the name of the VPN instance.	The value must be an existing VPN instance name.
all-instance	Displays information about all the RPF peers of a specific source's RP address in all instances. If **vpn-instance** or **all-instance** is not specified, only the public network instance is displayed.	-
original-rp *original-rp-address*	Displays information about all the RPF peers of a specific source's RP address. *original-rp-address* specifies the source's RP address.	The value is in dotted decimal notation.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

To prevent looping of SA messages between MSDP peers, MSDP peers perform RPF checks on received SA messages and drop the SA messages that do not comply with RPF rules.

The **display msdp rpf-peer** command is used to check whether the forwarding path of SA messages works properly. Based on the RPF peer information in the command output, you can check every hop in the forwarding path. If the forwarding path is not working properly, this command helps you locate the faulty node.

Precautions

A device does not perform RPF checks on the SA messages received from an MSDP peer in the following situations:

- The address of the MSDP peer is the RP address of the source.
- The MSDP peer is a static RPF peer of the device.
- The MSDP peer is a unique MSDP peer of the device.
- The MSDP peer has joined a full-mesh group.

Before configuring this command, ensure that MSDP peers are configured. Only the MSDP peers with Up TCP connection can become RPF peers.

Example

Display information about RPF peers of the source RP 192.168.4.5.

```
<HUAWEI> display msdp rpf-peer original-rp 192.168.4.5
MSDP RPF peer information
 MSDP RPF peer information for Original RP: 192.168.4.5
 01. RPF peer: 10.6.6.6
  RPF selection rule: Peer is IGP next hop of best route
  RPF used topology: default
  RPF route type: multicast(static)
```

Table 8-78 Description of the **display msdp rpf-peer original-rp** command output

Item	Description
MSDP RPF peer information	information about the MSDP RPF peer.
MSDP RPF peer information for Original RP	Information about the MSDP RPF peer of a specific source's RP address.
01. RPF peer	RPF peer address.

Item	Description
RPF selection rule	RPF peer selection rule: • Peer is IGP next hop of best route: RPF peer is a next hop of an IGP route. • Peer is IGP advertiser of best route: RPF peer is a forwarder of an IGP route. • Peer is in the AS-path to original RP: RPF peer is on an AS-path to the RP address of the source. • Peer is BGP/MBGP next hop of best route: RPF peer is a next hop of a/an BGP/MBGP route. • Peer is BGP/MBGP advertiser of best route: RPF peer is a forwarder of a/an BGP/MBGP route.
RPF used topology	RPF used topology: • default: default topology. • multicast: multicast topology. • topology name (user-defined): unicast topology.
RPF route type	RPF route type: • mbgp: MBGP route. • unicast(bgp): BGP route • multicast(static): static multicast route. • unicast: IGP route (unicast route).

8.5.9 display msdp sa-cache

Function

The **display msdp sa-cache** command displays (S, G) entries in the SA cache.

Format

display msdp [**vpn-instance** *vpn-instance-name* | **all-instance**] **sa-cache** [*group-address* | *source-address* | [*as-number-plain* | *as-number-dot*]] *

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Specifies a VPN instance. *vpn-instance-name* specifies the name of the VPN instance.	The value must be an existing VPN instance name.
all-instance	Indicates all the instances. If **vpn-instance** or **all-instance** is not specified, only statistics about the public network instance is displayed.	-
group-address	Specifies the group address of an (S, G) entry. It is used to display the corresponding (S, G) of the group in SA Cache.	The value is in dotted decimal notation and ranges from 224.0.1.0 to 239.255.255.255.
source-address	Specifies the source address of an (S, G) entry. It is used to display the corresponding the (S, G) of the source.	The value is in dotted decimal notation.
as-number-plain	Specifies the number of the AS, in integer format.	The value is an integer that ranges from 1 to 4294967295.
as-number-dot	Specifies the number of the AS, in dotted notation.	The value is in the x.y format. Here, "x" and "y" are integers that range from 1 to 65535 and 0 to 65535 respectively.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

If the SA cache function is enabled, the **display msdp sa-cache** command can be used to display the information about (S, G) entries learned from other MSDP peers in the SA cache. The information includes the source address, group address, address of the source's RP, routing protocol, AS number, and timeout period of entries.

Precautions

This command displays (S, G) entries in the SA cache only when SA cache is enabled (default setting).

Example

Display (S, G) entries in the SA cache.

```
<HUAWEI> display msdp sa-cache
MSDP Source-Active Cache Information
 MSDP Total Source-Active Cache - 2 entries
 MSDP matched 2 entries

(10.0.5.120, 225.0.0.1)
 Origin RP: 3.3.3.3
 Pro: ?, AS: ?
 Uptime: 00:01:01, Expires: 00:05:59

(10.0.5.120, 225.0.0.2)
 Origin RP: 3.3.3.3
 Pro: ?, AS: ?
 Uptime: 00:00:01, Expires: 00:05:59
```

Table 8-79 Description of the **display msdp sa-cache** command output

Item	Description
MSDP Source-Active Cache Information	MSDP SA cache.
MSDP Total Source-Active Cache - 2 entries	Two entries are cached by MSDP SA.
MSDP matched 2 entries	Two entries are matched by MSDP, such as the filtering policy and specified source/group address.
(10.0.5.120, 225.0.0.1)	(source address, group address) entry in the SA cache.
Origin RP	Source RP address that advertises the (S, G) entry.
Pro	Type of the protocol from which the AS number of the source RP is obtained. A question mark (?) indicates the protocol type if the AS number of the source RP cannot be obtained.
AS	AS number of the source RP. A question mark (?) indicates the protocol type if the AS number of the source RP cannot be obtained.
Uptime	Time when the (S, G) entry is created in the cache.

Item	Description
Expires	Time when the (S, G) entry in the cache times out.

8.5.10 display msdp sa-count

Function

The **display msdp sa-count** command displays statistics about the (S, G) entries in the SA cache.

Format

display msdp [**vpn-instance** *vpn-instance-name* | **all-instance**] **sa-count** [*as-number-plain* | *as-number-dot*]

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Specifies a VPN instance. *vpn-instance-name* specifies the name of the VPN instance.	The value must be an existing VPN instance name.
all-instance	Indicates all the instances. If **vpn-instance** or **all-instance** is not specified, only statistics about the public network instance is displayed.	-
as-number-plain	Specifies the number of the AS, in integer format.	The value is an integer that ranges from 1 to 4294967295.
as-number-dot	Specifies the number of the AS, in dotted notation.	The value is in the x.y format. Here, "x" and "y" are integers that range from 1 to 65535 and 0 to 65535 respectively.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

If the SA cache function is enabled, the **display msdp sa-count** command can be used to display the statistics about the (S, G) entries in the SA cache, including the addresses of the peers that send SA messages and the (S, G) entry statistics collected according to the AS numbers of sources' RPs.

Precautions

This command displays the number of (S, G) entries in the SA cache only when the MSDP peer has been enabled with SA cache (default setting).

Example

Display the number of (S, G) entries in the SA cache.

```
<HUAWEI> display msdp sa-count
MSDP Source-Active Count Information
  Number of cached Source-Active entries, counted by Peer
  Peer's Address     Number of SA
  10.10.10.10        5

  Number of source and group, counted by AS
  AS     Number of source    Number of group
  ?      3                   3

  Total 5 Source-Active entries matched
```

Table 8-80 Description of the **display msdp sa-count** command output

Item	Description
MSDP Source-Active Count Information	Number of MSDP SA messages.
Number of cached Source-Active entries, counted by Peer	Number of the (S, G) entries that are cached according to peers.
Peer's Address	Address of the peer that sends the SA message.
Number of SA	Number of the (S, G) entries received from the peer.
Number of source and group, counted by AS	Number of the (S, G) entries that is counted according to the AS to which the source RP belongs.
AS	AS number of the source RP. A question mark (?) indicates the protocol type if the AS number of the source RP cannot be obtained.

Item	Description
Number of source	Number of sources in the AS. **NOTE** If **0** is displayed in the **Number of source** and **Number of group** fields, the local device does not receive SA messages from its MSDP peer. Contact technical support personnel to troubleshoot faults.
Number of group	Number of groups in the AS.
Total 5 Source-Active entries matched	Number of (S, G) entries matching specified conditions in the cache.

8.5.11 encap-data-enable

Function

The **encap-data-enable** command enables the device to encapsulate a multicast data packet into an SA message.

The **undo encap-data-enable** command disables the device from encapsulating a multicast data packet into an SA message.

By default, no multicast data packet is encapsulated into an SA message.

Format

encap-data-enable

undo encap-data-enable

Parameters

None

Views

MSDP view of the public network instance or MSDP view of the VPN instance

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The source RP encapsulates information about all active sources into multiple SA messages to advertise it. Each SA message contains multiple (S, G) entries.

After the **encap-data-enable** command is configured on the source's RP, the RP encapsulates the multicast data carried in the Register message into an SA

message, and then sends the SA message to the MSDP peer. Only one multicast data packet can be encapsulated into an SA message.

After the **encap-data-enable** command is configured on the MSDP peer, the switch can transmit the SA messages carrying a multicast data packet between PIM-SM domains.

Prerequisites

MSDP has been enabled using the **msdp** command.

Example

Encapsulate a multicast data packet into an SA message

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] msdp
[HUAWEI-msdp] encap-data-enable
```

8.5.12 import-source

Function

The **import-source** command prevents the information about active sources in a domain from being advertised when an SA message is created.

The **undo import-source** command restores the default configuration.

By default, the information about all active sources is advertised in a domain through SA messages.

Format

import-source [**acl** *acl-number*]

undo import-source

Parameters

Parameter	Description	Value
acl	Indicates the ACL that controls which source is to be advertised to a domain through an SA message and to which groups the SA message is to be advertised. If this parameter is not specified, multicast sources are not advertised.	-
acl-number	Specifies the number of the basic ACL or advanced ACL. • Basic ACL: filters source addresses. • Advanced ACL: filters source addresses and multicast group addresses.	The value is an integer that ranges from 2000 to 3999.

Views

MSDP view of the public network instance or MSDP view of the VPN instance

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the **import-source** command is used to filter (S, G) forwarding entries to be advertised in SA messages based on source addresses. This configuration controls transmission of information about multicast sources.

You can also run the **peer sa-policy** command to filter the SA messages to be forwarded.

The **import-source** command takes effect for all peers. If both the **import-source** and **peer** *peer-address* **sa-policy local-export** commands are run, the parameters configured in the **peer** *peer-address* **sa-policy local-export** command take effect preferentially.

Prerequisites

MSDP has been enabled using the **msdp** command.

Precautions

The **import-source** and **acl** commands are used together.

- In the basic ACL view, set the source address range of advertised multicast packets using SA messages by specifying the **source** parameter in the **rule** command.
- In the advanced ACL view, set the source address range of advertised multicast packets using SA messages by specifying the **source** parameter in the **rule** command, and set the address range of advertised multicast groups using SA messages by specifying the **destination** parameter in the **rule** command.

Example

Configure an MSDP peer to advertise the information about a specified active source when creating SA messages. The multicast source is on 10.10.0.0/16 network segment, and the multicast group address is 225.1.0.0/16.

```
<HUAWEI> system-view
[HUAWEI] acl number 3101
[HUAWEI-acl-adv-3101] rule permit ip source 10.10.0.0 0.0.255.255 destination 225.1.0.0 0.0.255.255
[HUAWEI-acl-adv-3101] quit
[HUAWEI] multicast routing-enable
[HUAWEI] msdp
[HUAWEI-msdp] import-source acl 3101
```


8.5.13 msdp

Function

The **msdp** command enables MSDP and displays the MSDP view in the public network instance or the VPN instance.

The **undo msdp** command clears all configurations in the MSDP view, releases the resources occupied by MSDP, and restores the initial state.

By default, MSDP is disabled.

Format

msdp [**vpn-instance** *vpn-instance-name*]

undo msdp [**vpn-instance** *vpn-instance-name*]

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Specifies a VPN instance. *vpn-instance-name* specifies the name of the VPN instance.	The value must be an existing VPN instance name.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To configure MSDP, you can run the **msdp** command to enable MSDP and display the MSDP view. All the configurations related to MSDP peers must be done in the MSDP view.

Prerequisites

The multicast routing function has been enabled using the **multicast routing-enable** command.

Configuration Impact

Running the **undo msdp** command interrupts MSDP services. Therefore, use this command with caution.

Example

Enable MSDP and enter the MSDP view.


```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] msdp
[HUAWEI-msdp]
```

8.5.14 originating-rp

Function

The **originating-rp** command configures an RP to replace the source RP address in the SA message with an IP address of a specified interface when the RP constructs an SA message. This interface is also called a logical RP.

The **undo originating-rp** command restores the default configuration.

By default, the source RP address in an SA message is the address of the RP that actually sends the SA message.

Format

originating-rp *interface-type interface-number*

undo originating-rp

Parameters

Parameter	Description	Value
interface-type interface-number	Specifies the type and number of the interface that functions as a logical RP.	-

Views

MSDP view of the public network instance or MSDP view of the VPN instance

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You must run this command when configuring anycast RP in a PIM-SM domain.

An MSDP peer performs the RPF check on a received SA message and then discards the message if the addresses of the local RP and the remote RP are the same. In anycast RP, however, you need to configure RPs on two or more devices in a PIM-SM domain, assign the same IP address to these RPs, and set up MSDP peer relationships between these devices. You must configure an address that is different from the actual RP address for the logical RP so that the SA message can pass the RPF check.

Prerequisites

MSDP has been enabled using the **msdp** command.

Precautions

The interface functioning as a logical RP cannot be an actual RP interface. Commonly, the interfaces setting up an MSDP peer relationship can be specified as logical RP addresses.

Example

Configure VLANIF100 as the logical RP for the SA message.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] msdp
[HUAWEI-msdp] originating-rp vlanif 100
```

8.5.15 peer connect-interface (MSDP)

Function

The **peer connect-interface** command configures an MSDP peer.

The **undo peer** command removes the configured MSDP peer.

By default, no MSDP peer is configured.

Format

peer *peer-address* **connect-interface** *interface-type interface-number*

undo peer *peer-address*

Parameters

Parameter	Description	Value
peer-address	Specifies the address of a remote MSDP peer.	The address is in dotted decimal notation.
interface-type interface-number	Specifies the type and the number of the interface. The local switch uses the primary address of the interface as the source IP address to set up the TCP connection with the remote MSDP peer.	-

Views

MSDP view of the public network instance or MSDP view of the VPN instance

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

MSDP peers are identified by addresses. You can run the **peer connect-interface** command on two devices to specify the peer addresses for each other and specify interfaces for establishing the TCP connection. In this way, an MSDP peer connection is established.

Prerequisites

MSDP has been enabled using the **msdp** command.

Configuration Impact

You can run the **peer** *peer-address* **connect-interface** *interface-type interface-number* command repeatedly to configure multiple MSDP peers for the local switch.

- You can specify the same *interface-type interface-number* for different *peer-address*. That is, you can specify the same local interface for different remote peers.
- You can specify different *interface-type interface-number* for different *peer-address*. That is, you can specify different local interfaces for different remote peers.

Precautions

Run the **peer connect-interface** command before running other peer commands. Otherwise, the system displays a message indicating that the peer does not exist.

When configuring a static RPF peer, you need to first run the **peer connect-interface** command to set the remote end as an MSDP peer and then the **static-rpf-peer** command to set the MSDP peer as a static RPF peer.

Example

Configure IP address 10.10.7.6 for the remote MSDP peer and specify VLANIF100 as the local interface.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] msdp
[HUAWEI-msdp] peer 10.10.7.6 connect-interface vlanif 100
```

8.5.16 peer description (MSDP)

Function

The **peer description** command adds the description text for an MSDP peer.

The **undo peer description** command restores the default configuration.

By default, an MSDP peer does not have the description text.

Format

peer *peer-address* **description** *text*

undo peer *peer-address* **description**

Parameters

Parameter	Description	Value
peer-address	Specifies the address of an MSDP peer.	The address is in dotted decimal notation.
text	Specifies the description text.	The description text is a string of 1 to 80 case-sensitive characters.

Views

MSDP view of the public network instance or MSDP view of the VPN instance

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If multiple MSDP peers are configured on the network, the MSDP peers cannot be easily distinguished only by IP addresses. The administrator can distinguish the MSDP peers by setting the descriptions for them.

Prerequisites

MSDP peers have been configured using the **peer connect-interface (MSDP)** command.

Example

Add a description **ClientA** for the MSDP peer with the IP address being 10.10.7.6.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] msdp
[HUAWEI-msdp] peer 10.10.7.6 connect-interface vlanif 100
[HUAWEI-msdp] peer 10.10.7.6 description ClientA
```

8.5.17 peer keychain (MSDP)

Function

The **peer keychain** command configures keychain authentication for establishing a TCP connection between MSDP peers and transmitting MSDP message.

The **undo peer keychain** command removes keychain authentication between MSDP peers.

By default, MSDP keychain authentication is not configured.

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Format

peer *peer-address* **keychain** *keychain-name*

undo peer *peer-address* **keychain**

Parameters

Parameter	Description	Value
peer-address	Specifies the address of an MSDP peer.	The value is in dotted decimal notation.
keychain-name	Specifies the name of the keychain. This parameter is set using the **keychain** command.	The value is a string of 1 to 47 case-insensitive characters. Except the question mark (?) and space. However, when double quotation marks (") are used around the string, spaces are allowed in the string.

Views

MSDP view of the public network instance or MSDP view of the VPN instance

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

MSDP supports MD5 authentication and keychain authentication that improve security on TCP connections between MSDP peers. Keychain authentication supports multiple algorithms and is more suitable than MD5 authentication for networks that require high security.

Prerequisites

MSDP peers have been configured using the **peer connect-interface (MSDP)** command.

A keychain in accordance with the configured *keychain-name* has been enabled using the **keychain** command; otherwise, the TCP connection cannot be set up.

Precautions

You must configure keychain authentication on both MSDP peers. Note that encryption algorithms and passwords configured for keychain authentication on

both peers must be the same; otherwise, the TCP connection cannot be set up between MSDP peers and MSDP messages cannot be transmitted.

MSDP MD5 authentication and MSDP keychain authentication are mutually exclusive.

Example

Configure MSDP keychain authentication between the local switch and the peer 10.1.1.2 and configure a keychain named **test**.

```
<HUAWEI> system-view
[HUAWEI] keychain test mode absolute
[HUAWEI-keychain-test] key-id 1
[HUAWEI-keychain-test-keyid-1] algorithm sha-256
[HUAWEI-keychain-test-keyid-1] key-string cipher Test@1234
[HUAWEI-keychain-test-keyid-1] quit
[HUAWEI-keychain-test] quit
[HUAWEI] multicast routing-enable
[HUAWEI] msdp
[HUAWEI-msdp] peer 10.1.1.2 connect-interface vlanif 100
[HUAWEI-msdp] peer 10.1.1.2 keychain test
```

8.5.18 peer mesh-group

Function

The **peer mesh-group** command adds an MSDP peer to a mesh group.

The **undo peer mesh-group** command restores the default configuration.

By default, an MSDP peer does not belong to any mesh group.

Format

peer *peer-address* **mesh-group** *name*

undo peer *peer-address* **mesh-group**

Parameters

Parameter	Description	Value
peer-address	Specifies the address of an MSDP peer that is to be a member of a mesh group.	The address is in dotted decimal notation.
name	Specifies the name of a mesh group.	The name is a string of 1 to 32 case-sensitive characters.

Views

MSDP view of the public network instance or MSDP view of the VPN instance

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If multiple MSDP peers exist on a network, SA messages may be flooded between peers. Especially when many MSDP peers are configured in the same PIM-SM domain, RPF rules cannot filter out useless SA messages effectively. The MSDP peer needs to perform an RPF check on each SA message received, which brings a heavy load to the system.

Configuring multiple MSDP peers to join the same mesh group can reduce the number of SA messages transmitted between these MSDP peers and reduce the load on the system.

Prerequisites

The device has established MSDP peer relationships with current mesh group members using the **peer connect-interface** command.

Configuration Impact

One MSDP peer can join only one mesh group. If an MSDP peer is added to different mesh groups several times, the latest configuration takes effect.

When a member of the mesh group receives an SA message, it checks the source of the SA message:

- If the SA message is sent by a certain MSDP peer outside the mesh group, the member performs the RPF check on the SA message. If the SA message passes the check, the member forwards it to other members of the mesh group.
- If the SA message is sent by a member of the mesh group, the member directly accepts the message without performing the RPF check. In addition, it does not forward the message to other members in the mesh group.

Precautions

The MSDP peer relationships must be established between the peers in a mesh group.

Commonly, the MSDP peers in the same AS join the same mesh group and EBGP routes need be configured between inter-AS MSDP peers.

Example

Add the MSDP peer with the address of 10.10.7.6 to the mesh group **Group1**

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] msdp
[HUAWEI-msdp] peer 10.10.7.6 connect-interface vlanif 100
[HUAWEI-msdp] peer 10.10.7.6 mesh-group Group1
```


8.5.19 peer minimum-ttl

Function

The **peer minimum-ttl** command sets a TTL threshold for the multicast data packet that can be encapsulated in an SA message and forwarded to a specified MSDP peer.

The **undo peer minimum-ttl** command restores the default value.

By default, the TTL threshold is 0.

Format

peer *peer-address* **minimum-ttl** *ttl*

undo peer *peer-address* **minimum-ttl**

Parameters

Parameter	Description	Value
peer-address	Specifies the address of an MSDP peer.	The address is in dotted decimal notation.
ttl	Specifies the TTL threshold.	The value is an integer that ranges from 0 to 255.

Views

MSDP view of the public network instance or MSDP view of the VPN instance

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

MSDP peers transmit SA messages to each other over an established TCP connection. The **peer minimum-ttl** command limits the forwarding of SA messages with multicast data packets encapsulated.

After the TTL threshold is set for a specified peer, the switch checks the TTL values of multicast data packets before encapsulating them in SA messages. Only the multicast data packets with a TTL value greater than the threshold are encapsulated in an SA message and sent to the peer.

Prerequisites

MSDP peers have been configured using the **peer connect-interface (MSDP)** command.

Example

Set the TTL threshold to 10. Only the multicast data packet with the TTL value being greater than 10 is encapsulated in the SA message and forwarded to MSDP peer 10.10.10.1.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] msdp
[HUAWEI-msdp] peer 10.10.10.1 connect-interface vlanif 100
[HUAWEI-msdp] peer 10.10.10.1 minimum-ttl 10
```

8.5.20 peer password (MSDP)

Function

The **peer password** command configures MD5 authentication for establishing a TCP connection between MSDP peers.

The **undo peer password** command removes the MD5 authentication between MSDP peers.

By default, the MSDP MD5 authentication is not configured.

Format

peer *peer-address* **password** { **cipher** *cipher-password* | **simple** *simple-password* }

undo peer *peer-address* **password**

Parameters

Parameter	Description	Value
peer-address	Specifies the address of an MSDP peer.	The address is in dotted decimal notation.
cipher *cipher-password*	Specifies the password in the cipher text.	The value is a string of case sensitive characters without any space. A cipher password may contain 1 to 255 plain characters or 20 to 392 encrypted characters. When double quotation marks are used around the string, spaces are allowed in the string.

Parameter	Description	Value
simple *simple-password*	Specifies the password in the plain text. **NOTICE** If **simple** is selected, the password is saved in the configuration file in plain text. This brings high security risks. It is recommended that you select **cipher** to save the password in cipher text. To improve the device security, change the password periodically.	The value is a string of 1 to 255 case-sensitive characters without spaces. When double quotation marks are used around the string, spaces are allowed in the string.

Views

MSDP view of the public network instance or MSDP view of the VPN instance

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

MSDP supports MD5 authentication and keychain authentication that improves security on TCP connections between MSDP peers.

Prerequisites

MSDP peers have been configured using the **peer connect-interface (MSDP)** command.

Precautions

MD5 is not a secure authentication algorithm. For security purposes, you are advised to use the more secure Keychain algorithm for MSDP authentication.

MSDP peers must be configured with the same authentication password; otherwise, the TCP connections cannot be set up between MSDP peers and MSDP messages cannot be transmitted. The authentication password on peers can be in different formats, for example, the password on one end can be in the cipher text while the password on the peer can be in the plain text.

MSDP MD5 authentication and MSDP keychain authentication are mutually exclusive.

Example

Configure MSDP MD5 authentication between the local switch and the peer 10.1.1.1 and set the authentication password to **Test@1234** in the cipher text.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
```



```
[HUAWEI] msdp
[HUAWEI-msdp] peer 10.1.1.1 connect-interface vlanif 100
[HUAWEI-msdp] peer 10.1.1.1 password cipher Test@1234
```

8.5.21 peer request-sa-enable

Function

The **peer request-sa-enable** command enables the function of immediately sending the SA Request message to a specified MSDP peer.

The **undo peer request-sa-enable** command restores the default configuration.

By default, when receiving a new Join message for a group, the switch does not send an SA Request message to MSDP peer but waits to receive the next SA message.

Format

peer *peer-address* **request-sa-enable**

undo peer *peer-address* **request-sa-enable**

Parameters

Parameter	Description	Value
peer-address	Specifies the address of an MSDP peer.	The address is in dotted decimal notation.

Views

MSDP view of the public network instance or MSDP view of the VPN instance

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When a new user joins multicast group G in a PIM-SM domain, a (*, G) entry is created on the RP. If no corresponding (S, G) information exists on the RP and SA cache is not enabled on the RP, multicast routes cannot be generated for this user. The RP then must wait for the next SA message from the remote MSDP peer to obtain valid (S, G) information.

Generally, the interval for an MSDP peer to send SA messages is set to a large value to reduce traffic load in the PIM-SM domain. This, however, will cause a delay in joining the source's SPT. To minimize the delay, enable the function of immediately sending SA Request messages on the local RP and enable the SA cache function on the remote MSDP peer. If a new Join message is received but the local entries and SA cache do not contain corresponding (S, G) information,

the local RP immediately sends an SA Request message to the remote MSDP peer instead of waiting to receive the next SA message.

Prerequisites

MSDP peers have been configured using the **peer connect-interface (MSDP)** command.

Precautions

Before configuring the **peer request-sa-enable** command on the local switch, disable SA cache on the local switch and enable SA cache on the peer of the specified *peer-address*. Therefore, when the local switch has new receiving requests, it can actively send SA Request messages to the peer and receive responses from the peer.

Example

Configure the switch to send SA Request messages to the MSDP peer 10.10.7.6 when receiving a new Join message.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] msdp
[HUAWEI-msdp] peer 10.10.7.6 connect-interface vlanif 100
[HUAWEI-msdp] peer 10.10.7.6 request-sa-enable
```

8.5.22 peer sa-cache-maximum

Function

The **peer sa-cache-maximum** command limits the maximum number of (S, G) entries that are learnt from MSDP peers and cached by the SA cache.

The **undo peer sa-cache-maximum** command restores the maximum number of (S, G) entries that are learnt from MSDP peers and cached by the SA cache to the default configuration.

By default, the maximum number of (S, G) entries in the SA cache is 8192.

Format

peer *peer-address* **sa-cache-maximum** *sa-limit*

undo peer *peer-address* **sa-cache-maximum**

Parameters

Parameter	Description	Value
peer-address	Specifies the address of an MSDP peer.	The address is in dotted decimal notation.

Parameter	Description	Value
sa-limit	Specifies the maximum number of (S, G) entries that are allowed to cache.	The number is an integer that ranges from 1 to 4294967295.

Views

MSDP view of the public network instance or MSDP view of the VPN instance

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You are recommended to perform this configuration on all MSDP peers on the network vulnerable to DoS attacks.

Prerequisites

MSDP peers have been configured using the **peer connect-interface (MSDP)** command.

Configuration Impact

The total number of (S, G) entries that can be stored in SA-Cache is limited by the specification of the SA-Cache. At present, for an entire switch, the maximum number of (S, G) entries in SA-Cache is 8192.

For the (S, G) entries of a single peer:

- If the number of (S, G) entries is not set or exceeds 8192, the maximum number of (S, G) entries in the SA cache can be set to 8192.
- If the number of (S, G) entries is smaller than 8192, the maximum number of (S, G) entries in the SA cache is the configured value. The redundant (S, G) entries are not cached or advertised to PIM-SM but can be forwarded through SA messages.

Example

Set the maximum number of (S, G) entries that are learnt from MSDP peers and cached by the SA cache to 100 when the switch receives an SA message from MSDP peer 10.10.7.6.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] msdp
[HUAWEI-msdp] peer 10.10.7.6 connect-interface vlanif 100
[HUAWEI-msdp] cache-sa-enable
[HUAWEI-msdp] peer 10.10.7.6 sa-cache-maximum 100
```


8.5.23 peer sa-policy

Function

The **peer sa-policy** command sets a filtering policy for SA messages received or forwarded.

The **undo peer sa-policy** command restores the default configuration.

By default, a device accepts all SA messages from MSDP peers, sends all locally created SA messages to MSDP peers, and forwards all SA messages to MSDP peers.

Format

peer *peer-address* **sa-policy** { **import** | **export** | **local-export** } [**acl** *advanced-acl-number*]

undo peer *peer-address* **sa-policy** { **import** | **export** | **local-export** }

Parameters

Parameter	Description	Value
peer-address	Specifies the address of a remote MSDP peer.	The address is in dotted decimal notation.
import	Receives the SA messages from a specified MSDP peer.	-
export	Forwards the SA messages to a specified MSDP peer.	-
local-export	Indicates that the locally created SA messages to be sent to the specified peer are filtered.	-
acl	Indicates the ACL that defines the import or export policy.	-
advanced-acl-number	Specifies the number of the advanced ACL.	The number is an integer that ranges from 3000 to 3999.

Views

MSDP view of the public network instance or MSDP view of the VPN instance

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the **peer sa-policy** command is configured, MSDP can filter (S, G) forwarding entries carried in the SA message received from or forwarded to specified MSDP peers based on multicast source addresses, to control transmission of multicast source information.

- After the **peer** *peer-address* **sa-policy import** command is run, when an SA message reaches the local device from the specified peer, the local device filters the message using the import policy to determine whether to process the SA message.
  - If **acl** parameter is not configured, the device does not receive SA messages from any MSDP peer.
  - If **acl** parameter is configured, the device receives SA messages that carry the (S, G) entry only from a specified MSDP peer.
- After the **peer** *peer-address* **sa-policy export** command is run, the device filters an SA message using the export policy to determine whether to forward the SA message.
  - If **acl** parameter is not configured, the device does not forward SA messages from any MSDP peer.
  - If **acl** parameter is configured, the device forwards SA messages that carry the (S, G) entry only to a specified MSDP peer.
- After the **peer** *peer-address* **sa-policy local-export** command is run, the device filters the locally created SA messages to be sent to the peer specified by *peer-address*.
  - If **acl** parameter is not configured, no locally created SA messages that match the specified ACL to the specified MSDP peer.
  - If **acl** parameter is configured, the device sends only the locally created SA messages that match the specified ACL to the specified MSDP peer.

You can also run the **import-source** command on the peer nearest to a source to control the creation of SA messages.

The **import-source** command takes effect for all peers. If both the **import-source** and **peer** *peer-address* **sa-policy local-export** commands are run, the parameters configured in the **peer** *peer-address* **sa-policy local-export** command take effect preferentially.

Prerequisites

MSDP peers have been configured using the **peer connect-interface (MSDP)** command.

Example

Configure the switch to forward only the SA messages that pass the ACL3100 filtering to peer 10.10.7.6.


```
<HUAWEI> system-view
[HUAWEI] acl number 3100
[HUAWEI-acl-adv-3100] rule permit ip source 10.15.0.0 0.0.255.255 destination 225.1.0.0 0.0.255.255
[HUAWEI-acl-adv-3100] quit
[HUAWEI] multicast routing-enable
[HUAWEI] msdp
[HUAWEI-msdp] peer 10.10.7.6 connect-interface vlanif 100
[HUAWEI-msdp] peer 10.10.7.6 sa-policy export acl 3100
```

8.5.24 peer sa-request-policy

Function

The **peer sa-request-policy** command configures the filtering policy to respond to the SA Request messages sent by a specified MSDP peer. Once the SA Request message passes the filtering, the switch responds to the SA message immediately.

The **undo peer sa-request-policy** command restores the default configuration.

By default, the switch responds to all SA request messages sent by all MSDP peers.

Format

peer *peer-address* **sa-request-policy** [**acl** *basic-acl-number*]

undo peer *peer-address* **sa-request-policy**

Parameters

Parameter	Description	Value
peer-address	Specifies the address of MSDP peer that sends the SA Request message.	The address is in dotted decimal notation.
acl	Indicates an ACL. If the ACL is not specified, all SA Requests messages of the MSDP peer are ignored. If the ACL is specified, only the SA Request messages of the group that meets the requirements of the ACL are processed.	-
basic-acl-number	Indicates the number of the basic ACL.	The number is an integer that ranges from 2000 to 2999.

Views

MSDP view of the public network instance or MSDP view of the VPN instance

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When a local MSDP peer receives SA Request messages, the MSDP peer responds to all SA Request messages by default. To configure the switch to respond only to certain SA Request messages, configure the **peer sa-request-policy** command.

Prerequisites

MSDP peers have been configured using the **peer connect-interface (MSDP)** command.

Precautions

The **peer sa-request-policy** and **acl** commands are used together.

- In the basic ACL view, you can set the multicast group address range of SA messages that are forwarded by the MSDP peer by specifying the **source** parameter in the **rule** command.

Example

Configure the ACL for filtering SA request messages sent by the MSDP peer 10.58.6.5: only SA request messages bound for the group whose address is 225.1.1.0/24 are received.

```
<HUAWEI> system-view
[HUAWEI] acl number 2001
[HUAWEI-acl-basic-2001] rule permit source 225.1.1.0 0.0.0.255
[HUAWEI-acl-basic-2001] quit
[HUAWEI] multicast routing-enable
[HUAWEI] msdp
[HUAWEI-msdp] peer 10.58.6.5 connect-interface vlanif 100
[HUAWEI-msdp] peer 10.58.6.5 sa-request-policy acl 2001
```

8.5.25 reset msdp control-message counters

Function

The **reset msdp control-message counters** command clears statistics about MSDP messages.

Format

reset msdp [**vpn-instance** *vpn-instance-name* | **all-instance**] **control-message counters** [**peer** *peer-address*]

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Specifies a VPN instance. *vpn-instance-name* specifies the name of the VPN instance.	The value must be an existing VPN instance name.

Parameter	Description	Value
all-instance	Indicates all instances, including the public network instance and all VPN instances. If **vpn-instance** or **all-instance** is not specified, only information about the public network instance is cleared.	-
peer *peer-address*	Specifies IP address of MSDP peer. If **peer** *peer-address* is specified, only statistics about the MSDP messages exchanged with a specified MSDP peer are cleared.	The value is in dotted decimal notation.

Views

User view

Default Level

3: Management level

Usage Guidelines

This command clears statistics about the received, sent, and discarded MSDP messages.

Example

Clear statistics about the MSDP messages received, sent, and discarded on the peer 10.3.3.3.

```
<HUAWEI> reset msdp control-message counters peer 10.3.3.3
```

8.5.26 reset msdp peer

Function

The **reset msdp peer** command resets the TCP connection with a specified MSDP peer, and clears statistics about the specified MSDP peer.

Format

reset msdp [**vpn-instance** *vpn-instance-name* | **all-instance**] **peer** [*peer-address*]

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Specifies a VPN instance. *vpn-instance-name* specifies the name of the VPN instance.	The value must be an existing VPN instance name.
all-instance	Indicates all the instances. If **vpn-instance** or **all-instance** is not specified, the TCP connections set up between MSDP peers in the public network instance are reset and statistics about MSDP peers in the public network instance are cleared.	-
peer-address	Specifies the address of an MSDP peer. If the *peer-address* is not specified, all peers are reset.	The value is in dotted decimal notation.

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To re-configure the TCP connection between MSDP peers and clear statistics about the specified MSDP peer, run the **reset msdp peer** command.

Use the **reset msdp statistics** command to clear the statistics about an MSDP peer without resetting the MSDP peer.

Configuration Impact

NOTICE

After you run this command, the TCP connection with the specified MSDP peer is torn down and a new TCP is set up again. During this process, MSDP services are interrupted, which may affect multicast services; for example, multicast data transmission may fail. Therefore, use this command with caution.

Example

Reset the TCP connection with MSDP peer 10.10.7.6 and clear the statistics about MSDP peer 10.10.7.6.

```
<HUAWEI> reset msdp peer 10.10.7.6
```

8.5.27 reset msdp sa-cache

Function

The **reset msdp sa-cache** command clears (S, G) entries in the SA cache.

Format

reset msdp [**vpn-instance** *vpn-instance-name* | **all-instance**] **sa-cache** [*group-address*]

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Specifies a VPN instance. *vpn-instance-name* specifies the name of the VPN instance.	The value must be an existing VPN instance name.
all-instance	Indicates all the instances. If **vpn-instance** or **all-instance** is not specified, only the entries in the SA cache of the public network instance are cleared.	-
group-address	Specifies the group address carried in (S, G) information. If this parameter is not specified, all (S, G) information in the SA cache is cleared.	The value ranges from 224.0.1.0 to 239.255.255.255, in dotted decimal notation.

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To clear (S, G) information from an SA cache, run the **reset msdp sa-cache** command.

Configuration Impact

NOTICE

(S, G) information in the SA cache cannot be restored after you clear it. Therefore, confirm the action before you use this command.

Example

Clear the (S, G) entries with the group address of 225.5.4.3 in the SA cache.

```
<HUAWEI> reset msdp sa-cache 225.5.4.3
```

8.5.28 reset msdp statistics

Function

The **reset msdp statistics** command clears statistics about one or more MSDP peers without resetting the MSDP peer (s).

Format

reset msdp [**vpn-instance** *vpn-instance-name* | **all-instance**] **statistics** [*peer-address*]

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Specifies a VPN instance. *vpn-instance-name* specifies the name of the VPN instance.	The value must be an existing VPN instance name.
all-instance	Indicates all the instances. If **vpn-instance** or **all-instance** is not specified, only information about the public network instance is cleared.	-
peer-address	Specifies the address of an MSDP peer. If the *peer-address* is not specified, the statistics about all MSDP peers are cleared.	The value is in dotted decimal notation.

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

After the **reset msdp statistics** command is used, the statistics about the MSDP peer are cleared automatically. However, the TCP connections among peers are not closed, and MSDP services are not affected.

To clear the statistics about an MSDP peer and to rebuild the TCP connections among MSDP peers at the same time, use the **reset msdp peer** command.

Example

Clear the statistics of MSDP peer 10.10.7.6.

```
<HUAWEI> reset msdp statistics 10.10.7.6
```

8.5.29 shutdown (MSDP)

Function

The **shutdown** command terminates a specified MSDP peer.

The **undo shutdown** command restores the default configuration.

By default, the MSDP peers are not closed after the peer relationship is established.

Format

shutdown *peer-address*

undo shutdown *peer-address*

Parameters

Parameter	Description	Value
peer-address	Specifies the address of an MSDP peer.	The address is in dotted decimal notation.

Views

MSDP view of the public network instance or MSDP view of the VPN instance

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **shutdown** command can be used to close the TCP connection between two MSDP peers while keeping the MSDP peer relationship.

Prerequisites

MSDP peers have been configured using the **peer connect-interface (MSDP)** command.

Configuration Impact

After the **shutdown** command is run on MSDP peers, the MSDP peers do not transmit SA messages or attempt to establish a connection. When the **display msdp brief** command or the **display msdp peer-status** command is used to check the status of MSDP peers, **State** in the command output is displayed as **Shutdown**.

Precautions

You only need to run the **undo shutdown** command to restore the configuration, and do not need to re-configure the MSDP peer using the **peer connect-interface (MSDP)** command.

Example

Close MSDP peer 10.10.7.6.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] msdp
[HUAWEI-msdp] peer 10.10.7.6 connect-interface vlanif 100
[HUAWEI-msdp] shutdown 10.10.7.6
```

8.5.30 static-rpf-peer

Function

The **static-rpf-peer** command configures an MSDP peer as a static RPF peer. The SA messages sent by the static RPF peer do not require RPF checks.

The **undo static-rpf-peer** command restores the default configuration.

By default, no MSDP peer is configured as a static RPF peer.

Format

static-rpf-peer *peer-address* [**rp-policy** *ip-prefix-name*]

undo static-rpf-peer *peer-address*

Parameters

Parameter	Description	Value
peer-address	Specifies the address of a static RPF peer.	The value is in dotted decimal notation.

Parameter	Description	Value
rp-policy *ip-prefix-name*	Specifies the filtering policy that is used to filter SA messages based on RP addresses. **ip ip-prefix** specifies the name of the filtering policy.	The name is a string of 1 to 169 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Views

MSDP view of the public network instance or MSDP view of the VPN instance

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To prevent SA messages from being circularly forwarded between MSDP peers, MSDP performs the RPF check on the received SA message. MSDP strictly controls the incoming SA messages. The SA messages that do not comply with the RPF rules are discarded.

To protect the SA messages transmitted between MSDP peers from being discarded in RPF checks and reduce redundant traffic, you can specify MSDP peers as static RPF peers. The SA messages received from a static RPF peer do not need to be checked according to RPF rules.

Prerequisites

The MSDP peer relationship has been established between the switch and a specified RPF peer using the **peer connect-interface (MSDP)** command.

Configuration Impact

You can specify multiple remote static RPF peers for the switch using the **static-rpf-peer** *peer-address* command repeatedly.

Precautions

When you specify multiple static RPF peers for the switch, pay attention to the following points:

- All the peers are configured with **rp-policy**

  When SA messages sent by a static RPF peer in the active state reaches the local switch, the local switch filters the SA messages according to specified **rp-policy** on the peers, and receives only the SA messages that pass the filter.
- None of the peers is configured with **rp-policy**

  The local switch receives all the SA messages from the static RPF peers in the active state.

Example

Configure 192.168.3.2 as a static RPF peer, with the source RP address range of 192.168.0.0/16.

```
<HUAWEI> system-view
[HUAWEI] ip ip-prefix list-df permit 192.168.0.0 16 greater-equal 16 less-equal 32
[HUAWEI] multicast routing-enable
[HUAWEI] msdp
[HUAWEI-msdp] peer 192.168.3.2 connect-interface vlanif 100
[HUAWEI-msdp] static-rpf-peer 192.168.3.2 rp-policy list-df
```

8.5.31 timer retry

Function

The **timer retry** command sets the interval for retrying to set up an MSDP peer relationship.

The **undo timer retry** command restores the default value.

By default, the interval for retrying to set up an MSDP peer relationship is 30 seconds.

Format

timer retry *interval*

undo timer retry

Parameters

Parameter	Description	Value
interval	Specifies the interval for retrying to set up an MSDP peer relationship.	The value is an integer that ranges from 1 to 60, in seconds.

Views

MSDP view of the public network instance or MSDP view of the VPN instance

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A TCP connection needs to be set up between two MSDP peers. The peer with a larger IP address listens to port 639, and the peer with a smaller IP address initiates a connection. If the connection setup fails, the peer retries connection setup after a specified interval.

A TCP connection needs to be established between MSDP peers in one of the following situations:

- An MSDP peer is created.
- A disconnected MSDP peer needs to be reconnected
- A faulty MSDP peer attempts to restore work.

You can run the **timer retry** command to adjust the interval for retrying to set up an MSDP peer relationship.

Prerequisites

MSDP has been enabled using the **msdp** command.

Example

Set the interval for retrying to set up an MSDP peer relationship to 60 seconds.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] msdp
[HUAWEI-msdp] timer retry 60
```

8.6 Multicast VPN Configuration Commands

8.6.1 Command Support

Only the following switch models support Multicast VPN:

S5731-S, S5731-H, S5731S-H, S5732-H,, S6720-EI, S6720S-EI, S6730-S, S6730-H, and S6730S-H

8.6.2 auto-discovery

Function

The **auto-discovery** command configures the auto-discovery (A-D) mode for the multicast VPN, and associates an inbound multicast routing policy with the IPv4 address family of the current VPN instance.

The **undo auto-discovery** command deletes the A-D mode configuration for the multicast VPN and removes the association between the inbound multicast routing policy and the IPv4 address family of the current VPN instance.

By default, the A-D mode is not configured for the multicast VPN and the IPv4 address family of the current VPN instance is not associated with an inbound multicast routing policy.

Format

auto-discovery { **mdt** | **mvpn** } [**import route-policy** *route-policy-name*]

undo auto-discovery

Parameters

Parameter	Description	Value
mdt	Specifies the MDT-Subsequent Address Family Identifier (SAFI) A-D mode for the multicast VPN.	-
mvpn	Specifies the MCAST-VPN SAFI A-D mode for the multicast VPN.	-
route-policy *route-policy-name*	Specifies the inbound multicast routing policy that is to be associated with the IPv4 address family of the VPN instance.	The name is a string of 1 to 40 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Views

VPN instance view, VPN IPv4 address family view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Currently, the multicast VPN is implemented by establishing the PIM-SSM MDT on the public network to transmit multicast VPN services as all Provider Edges (PEs) on the network know information about the Rendezvous Point (RP). This mechanism, however, does not support the Share-Group address within the SSM address range. This is because PEs in the same VPN do not know the peer information of each other, therefore knowing nothing about the multicast source information. As a result, these PEs cannot directly send Join messages to the multicast source and establish the PIM-SSM MDT.

To solve this problem, in an autonomous system (AS), you can configure the BGP A-D mode to enable automatic discovery of the peer information about PEs in the same VPN. In this manner, multicast VPN services can be transmitted over the public network tunnel which is based on the PIM-SSM MDT.

At present, the multicast VPN supports two A-D modes:

- MDT-SAFI A-D mode: In this mode, a new address family is defined in the MDT-SAFI message advertised through BGP. After the multicast VPN is configured on a PE, the multicast VPN configurations, including the Route Distinguisher (RD) and the Share-Group address, can be advertised to all BGP peers. After a remote PE (a BGP peer) receives the MDT-SAFI message advertised through BGP, the remote PE compares the RD carried in the message with its local RD. If the RDs are the same, the remote PE is in the same VPN as the local PE. The remote PE then uses the MDT-SAFI message to establish the PIM-SSM MDT for transmitting multicast VPN services.

- MCAST-VPN SAFI A-D mode: In this mode, a new address family is defined in the MCAST-VPN-SAFI message advertised through BGP. Similar to the MDT-SAFI A-D mode, the MCAST-VPN SAFI A-D mode uses the MCAST-VPN-SAFI message advertised between BGP peers to transmit multicast VPN configurations, including the RD and Share-Group address. The difference is that the MCAST-VPN SAFI A-D mode has a broader definition, supports more extensions, and carries more multicast VPN attributes and information for establishing the public network tunnel. Therefore, the MCAST-VPN SAFI A-D mode applies to the next-generation multicast VPN.

Prerequisites

The **multicast routing-enable** command is configured in the public network instance view or the VPN instance view.

Precautions

- When configuring the A-D mode for the multicast VPN, you need to configure a matching A-D address family in the BGP view so that the BGP A-D mode can be used to implement the multicast VPN function. If the configured A-D mode is inconsistent with the A-D address family enabled in the BGP view, the A-D mode will not take effect.
- This command applies to the single-AS scenario, with no RP configured on the public network.
- In a VPN enabled with the IPv4 address family, only one A-D mode can be used. Different VPNs enabled with the IPv4 address family on a PE can use different A-D modes. Therefore, you need to enable two types of A-D address families in the BGP view, so that the VPNs can use different A-D modes to forward multicast data.
- The PEs enabled with the BGP A-D function must support the same PIM protocol and use the Share-Group address within the SSM address range.
- Running this command does not affect the original multicast VPN service flow. If the Share-Group address is in the Any-Source Multicast (ASM) address range, or if the PIM-DM protocol is used on the public network, multicast VPN traffic can still be transmitted over the public network tunnel for which PIM-SM or PIM-DM is configured.

Example

Configure the MDT-SAFI A-D mode for vpn1 enabled with the IPv4 address family, so that the multicast VPN services are transmitted over the public network tunnel based on the PIM-SSM MDT.

```
<HUAWEI> system-view
[HUAWEI] bgp 100
[HUAWEI-bgp] ipv4-family mdt
[HUAWEI-bgp-af-mdt] peer 3.3.3.3 enable
[HUAWEI-bgp-af-mdt] quit
[HUAWEI-bgp] quit
[HUAWEI] ip vpn-instance vpn1
[HUAWEI-vpn-instance-vpn1] ipv4-family
[HUAWEI-vpn-instance-vpn1-af-ipv4] route-distinguisher 100:1
[HUAWEI-vpn-instance-vpn1-af-ipv4] vpn-target 100:1 both
[HUAWEI-vpn-instance-vpn1-af-ipv4] multicast routing-enable
[HUAWEI-vpn-instance-vpn1-af-ipv4] multicast-domain share-group 232.2.2.0 binding mtunnel 0
[HUAWEI-vpn-instance-vpn1-af-ipv4] auto-discovery mdt
```


8.6.3 display default-parameter mvpn

Function

The **display default-parameter mvpn** command displays default configurations about the multicast VPN (MVPN).

Format

display default-parameter mvpn

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Using this command displays only default configurations, regardless of whether the configurations about MVPN parameters are changed.

Example

Display default configurations about the MVPN.

```
<HUAWEI> display default-parameter mvpn
  MVPN Instance View Default Configurations:
  ------------------------------------------
  Multicast-domain switch-delay: 5 s
  Multicast-domain switch threshold: 0 kbps-preferred
  Multicast-domain holddown-time: 60 s
  Multicast-domain log switch-group-reuse: disabled
  Multicast-domain share-group: disabled
  Multicast-domain switch-group-pool: disabled
  Multicast-domain auto-discovery: disabled
  Multicast-domain switch-without-register: disabled
  Multicast extranet select-rpf rule: disabled
```

Table 8-81 Description of the **display default-parameter mvpn** command output

Item	Description
MVPN Instance View Default Configurations	Default configurations in the MVPN instance view.

Item	Description
Multicast-domain switch-delay	Delay in switching from the share-MDT to the switch-MDT. This parameter can be configured using the **multicast-domain switch-delay** command in the VPN instance view or VPN IPv4 address family view.
Multicast-domain switch threshold	Threshold of the multicast packet rate that can trigger the switch to the switch-MDT. This parameter can be configured using the **multicast-domain switch-group-pool** command in the VPN instance view or VPN IPv4 address family view.
Multicast-domain holddown-time	Delay in switching from the switch-MDT to the share-MDT. This parameter can be configured using the **multicast-domain holddown-time** command in the VPN instance view or VPN IPv4 address family view.
Multicast-domain log switch-group-reuse	Whether recording logs about switch-group address reuse is configured. This parameter can be configured using the **multicast-domain log switch-group-reuse** command in the VPN instance view or VPN IPv4 address family view.
Multicast-domain share-group	Whether the Share-Group address is configured and whether the MTI is bound to a VPN instance. This parameter can be configured using the **multicast-domain share-group binding** command in the VPN instance view or VPN IPv4 address family view.
Multicast-domain switch-group-pool	Whether the range of the switch-MDT switch-group-pool is configured. This parameter can be configured using the **multicast-domain switch-group-pool** command in the VPN instance view or VPN IPv4 address family view.
Multicast-domain auto-discovery	Whether the A-D mode is configured for the VPN. The switch does not support the A-D mode currently.

Item	Description
Multicast-domain switch-without-register	Whether the source PE sends the null Register message to the RP to establish the SPT on the public network before the Switch-Group address is used to encapsulate VPN data. This parameter can be configured using the **multicast-domain switch-without-register** command in the VPN instance view or VPN IPv4 address family view.
Multicast extranet select-rpf rule	Whether the multicast routing policy configured for a VPN is configured. The switch does not support the configuration of a multicast routing policy for a VPN currently.

8.6.4 display multicast-domain control-message counters

Function

The **display multicast-domain control-message counters** command displays statistics about sent and received MDT switch messages in a specified VPN instance or all VPN instances.

Format

display multicast-domain { **vpn-instance** *vpn-instance-name* | **all-instance** } **control-message counters**

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Displays statistics about sent and received MDT switch messages in a specified VPN instance. The parameter *vpn-instance-name* specifies the name of an existing VPN instance on the device.	The value must be an existing VPN instance name.
all-instance	Displays statistics about sent and received MDT switch messages in all VPN instances.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After configuring a Switch-MDT, you can run the **display multicast-domain control-message counters** command to view statistics about sent and received MDT switch messages in a specified VPN instance or all VPN instances and check whether packets are normally sent and received on the current device.

You can run the **reset multicast-domain control-message counters** command to clear the statistics.

Example

Display statistics about sent and received MDT switch messages in VPN instance **red**.

```
<HUAWEI> display multicast-domain vpn-instance red control-message counters
VPN-Instance red:
 Message Type     Received        Sent          Invalid
 Switch           5000            0             5000
```

Table 8-82 Description of the **display multicast-domain vpn-instance red control-message counters** command output

Item	Description
VPN-Instance red	VPN instance in which statistics about sent and received MDT switch messages need to be displayed.
Message Type	Message type, that is MDT switch messages.
Received	Number of received messages.
Sent	Number of sent messages.
Invalid	Number of received invalid messages.

8.6.5 display multicast-domain invalid-packet

Function

The **display multicast-domain invalid-packet** command displays statistics about invalid MDT switch messages received by a device and details of these messages.

Format

display multicast-domain { **vpn-instance** *vpn-instance-name* | **all-instance** } **invalid-packet**

display multicast-domain invalid-packet [*packet-number*] **verbose**

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Displays statistics about invalid MDT switch messages received in a specified VPN instance. The parameter *vpn-instance-name* specifies the name of an existing VPN instance on the device.	The value must be an existing VPN instance name.
all-instance	Displays statistics about invalid MDT switch messages received in all VPN instances.	-
packet-number	Displays details of a specified number of invalid MDT switch messages recently received.	The value is an integer ranging from 1 to 100. By default, details of all the invalid MDT switch messages currently stored are displayed.
verbose	Displays details of invalid MDT switch messages.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display multicast-domain invalid-packet** command to view statistics and details of invalid MDT switch messages for fault location and rectification.

If an SPT fails to be set up in a VPN instance on a multicast network, you can run the **display multicast-domain invalid-packet** command first to check whether devices have received invalid MDT switch messages. If the command output contains statistics about invalid MDT switch messages, you need to run the **display multicast-domain invalid-packet** [*packet-number*] **verbose** command to view details of invalid MDT switch messages to locate the fault.

Example

Displays statistics about invalid MDT switch messages received in **vpn1**.

```
<HUAWEI> display multicast-domain vpn-instance vpn1 invalid-packet

          Statistics of invalid packets for vpn1:
------------------------------------------------------------------------
MDT Switch invalid packet:
Fault Length          : 0          Invalid Message Type    : 0
```



```
Invalid Multicast Source: 0          Invalid Multicast Group : 0
Invalid Switch Group    : 0
------------------------------------------------------------------------
```

Table 8-83 Description of the **display multicast-domain vpn-instance vpn1 invalid-packet** command output

Item	Description
Statistics of invalid packets for vpn1	VPN instance in which statistics about MDT switch messages need to be displayed.
MDT Switch invalid packet	Invalid MDT switch messages.
Fault Length	Messages with invalid lengths.
Invalid Message Type	Messages with invalid message types.
Invalid Multicast Source	Messages with invalid multicast source addresses.
Invalid Multicast Group	Messages with invalid multicast group addresses.
Invalid Switch Group	Messages with invalid switch group addresses.

Display details of one invalid MDT switch message recently received in the public network instance.

```
<HUAWEI> display multicast-domain invalid-packet 1 verbose
      Detailed information of invalid packets
------------------------------------------------------
Packet information (Index 1):
------------------------------------------------------
Interface          :  10.44.44.44
Time               :  2010-6-9 10:50:08 UTC-08:00
Message Length     :  16
Invalid Type       :  Invalid Switch Group
0000: 01 00 10 00 64 64 64 64 e8 00 00 00 0a 00 00 00
------------------------------------------------------
```

Table 8-84 Description of the **display multicast-domain invalid-packet 1 verbose** command output

Item	Description
Detailed information of invalid packets	Details of the invalid MDT switch message.
Packet information (Index 1)	Sequence number of the invalid MDT switch message (numbered in the opposite order that the message is received, for example, the index of the last received message is 1, the index of the last but one message is 2, and so on).

Item	Description
Interface	IP address of interface receiving the invalid MDT switch message
Time	Time when the invalid MDT switch message is received, in any of the following formats: • YYYY-MM-DD HH:MM:SS • YYYY-MM-DD HH:MM:SS UTC±HH:MM DST • YYYY-MM-DD HH:MM:SS UTC±HH:MM • YYYY-MM-DD HH:MM:SS DST UTC±HH:MM indicates that a time zone is configured through the **clock timezone** command; DST indicates that the daylight saving time is configured through **clock daylight-saving-time** command.
Message Length	Length of the invalid MDT switch message.
Invalid Type	Type of the invalid MDT switch message.
0000: 01 00 10 00 64 64 64 64 e8 00 00 00 0a 00 00 00	Contents of the invalid MDT switch message.

8.6.6 display multicast-domain vpn-instance share-group

Function

The **display multicast-domain vpn-instance share-group** command displays information about the Share-Group address configured for a specified VPN instance.

Format

display multicast-domain vpn-instance *vpn-instance-name* **share-group** [**local** | **remote**]

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Displays information about the Share-Group of a specified VPN instance. The parameter *vpn-instance-name* specifies the name of an existing VPN instance on the device.	The value must be an existing VPN instance name.

Parameter	Description	Value
local	Indicates the locally configured Share-Group address.	-
remote	Indicates the Share-Group address configured on remote PE and learned through BGP Update packets.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The **display multicast-domain vpn-instance share-group** command displays information about the Share-Group, peer IP address, and tunnel type, which allows you to determine whether the multicast tunnel is correctly established to forward multicast services.

Example

Display the Share-Group information of VPN instance **BLUE** in an MD.

```
<HUAWEI> display multicast-domain vpn-instance BLUE share-group
MD local share-group information for VPN-Instance: BLUE
  Share-group: 239.2.2.0
  MTunnel address: 3.3.3.3
```

Table 8-85 Description of the **display multicast-domain vpn-instance share-group** command output

Item	Description
MD local share-group information for VPN-Instance	VPN instance to which local Share-Group information in the multicast domain belongs.
Share-group	Share-MDT group address configured on the local switch. This parameter can be configured using the **multicast-domain share-group binding** command in the VPN instance view or VPN IPv4 address family view.

Item	Description
MTunnel address	Configured IP address of the MTI bound to the Share-Group on the local switch. The source interface whose IP address is referenced by the MTI can be configured using the **multicast-domain source-interface** command in the VPN IPv4 address family view. In this way, the IP address of the MTI is obtained. You can also directly configure an IP address for an MTI in the MTI interface view.

8.6.7 display multicast-domain vpn-instance switch-group receive

Function

The **display multicast-domain vpn-instance switch-group receive** command displays the Switch-Group information received by a specified VPN instance.

Format

display multicast-domain vpn-instance *vpn-instance-name* **switch-group receive brief**

display multicast-domain vpn-instance *vpn-instance-name* **switch-group receive** [**active** | **sender** *source-address* | **group** *group-address* | *vpn-source-address* [**mask** { *source-mask-length* | *source-mask* }] | *vpn-group-address* [**mask** { *group-mask-length* | *group-mask* }]] *

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Displays the Switch-Group information received by a specified VPN instance. The parameter *vpn-instance-name* specifies the name of an existing VPN instance on the device.	The value must be an existing VPN instance name.
active	Displays the received Switch-Group that joins the Switch-MDT.	-
brief	Displays brief information about the received Switch-Group.	-

Parameter	Description	Value
group *group-address*	Displays the Switch-Group related to a multicast group specified by *group-address* of the public network. *group-address* specifies the address of the multicast group.	The value is in dotted decimal notation and ranges from 224.0.1.0 to 239.255.255.255.
sender *source-address*	Displays the Switch-Group information related to the specified multicast source *source-address* of the public network. The *source-address* indicates the multicast.	The value is in dotted decimal notation.
vpn-source-address	Displays the Switch-Group information related to a VPN multicast source specified by *vpn-source-address*.	The value is in dotted decimal notation.
mask	Indicates the mask of the VPN multicast group or source address.	-
source-mask-length	Specifies the mask length of the VPN multicast source address.	The value is an integer that ranges from 0 to 32.
source-mask	Specifies the mask of the VPN multicast source address.	The value is in dotted decimal notation.
vpn-group-address	Displays the Switch-Group information related to a VPN multicast group specified by *vpn-group-address*.	The value is in dotted decimal notation and ranges from 224.0.1.0 to 239.255.255.255.
group-mask-length	Specifies the mask length of the VPN multicast group address.	The value is an integer that ranges from 4 to 32.
group-mask	Specifies the mask of the VPN multicast group address.	The value is in dotted decimal notation.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display multicast-domain vpn-instance switch-group receive** command to display the Switch-Group information received by the local router:

- Each VPN instance corresponds to an MD. *vpn-instance-name* specifies a VPN instance. Use the command to display the information about the Switch-Group of a specified MD.

- If **brief** is specified, brief information about all Switch-Groups is displayed in ascending order of the Switch-Group address.
- If **active** is specified, only information about the Switch-Groups that have joined the Switch-MDT is displayed, in ascending order of the VPN (S, G).

Example

Display Switch-Group information received by VPN instance **VPN1** in an MD.

```
<HUAWEI> display multicast-domain vpn-instance VPN1 switch-group receive
MD switch-group information received by VPN-Instance: VPN1
Switch group:  226.1.1.0 ref count: 8, active count: 8
  Sender:  172.16.1.1 active count: 8
    (192.168.1.5, 239.1.1.1)
    Up time: 01:20:20  expire time: 00:03:10  active
    (192.168.1.5, 239.1.1.158)
    Up time: 01:20:20  expire time: 00:03:10  active
    (192.168.1.5, 239.1.2.12)
    Up time: 01:20:20  expire time: 00:03:10  active
    (192.168.1.5, 239.1.2.197)
    Up time: 01:20:20  expire time: 00:03:10  active
    (192.168.1.5, 239.1.3.62)
    Up time: 01:20:20  expire time: 00:03:10  active
    (192.168.1.2, 225.1.1.109)
    Up time: 01:20:20  expire time: 00:03:10  active
    (192.168.1.2, 225.1.4.80)
    Up time: 01:20:20  expire time: 00:03:10  active
    (192.168.1.2, 225.1.4.173)
    Up time: 01:20:20  expire time: 00:03:10  active
```

Display brief Switch-Group information received by VPN instance **VPN1** in an MD.

```
<HUAWEI> display multicast-domain vpn-instance VPN1 switch-group receive brief
MD switch-group information received by VPN-Instance: VPN1
switch group:  226.1.1.0 ref count: 8, active count: 0
switch group:  226.1.1.1 ref count: 4, active count: 0
switch group:  226.1.1.2 ref count: 8, active count: 0
switch group:  226.1.1.3 ref count: 4, active count: 0
switch group:  226.1.1.4 ref count: 8, active count: 0
```

Table 8-86 Description of the **display multicast-domain vpn-instance switch-group receive** command output

Item	Description
MD switch-group information received by VPN-Instance	VPN instance to which MD Switch-Group information belongs.
switch group	Address of the received Switch-Group.
ref count	Number of VPN multicast groups referenced by the Switch-Group.
active count	Number of active VPN multicast groups (where receivers exist) referenced by the Switch-Group.
sender	BGP peer IP address of the PE that sends Switch-Group information.

Item	Description
Up time	Creation time of switching messages in which the VPN multicast (S, G) entry is referenced by the Switch-group
expire time	Timeout period of the VPN multicast (S, G) entry referenced by the Switch-Group.

8.6.8 display multicast-domain vpn-instance switch-group send

Function

The **display multicast-domain vpn-instance switch-group send** command displays the Switch-Group information sent by the specified VPN instance in an MD.

Format

display multicast-domain vpn-instance *vpn-instance-name* **switch-group send** [**reuse** *interval* | *vpn-source-address* [**mask** { *source-mask-length* | *source-mask* }] | *vpn-group-address* [**mask** { *group-mask-length* | *group-mask* }] | **group** *group-address*] *

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Displays the Switch-Group information sent by a specified VPN instance. The parameter *vpn-instance-name* specifies the name of an existing VPN instance on the device.	The value must be an existing VPN instance name.
group *group-address*	Displays the Switch-Group information related to a multicast group G. The parameter *group-address* indicates multicast group address.	The value is in dotted decimal notation format. The address ranges from 224.0.1.0 to 239.255.255.255.
reuse *interval*	Displays Switch-Group information that is reused by an MD in the specified period. The parameter *interval* indicates the specified period.	The value of the interval is an integer that ranges from 1 to 2147483647 seconds.

Parameter	Description	Value
vpn-source-address	Displays the Switch-Group information related to the specified VPN multicast source.	The value is in dotted decimal notation format.
mask	Indicates the mask of the VPN multicast group or source address.	-
source-mask-length	Specifies the mask length of the VPN multicast source address.	The value is an integer that ranges from 0 to 32.
source-mask	Specifies the mask of the VPN multicast source address.	The value is in dotted decimal notation.
vpn-group-address	Displays the Switch-Group information related to the specified VPN multicast group G.	The value is in dotted decimal notation and ranges from 224.0.1.0 to 239.255.255.255.
group-mask-length	Specifies the mask length of the VPN multicast group address.	The value is an integer that ranges from 4 to 32.
group-mask	Specifies the mask of the VPN multicast group address.	The value is in dotted decimal notation.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Use the **display multicast-domain vpn-instance switch-group send** command to display the Switch-Group information sent by the local switch:

- Each VPN instance corresponds to an MD. *vpn-instance-name* specifies a VPN instance. The command is only used to display the Switch-Group information related to the specified MD.
- The Switch-Group information is displayed in ascending order of VPN (S, G) entry.
- If **reuse** *interval* is specified, the group information that is reused in a specified interval is displayed in ascending order of Switch-Group address.

Example

Display the Switch-Group information sent by VPN instance **VPN1** in an MD.

```
<HUAWEI> display multicast-domain vpn-instance VPN1 switch-group send
MD switch-group information sent by VPN-Instance: VPN1
 226.1.1.0 reference_count: 3
   (1.1.1.1, 239.1.1.1)              switch time: 00:00:21
   (1.1.1.1, 239.1.1.158)             switch time: 00:00:21
```



```
  (1.1.1.1, 239.1.2.50)              switch time: 00:00:05
226.1.1.1 reference_count: 3
  (1.1.1.1, 225.1.1.1)              switch time: 00:00:21
  (1.1.1.1, 225.1.2.50)              switch time: 00:00:05
  (1.1.1.1, 239.1.1.159)             switch time: 00:00:21
```

Display information about the Switch-Group reuse sent by VPN instance **VPN1** in an MD within the latest 30s.

```
<HUAWEI> display multicast-domain vpn-instance VPN1 switch-group send reuse 30
MD switch-group information sent by VPN-Instance: VPN1
 226.1.1.0 reuse_count: 1
 226.1.1.1 reuse_count: 1
 226.1.1.2 reuse_count: 1
```

Table 8-87 Description of the **display multicast-domain vpn-instance switch-group send** command output

Item	Description
MD switch-group information sent by VPN-Instance	VPN instance to which MD Switch-Group information belongs.
226.1.1.0 reference_count	Number of VPN multicast groups referenced by the Switch-Group.
switch time	Switching time of the VPN multicast (S, G) entry referenced by the Switch-Group.
226.1.1.0 reuse_count	Number of times of reusing the Switch-Group sent in the specified period.

8.6.9 interface mtunnel

Function

The **interface mtunnel** command displays the MTI view.

Format

interface mtunnel *interface-number*

Parameters

Parameter	Description	Value
interface-number	Specifies an MTI number.	The value is an integer that ranges from 0 to 1023.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

An MTI is the inbound/outbound interface of a multicast tunnel and also functions as the inbound/outbound interfaces of the MD. A local PE sends VPN data through the MTI, and the remote PE receives data from the MTI. The MTI is the tunnel for data exchange between the public network instance and the VPN instance on the PE. A PE connects to the MT through the MTI. The VPN instances on PEs in the MD establish PIM neighbor relationships with each other on the MTI.

When you run the **multicast-domain share-group binding** command, the MTI is automatically created. You can run the **interface mtunnel** command to enter the MTI view and configure MTI parameters

Prerequisites

The MIT has been automatically created after the **multicast-domain share-group binding** command is executed to configure a Share-Group for a VPN instance and bind the Share-Group to the MTI.

Example

Enter the view of MTunnel interface 10, which has been automatically created.

```
<HUAWEI> system-view
[HUAWEI] interface mtunnel 10
[HUAWEI-MTunnel10]
```

8.6.10 mtu (MTI view)

Function

The **mtu** command sets the MTU for a multicast tunnel interface (MTI).

The **undo mtu** command restores the default MTU of an MTI.

By default, the MTU of an MTI is 1472 bytes.

Format

mtu *mtu*

undo mtu

Parameters

Parameter	Description	Value
mtu	Specifies the MTU value of an MTI.	The value is an integer that ranges from 46 to 1500, in bytes.

Views

MTI view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If the length of a VPN multicast packet is equal or close to the MTU of the outbound interface of the public network instance, the length of the GRE-encapsulated public network multicast data packet is larger than the MTU of the outbound interface of the public network instance. In this case, the local PE must fragment the encapsulated packet and sends it through the outbound interface of the public network instance. Upon receiving the packet, the remote PE reassembles the packet.

You can set the MTU of the MTI to a smaller value so that VPN multicast packets can be fragmented before being encapsulated using the GRE. The remote PE does not need to reassemble the packets, improving efficiency.

Precautions

If the MTU is set too small and the size of packets is large, packets are broken into a great number of fragments, and may be discarded by QoS queues.

Example

Set the MTU of MTunnel 10 to 1400.

```
<HUAWEI> system-view
[HUAWEI] interface mtunnel 10
[HUAWEI-MTunnel10] mtu 1400
```

8.6.11 multicast-domain holddown-time

Function

The **multicast-domain holddown-time** command sets the delay for the switching from the Switch-MDT to the Share-MDT.

The **undo multicast-domain holddown-time** command restores the default value of the interval.

By default, the delay for the switching from the Switch-MDT to the Share-MDT is 60 seconds.

Format

multicast-domain holddown-time *interval*

undo multicast-domain holddown-time

Parameters

Parameter	Description	Value
interval	Specifies the delay for the switching from the Switch-MDT to the Share-MDT.	The value of the delay ranges from 0 to 512, in seconds.

Views

VPN instance view, VPN IPv4 address family view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

During the Switch-MDT configuration, the forwarding rate of VPN multicast data may fluctuate above and below the switchover threshold due to network instability. To prevent multicast data traffic from being frequently switched between the Switch-MDT and Share-MDT, the system does not perform the switchover immediately after it finds that the forwarding rate is smaller than the switching threshold. Instead, the system starts the hold-down timer and performs the switchover after the hold-down timer expires.

Prerequisites

A Share-Group has been configured using the **multicast-domain share-group binding** command.

Precautions

During a switchover, there is a delay about 1 to 30 seconds from the time when the forwarding rate ranges to the time when the system starts the Switch-Delay timer. The delay is not included in the hold-down time. Consequently, the total delay from the time when the forwarding rate changes to the time when the system completes the switchover is 1-30 seconds longer than the hold-down time.

When *interval* is set to 0, the system triggers a switchover from the Switch-MDT to the Share-MDT immediately after it finds that the forwarding rate is below the threshold.

If a VPN instance has many multicast forwarding entries, the time taken to collect multicast traffic statistics will exceed the default hold-down time. In this case,

increase the hold-down time to prevent frequent switchovers between the Switch-MDT and Share-MDT. **Table 8-88** lists the recommended hold-down time values in various conditions.

Table 8-88 Recommended hold-down time values

Number of Multicast Forwarding Entries in a VPN Instance	Recommended Hold-down Time Value (Seconds)
1024	60
2048	128
4094	256

Example

Set the delay for the switching from the Switch-MDT to the Share-MDT to 80 seconds.

```
<HUAWEI> system-view
[HUAWEI] ip vpn-instance mytest
[HUAWEI-vpn-instance-mytest] route-distinguisher 11:11
[HUAWEI-vpn-instance-mytest-af-ipv4] multicast routing-enable
[HUAWEI-vpn-instance-mytest-af-ipv4] multicast-domain share-group 224.1.1.1 binding mtunnel 0
[HUAWEI-vpn-instance-mytest-af-ipv4] multicast-domain holddown-time 80
```

8.6.12 multicast-domain log switch-group-reuse

Function

The **multicast-domain log switch-group-reuse** command enables the output of log information about reusing group address in Switch-Group-Pool.

The **undo multicast-domain log** command disables the output of log information about reusing group address in Switch-Group-Pool.

By default, the output of log information about reusing Switch-Group is disabled.

Format

multicast-domain log switch-group-reuse

undo multicast-domain log

Parameters

None

Views

VPN instance view, VPN IPv4 address family view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In the VPN instance that the source PE is bound to, if the Switch-Group-Pool cannot provide enough addresses for VPN multicast data packets whose transmission path needs to be switched to the Switch-MDT, the multicast group addresses can be reused. To record information about reusing Switch-Group, enable the output of log information about reusing Switch-Group addresses.

Prerequisites

A Share-Group has been configured using the **multicast-domain share-group binding** command.

Example

Enable the output of log information about reusing Switch-Group addresses in VPN **mytest**.

```
<HUAWEI> system-view
[HUAWEI] ip vpn-instance mytest
[HUAWEI-vpn-instance-mytest] route-distinguisher 11:11
[HUAWEI-vpn-instance-mytest-af-ipv4] multicast routing-enable
[HUAWEI-vpn-instance-mytest-af-ipv4] multicast-domain share-group 224.1.1.1 binding mtunnel 0
[HUAWEI-vpn-instance-mytest-af-ipv4] multicast-domain log switch-group-reuse
```

8.6.13 multicast-domain share-group binding

Function

The **multicast-domain share-group binding** command specifies the Share-MDT group and binds the Multicast Tunnel Interface (MTI) to a VPN instance.

The **undo multicast-domain share-group** command restores the default configuration.

By default, the group address of Share-MDT is not specified.

Format

multicast-domain share-group *group-address* **binding mtunnel** *number*

undo multicast-domain share-group

Parameters

Parameter	Description	Value
group-address	Specifies the multicast group address. **NOTE** Do not enter an IP address in the SSM address range (232.*.*.*); otherwise, the multicast VPN cannot be established.	The value is in the dotted decimal notation. The address ranges from 224.0.1.0 to 239.255.255.255.
mtunnel *number*	Specifies the MTI number.	The value is an integer that ranges from 0 to 1023.

Views

VPN instance view, VPN IPv4 address family view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When you run the **multicast-domain share-group binding** command, the device automatically creates the MTI and establishes a Share-MDT with the *group-address* value as the multicast group address for forwarding VPN multicast packets.

Prerequisites

The multicast routing function has been enabled using the **multicast routing-enable** command in the VPN instance.

Follow-up Procedure

Manually configure an IP address for the MTI in the MTI view or run the **multicast-domain source-interface** command in the VPN IPv4 address family view to configure the MTI to automatically obtain an IP address.

Precautions

You cannot configure the same Share-Group address for different VPN instances on a PE. The Share-Group address cannot be the same as the Switch-Group address. The *number* value must be set different from the MTI number.

You cannot repeatedly run the **multicast-domain share-group binding** command in the same VPN instance view. You can configure a new Share-MDT group address and MTI only after deleting the existing ones.

After the **undo multicast-domain share-group** command is executed, configurations about the MTI and Switch-MDT are deleted.

Some multicast protocol packets (such as Register and Graft packets) are sent in unicast mode. These packets are transmitted over unicast VPN tunnels but not multicast VPN tunnels (Mtunnels) on the public network.

Example

Specify the Share-Group of VPN instance **mytest** as 224.1.1.1 and bind MTI0.

```
<HUAWEI> system-view
[HUAWEI] ip vpn-instance mytest
[HUAWEI-vpn-instance-mytest] route-distinguisher 11:11
[HUAWEI-vpn-instance-mytest-af-ipv4] multicast routing-enable
[HUAWEI-vpn-instance-mytest-af-ipv4] multicast-domain share-group 224.1.1.1 binding mtunnel 0
```

8.6.14 multicast-domain source-interface

Function

The **multicast-domain source-interface** command allows an MTI to use an IP address of a default interface.

The **undo multicast-domain source-interface** command restores the default setting.

By default, an MTI does not use an IP address of a default interface.

Format

multicast-domain source-interface *interface-type interface-number*

undo multicast-domain source-interface

Parameters

Parameter	Description	Value
interface-type interface-number	Specifies the type and number of an interface. **NOTE** To avoid frequent protocol changes caused by interface flapping, use the loopback interface address as the MTI address.	-

Views

System view, VPN IPv4 address family view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When a PE encapsulates VPN multicast packets, the MTI address is used as the multicast source address of the encapsulated public network multicast data

packets. You can run the **multicast-domain source-interface** command to configure the source interface whose address is referenced by the MTI. This keeps the MTI address consistent with the IP address of the interface on which IBGP neighbor relationships are established, which ensures that VPN multicast packets pass the RPF check.

Prerequisites

The multicast routing function has been enabled using the **multicast routing-enable** command in the VPN instance.

Precautions

If the **multicast-domain source-interface** command is run in the system view, the setting takes effect globally. The command run in the VPN IPv4 address family view takes precedence over that run in the system view. If the command is configured in the system view rather than the VPN IPv4 address family view, the setting in the system view takes effect.

A manually configured IP address on an MTI takes precedence over a default interface address specified using the **multicast-domain source-interface** command.

The source interface whose address is referenced by the MTI must be the interface on which public network IBGP neighbor relationships are established on the PE; otherwise, VPN multicast packets cannot pass the RPF check.

Example

Configure the MTI to use the IP address of the default interface named **loopback 1**.

```
<HUAWEI> system-view
[HUAWEI] ip vpn-instance mytest
[HUAWEI-vpn-instance-mytest] route-distinguisher 11:11
[HUAWEI-vpn-instance-mytest-af-ipv4] multicast routing-enable
[HUAWEI-vpn-instance-mytest-af-ipv4] multicast-domain source-interface loopback 1
```

8.6.15 multicast-domain switch-delay

Function

The **multicast-domain switch-delay** command specifies the delay for the switchover from the Share-MDT to Switch-MDT in a specified VPN instance.

The **undo multicast-domain switch-delay** command restores the default value of the delay.

By default, the delay for the switchover from the Share-MDT to Switch-MDT is 5 seconds.

Format

multicast-domain switch-delay *switch-delay*

undo multicast-domain switch-delay

Parameters

Parameter	Description	Value
switch-delay	Specifies the delay for the switchover from the Share-MDT to Switch-MDT.	The value of the delay is an integer that ranges from 3 to 60, in seconds.

Views

VPN instance view, VPN IPv4 address family view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In some cases, the forwarding rate of VPN multicast data packets fluctuates above and below the switchover threshold. To prevent frequent switchovers between the Share-MDT and Switch-MDT, configure a delay for the switchover from the Share-MDT to Switch-MDT. When detecting that the forwarding rate is higher than the switchover threshold, the system does not immediately perform the switchover but starts the Switch-Delay timer. Before the Switch-Delay timer expires, the system continues to detect the data forwarding rate. If the rate remains higher than the switchover threshold throughout the duration of the Switch-Delay timer, the transmission path of data packets is switched to the Switch-MDT; otherwise, the packets are still forwarded along the Share-MDT.

Prerequisites

The Share-Group has been configured using the **multicast-domain share-group binding** command in the VPN instance.

Precautions

During a switchover, there is a delay about 1 to 30 seconds from the time when the forwarding rate ranges to the time when the system starts the Switch-Delay timer. The delay is not included in the value of the Switch-Delay. Consequently, the total delay from the time when the forwarding rate of the data changes to the time when the system completes the switchover is 1-30 seconds longer than the Switch-Delay.

Example

Specify the delay for the switching to Switch-MDT to 20 seconds in VPN instance **mytest**.

```
<HUAWEI> system-view
[HUAWEI] ip vpn-instance mytest
[HUAWEI-vpn-instance-mytest] route-distinguisher 11:11
[HUAWEI-vpn-instance-mytest-af-ipv4] multicast routing-enable
[HUAWEI-vpn-instance-mytest-af-ipv4] multicast-domain share-group 224.1.1.1 binding mtunnel 0
[HUAWEI-vpn-instance-mytest-af-ipv4] multicast-domain switch-delay 20
```


8.6.16 multicast-domain switch-group-pool

Function

The **multicast-domain switch-group-pool** command specifies the conditions for the switchover from the Share-MDT to Switch-MDT and configures the Switch-Group-Pool in a specified VPN instance.

The **undo multicast-domain switch-group-pool** command restores the default configuration.

By default, the Switch-Group-Pool is not specified, and the switchover to the Switch-MDT is not performed.

Format

multicast-domain switch-group-pool *switch-group-pool* { *network-mask* | *network-mask-length* } [**threshold** *threshold-value* | **acl** *advanced-acl-number*] *

undo multicast-domain switch-group-pool

Parameters

Parameter	Description	Value
switch-group-pool	Specifies the start address of the Switch-Group-Pool.	The value is in dotted decimal notation and ranges from 224.0.1.0 to 239.255.255.255.
network-mask	Specifies the mask of a Switch-Group-Pool address.	The value is in dotted decimal notation and ranges from 255.255.255.0 to 255.255.255.255.
network-mask-length	Specifies the mask length of a Switch-Group-Pool address.	The value is an integer that ranges from 24 to 32; that is, the range of the group address in the Switch-MDT Switch-Group-Pool is from 0 to 255.
threshold *threshold-value*	Specifies the switchover threshold.	The value is an integer that ranges from 0 to 4194304, in kbit/s. By default, it is 0.
acl *advanced-acl-number*	Specifies the (S, G) entry which the Switch-Group-Pool takes effect on. *advanced-acl-number* indicates the advanced ACL number. If the ACL is not specified, the Switch-Group-Pool takes effect on all (S, G) entries.	The value is an integer that ranges from 3000 to 3999.

Views

VPN instance view, VPN IPv4 address family view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Between the PE connected to the VPN receivers and the PE connected to the VPN multicast source, a special Switch-MDT is set up for the high-speed VPN multicast data packets flowing into the public network. The multicast data flow can be switched from the Share-MDT to the Switch-MDT. Therefore, on-demand multicast can be realized. This prevents data from be flooded in the public network when the Share-MDT is used to transmit VPN multicast data packets.

Prerequisites

A Share-Group has been configured using the **multicast-domain share-group binding** command.

Follow-up Procedure

In some cases, the forwarding rate of VPN multicast data packets fluctuates above and below the switchover threshold. Configure a delay for the switchover from the Share-MDT to Switch-MDT using the **multicast-domain switch-delay** command. If the rate remains higher than the switchover threshold throughout the duration of the Switch-Delay timer, the transmission path of data packets is switched to the Switch-MDT; otherwise, the packets are still forwarded along the Share-MDT.

Precautions

On a PE, the address ranges defined by the Switch-Group-Pool cannot overlap for VPN instances.

From the time when data forwarding rate changes to the time when the system starts the switch-delay timer, there is a delay of 1 to 30 seconds because of necessary traffic calculation and protocol processing. In actual switchover, the delay is longer than the switch-delay period by 1 to 30 seconds.

Example

Configure the Switch-Group-Pool of VPN instance named **mytest** to range from 225.2.2.1 to 225.2.2.15.

```
<HUAWEI> system-view
[HUAWEI] ip vpn-instance mytest
[HUAWEI-vpn-instance-mytest] route-distinguisher 11:11
[HUAWEI-vpn-instance-mytest-af-ipv4] multicast routing-enable
[HUAWEI-vpn-instance-mytest-af-ipv4] multicast-domain share-group 224.1.1.1 binding mtunnel 0
[HUAWEI-vpn-instance-mytest-af-ipv4] multicast-domain switch-group-pool 225.2.2.1 28
```


8.6.17 multicast-domain switch-without-register

Function

The **multicast-domain switch-without-register** command disables the source PE from sending null Register messages to the RP to establish the SPT on the public network before the Switch-Group address is used to encapsulate VPN data.

The **undo multicast-domain switch-without-register** command restores the default setting.

By default, before the Switch-Group address is used to encapsulate VPN data, the source PE sends null Register messages to the RP and establishes the SPT on the public network.

Format

multicast-domain switch-without-register

undo multicast-domain switch-without-register

Parameters

None

Views

VPN instance view, VPN IPv4 address family view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In previous implementation, if the Switch-Group address is in the ASM address range, when the SPT switchover occurs on the multicast tunnel of the public network, the source PE sends the switchover message to all receiver PEs. After receiving the switchover message, these receiver PEs send the (*, G) Join messages to the RP of the public network to establish the RPT. When the Switch-Group address is used in the VPN to encapsulate multicast data, the public network side of the source PE receives the data forwarded from the VPN based on the Switch-Group address. Then the forwarding entries are created on the source PE, and the source PE encapsulates the data in the Register messages which are sent to the RP of the public network. Then, the RP decapsulates the Register messages, and sends the data to the receiver PEs. Finally, the receiver PEs trigger the SPT switchover towards the source PE. In this manner, the SPT is established on the public network.

When there are many entries involved in SPT switchovers, the speed of sending Register messages is reduced. As a result, sending the first Register message to the RP takes a long time for certain entries, and establishing the SPT on the public

network is delayed. In addition, in the process of establishing the SPT on the public network, multicast services are interrupted and certain VPN data may also be discarded, leading to the service interruption on the user end.

To address the preceding problems, disable the source PE from sending the null Register message to the RP and establishing a public network SPT before the Switch-Group address is used to encapsulate VPN data.

Prerequisites

A Share-Group has been configured using the **multicast-domain share-group binding** command.

Configuration Impact

After the VPN data traffic exceeds the upper limit, the source PE uses the Switch-Group address to encapsulate data and sends the switchover message to the receiver PEs. If the Switch-Group address is allocated for the first time, when sending the switchover message, the source PE sends the Register message that is encapsulated with the VPN Hello message to the RP, and the RP forwards the Register message to the receiver PEs. Based on the received messages, the receiver PEs and the RP directly send the (S, G) Join messages to the source PE and establish the SPT on the public network in advance. In this manner, when the public network tunnel is switched from the RPT to the SPT, the number of discarded multicast messages is reduced and the impact on multicast services is minimized.

Example

When the Switch-Group address is not used to encapsulate VPN data for mytest, configure the source PE to send the null Register message to the RP to establish the SPT on the public network.

```
<HUAWEI> system-view
[HUAWEI] ip vpn-instance mytest
[HUAWEI-vpn-instance-mytest] route-distinguisher 11:11
[HUAWEI-vpn-instance-mytest-af-ipv4] multicast routing-enable
[HUAWEI-vpn-instance-mytest-af-ipv4] multicast-domain share-group 224.1.1.1 binding mtunnel 0
[HUAWEI-vpn-instance-mytest-af-ipv4] multicast-domain switch-without-register
```

8.6.18 reset multicast-domain control-message counters

Function

The **reset multicast-domain control-message counters** command clears statistics about sent and received MDT switch messages in a specified VPN instance or all VPN instances.

Format

reset multicast-domain { **vpn-instance** *vpn-instance-name* | **all-instance** } **control-message counters**

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Clears statistics about sent and received MDT switch messages in a specified VPN instance. The parameter *vpn-instance-name* specifies the name of an existing VPN instance on the device.	The value must be an existing VPN instance name.
all-instance	Clears statistics about sent and received MDT switch messages in all VPN instances.	-

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

If a fault occurs on a multicast VPN network, you need to check whether MDT switch messages are properly sent and received. If the current device already records a large number of statistics about MDT switch messages, you can run the **reset multicast-domain control-message counters** command to clear statistics about sent and received messages in a specified VPN instance or all VPN instances and then run the **display multicast-domain control-message counters** command to check whether the count of MDT switch messages increases, which helps fault location.

Precautions

Running the **reset multicast-domain control-message counters** command will clear all statistics about MDT switch messages. Therefore, exercise caution before using this command.

Example

Clear statistics about sent and received MDT switch messages in VPN instance **red**.

```
<HUAWEI> reset multicast-domain vpn-instance red control-message counters
```

8.6.19 service type (Eth-trunk interface view)

Function

The **service type multicast-tunnel** command configures an Eth-trunk interface as a multicast loopback interface.

The **undo service type multicast-tunnel** command cancels the configuration.

By default, an Eth-trunk interface is not configured as a multicast loopback interface.

Format

service type multicast-tunnel

undo service type multicast-tunnel

Parameters

None

Views

Eth-trunk interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The switch can receive the VPN multicast packets and use GRE to encapsulate them only after a multicast loopback interface has been configured.

Follow-up Procedure

Configure member interfaces of the multicast loopback interface using the **trunkport** command.

Precautions

- After you configure an interface as a multicast loopback interface, the switch automatically disables STP on this interface. The interface then does not support STP configuration commands. After the multicast loopback interface configuration is cancelled, the switch automatically enables STP on the interface.
- On the switch, only one Eth-Trunk interface can function as the multicast loopback interface. All VPN multicast packets are encapsulated on this interface into public network multicast data packets.
- The configurations allowed on an Eth-Trunk to be configured as a loopback interface include **description**, **enable snmp trap updown**, **jumboframe enable**, **mixed-rate link enable**, **qos phb marking enable**, **set flow-stat interval**, **shutdown**, **local-preference enable**, **traffic-policy (interface view)**, and **trust**. If other configurations exist on the Eth-Trunk, the Eth-Trunk cannot be configured as a loopback interface.
- After an Eth-Trunk is configured as a loopback interface, the Eth-Trunk supports only the following configurations: **authentication open ucl-policy enable**, **description**, **enable snmp trap updown**, **jumboframe enable**, **mixed-rate link enable**, **qos phb marking enable**, **set flow-stat interval**, **shutdown**, **local-preference enable**, **statistic enable (interface view)**, **traffic-policy (interface view)**, **vcmp disable**, and **trust**.

- Before disabling an Eth-Trunk interface from working as the multicast loopback interface, delete all member interfaces of the Eth-Trunk interface.
- If "Warning: ACL resources are insufficient when the physical interface is added to the multicast loopback interface, so the multicast VPN function may be abnormal." is displayed when you add a physical interface to a multicast loopback interface, resources on the multicast loopback interface are occupied by other services. To ensure normal running of services, delete this physical interface from the multicast loopback interface or delete unnecessary configurations, for example, unnecessary traffic policies.
- If an Eth-Trunk has been configured as a multicast VPN loopback interface, do not use the MIB to perform other service configuration on the Eth-Trunk. Otherwise, the multicast VPN loopback interface will become invalid or the service configuration issued by the MIB may not take effect.

Example

Configure Eth-Trunk 1 as a multicast loopback interface.

```
<HUAWEI> system-view
[HUAWEI] interface Eth-Trunk 1
[HUAWEI-Eth-Trunk1] service type multicast-tunnel
```

8.6.20 set multicast tunnel enhanced

Function

The **set multicast tunnel enhanced** command allows an Eth-Trunk that works as a multicast VPN loopback interface to have member interfaces from different cards.

The **undo set multicast tunnel enhanced** command forbids an Eth-Trunk that works as a multicast VPN loopback interface to have member interfaces from different cards.

By default, an Eth-Trunk that works as a multicast VPN loopback interface cannot have member interfaces from different cards.

Format

set multicast tunnel enhanced

undo set multicast tunnel enhanced

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When an Eth-Trunk that works as a multicast VPN loopback interface have member interfaces from different member switches in a stack system, multicast VPN services can function properly if the switch where a member interface is located fails. This improves device reliability.

Follow-up Procedure

Run the **service type multicast-tunnel** command to configure an Eth-Trunk as a multicast VPN loopback interface.

Configuration Impact

After the **set multicast tunnel enhanced** command is executed, the number of ACLs for multicast VPN will increase if the Eth-Trunk that functions as a multicast VPN loopback interface contains more than one member interface from a device. The number of ACLs equals to the number of interfaces on a device configured as the member interfaces of an Eth-Trunk functioning as a multicast VPN loopback interface multiplied by the number of Mtunnel outbound interfaces for accessing the public network. For example, if two interfaces on a device are configured as member interfaces of the Eth-Trunk functioning as a multicast VPN loopback interface, and if the device is configured with four Mtunnel outbound interfaces for accessing the public network, a total of eight (2*4) ACLs will be used by multicast VPN services. If there are insufficient ACL resources, multicast VPN services cannot run properly.

Precautions

A multicast VPN loopback interface cannot be configured together with the **set multicast tunnel enhanced** and **undo set multicast tunnel enhanced** commands.

Example

Configure the Eth-Trunk that works as a multicast VPN loopback interface to allow member ports from different cards.

```
<HUAWEI> system-view
[HUAWEI] set multicast tunnel enhanced
```

8.7 IPv4 Multicast Route Management Commands

8.7.1 Command Support

Product	Support
S1700	Not supported.
S300	Supported.
S500	Supported.

Product	Support
S2700	Supported.
S5700	Supported except S5731-L and S5731S-L.
S6700	Supported.

NOTE

Only S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support the multicast multi-instance feature.

8.7.2 display default-parameter mrm

Function

The **display default-parameter mrm** command displays the default configurations for multicast routing management (MRM).

Format

display default-parameter mrm

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

This command displays only the default configurations, regardless of whether MRM parameters are changed. Therefore, you can use this command to check which parameters have been modified.

Example

Display default configurations for MRM.

```
<HUAWEI> display default-parameter mrm
  System View Default Configurations:
  ----------------------------------
  Load splitting rule: disabled
  Load-splitting-timer: 1800 s
  Route selection rule: preference-preferred
```



```
Multi-topology: disabled

Interface View Default Configurations:
--------------------------------------
Minimum TTL: 1
Reject inbound data: disabled
Reject outbound data: disabled
Multicast load-splitting weight: 1
```

Table 8-89 Description of the **display default-parameter mrm** command output

Item	Description
System View Default Configurations	Default configurations for multicast routing management (MRM) in the system view.
Load splitting rule	Whether multicast load splitting is configured. By default, multicast load splitting is not configured. To configure multicast load splitting, run the **multicast load-splitting** command.
Load-splitting-timer	Default value of the multicast load splitting balancing timer. By default, the value is 1800s. You can run the **multicast load-splitting-timer** command to set the value of the multicast load splitting balancing timer.
Route selection rule	RPF route selection rule. By default, RPF route selection is based on the preference of the routing protocol.
Interface View Default Configurations	Default configurations for multicast routing management (MRM) in the interface view.
Minimum TTL	Minimum TTL value for multicast packet forwarding.
Reject inbound data	Whether the interface is disabled from receiving multicast packets.
Reject outbound data	Whether the interface is disabled from forwarding multicast packets.
Multicast load-splitting weight	Multicast load splitting weight of the interface. By default, the multicast load splitting weight of an interface is 1. You can run the **multicast load-splitting weight** command to set the value of the multicast load splitting weight.

8.7.3 display migp routing-table

Function

The **display migp routing-table** command displays brief information about the MIGP routing table.

Format

display migp routing-table [*ip-address* [*mask-length* | *mask*]] [**verbose**]

Parameters

Parameter	Description	Value
ip-address	Specifies a destination IP address.	The address is in dotted decimal notation.
mask	Indicates a mask.	The mask is in dotted decimal notation.
mask-length	Specifies the length of the mask.	The value is a decimal integer ranging from 0 to 32.
verbose	Displays detailed information about active routes and inactive routes. If the parameter is not specified, only brief information about active routes is displayed.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

This command displays the MIGP routing table. You can specify parameters in the command to view specified routes.

Example

Display brief information about the MIGP routing table.

```
<HUAWEI> display migp routing-table
Route Flags: R - relay, D - download to fib, T - to vpn-instance
------------------------------------------------------------------------------
```



```
Routing Tables: MIGP
         Destinations : 4        Routes : 4

Destination/Mask    Proto  Pre  Cost      Flags NextHop         Interface

10.4.4.4/32         OSPF   10   3           10.0.1.1        Vlanif100
10.5.5.5/32         OSPF   10   4           10.0.1.1        Vlanif100
10.0.3.0/24         OSPF   10   3           10.0.1.1        Vlanif100
192.168.3.0/24      OSPF   10   4             10.0.1.1        Vlanif100
```

Table 8-90 Description of the **display migp routing-table** command output

Item	Description
Route Flags	Flag of a route: • R: indicates that the route is a recursive route. • D: indicates that the route is delivered to the FIB table. • T: indicates a route whose next hop belongs to a VPN instance.
Routing Tables: MIGP	MIGP routing table.
Destinations	Total number of destination networks or hosts.
Routes	Total number of routes.
Destination/Mask	Address and mask length of the destination network or host.
Proto	Routing protocol that learns a route.
Pre	Route preference.
Cost	Route cost.
Flags	Route flags in the header of the routing table.
NextHop	Next hop of a route.
Interface	Outbound interface to a reachable next hop.

Display detailed information about the MIGP routing table.

```
<HUAWEI> display migp routing-table verbose
Route Flags: R - relay, D - download to fib, T - to vpn-instance
------------------------------------------------------------------------------
Routing Table : MIGP
         Destinations : 5        Routes : 5


Destination: 10.4.4.4/32
    Protocol: ISIS            Process ID: 1
  Preference: 15                    Cost: 20
     NextHop: 10.0.1.1         Interface: Vlanif100
```



```
      State: Active Adv          Age: 00h34m26s

Destination: 10.5.5.5/32
    Protocol: ISIS          Process ID: 1
  Preference: 15                  Cost: 30
     NextHop: 10.0.1.1       Interface: Vlanif100
       State: Active Adv          Age: 00h34m26s

Destination: 10.0.2.0/24
    Protocol: ISIS          Process ID: 1
  Preference: 15                  Cost: 20
     NextHop: 10.0.1.1       Interface: Vlanif100
       State: Active Adv          Age: 00h34m26s

Destination: 10.0.3.0/24
    Protocol: ISIS          Process ID: 1
  Preference: 15                  Cost: 30
     NextHop: 10.0.1.1       Interface: Vlanif100
       State: Active Adv          Age: 00h34m27s

Destination: 192.168.3.0/24
    Protocol: ISIS          Process ID: 1
  Preference: 15                  Cost: 40
     NextHop: 10.0.1.1       Interface: Vlanif100
       State: Active Adv          Age: 00h34m28s
```

Table 8-91 Description of the **display migp routing-table** verbose command output

Item	Description
Destination	Address and mask length of the destination network or host.
Protocol	Routing protocol that learns a route.
Process ID	Process ID of the routing protocol.
Preference	Preference of a route.
Cost	Indicates the route cost.
NextHop	Next hop of a route.
Interface	Outbound interface of a route.

Item	Description
State:	Status of routes, which can be: • Active: indicates routes in the Active state. • Invalid: indicates invalid routes. • Inactive: indicates routes in the Inactive state. • NoAdv: indicates routes that cannot be advertised. • Adv: indicates routes that can be advertised. • Del: indicates routes to be deleted. • GotQ: indicates routes that are relayed successfully. • WaitQ: indicates routes that are not relayed successfully yet. • Stale: indicates routes with the Stale flag. The routes are used in GR.
Age	Time that elapsed since a route is generated.

8.7.4 display migp routing-table statistics

Function

The **display migp routing-table statistics** command displays the statistics about the MIGP routing table.

Format

display migp routing-table statistics

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Integrated route statistics contain the total number of routes added or deleted through protocols and the total number of active or inactive routes with deletion flags but are not deleted.

Example

Display the statistics about routes in the MIGP routing table.

```
<HUAWEI> display migp routing-table statistics
Proto     total      active      added       deleted      freed
          routes     routes      routes      routes       routes
OSPF      0          0           0           0            0
IS-IS     5          5           45          40           40
Total     5          5           45          40           40
```

Table 8-92 Description of the **display migp routing-table statistics** command output

Item	Description
Proto	Routing protocol.
total routes	Total number of routes in the current routing table.
active routes	Number of active routes in the routing table.
added routes	Number of routes (active and inactive) added to the routing table.
deleted routes	Number of routes deleted from the routing table.
freed routes	Number of released routes that are deleted permanently from the routing table.

8.7.5 display mrt routing-table

Function

The **display mrt routing-table** command displays MRT routes.

Format

display mrt routing-table [**vpn-instance** *vpn-instance-name*] [*ip-address* [*mask* | *mask-length*]] [**verbose**]

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Specifies a VPN instance. *vpn-instance-name* specifies the name of the VPN instance.	The value must be an existing VPN instance name.
ip-address	Specifies a destination IP address.	The address is in dotted decimal notation.
mask	Specifies mask.	The mask is in dotted decimal notation.
mask-length	Specifies mask length.	It is an integer ranging from 0 to 32.
verbose	Displays detailed information about active and inactive routes. If the parameter **verbose** is not specified, detailed information about active routes is displayed.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can specify different parameters to view specific routing information.

Example

Display information about all MRT routes.

```
<HUAWEI> display mrt routing-table
Route Flags: R - relay, D - download to fib, T - to vpn-instance
------------------------------------------------------------------------------
Routing Tables: MRT
         Destinations : 1        Routes : 1

Destination/Mask  Proto  Pre  Cost  Flags NextHop  Interface

 10.5.5.1/32     MSR    255     0     R   10.1.1.1  Vlanif100
```


Table 8-93 Description of the **display mrt routing-table** command output

Item	Description
Route Flags	Flag of a route: ● R: indicates that the route is a recursive route. ● D: indicates that the route is delivered to the FIB table. ● T: indicates a route whose next hop belongs to a VPN instance.
Routing Tables: MRT	IMRT routing table.
Destinations	Total number of destination networks or hosts.
Routes	Total number of routes.
Destination/Mask	Address and mask length of the destination network or host.
Proto	Protocol that learns a route.
Pre	Route preference.
Cost	Route cost.
Flags	Route flags in the header of the routing table.
NextHop	Next hop of a route.
Interface	Outbound interface to a reachable next hop.

Display the detailed information of the specified routes.

```
<HUAWEI> display mrt routing-table 10.12.12.12 verbose
Route Flags: R - relay, D - download to fib, T - to vpn-instance
------------------------------------------------------------------------------
Routing Table : MRT
Summary Count : 1

Destination: 10.12.12.12/32
     Protocol: MSR            Process ID: 0
   Preference: 1                  Cost: 0
      NextHop: 10.11.11.12      Neighbour: 0.0.0.0
        State: Active Adv Relied      Age: 00h04m49s
          Tag: 0                 Priority: low
        Label: NULL              QoSInfo: 0x0
   IndirectID: 0x80000002
 RelayNextHop: 0.0.0.0            Interface: Vlanif100
     TunnelID: 0x0                Flags: R
```

Table 8-94 Description of the **display mrt routing-table verbose** command output

Item	Description
Routing Table: MRT	MRT routing table.

Item	Description
Summary Count	Number of the destination network and host.
Destination	Address and mask length of the destination network or host.
Protocol	Routing protocol that learns a route.
Process ID	Process ID of the routing protocol.
Preference	Route preference.
Cost	Route cost.
NextHop	Next hop of a route.
Neighbour	Address of the neighbor.
State	Status of routes: ● Active: indicates active routes. ● Invalid: indicates invalid routes. ● Inactive: indicates inactive routes. ● NoAdv: indicates the routes that cannot be advertised. ● Adv: indicates the routes that can be advertised. ● Del: indicates the routes to be deleted. ● Relied: indicates the route that finds the next hop and outbound interface or the route that finds the tunnel during packet forwarding. ● WaitQ: indicates the route that does not find the next hop or outbound interface or the route that does not find the tunnel. ● Stale: indicates the routes with the stale flag. The routes are used in GR.
Age	Time that elapsed since a route is generated.
Tag	Administrative tag for routes.
Priority	Priority of a route.
Label	MPLS label allocated to a route.
QoSInfo	QoS information.
IndirectID	ID of the indirect next hop.
RelayNextHop	Relay next hop.
Interface	Outbound interface through which the next hop is reachable.
TunnelID	Tunnel ID.

Item	Description
Flags	Route flags in the header of the routing table.

8.7.6 display mrt routing-table statistics

Function

The **display mrt routing-table statistics** command displays statistics about the MRT routes.

Format

display mrt routing-table [**vpn-instance** *vpn-instance-name*] **statistics**

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Specifies a VPN instance. *vpn-instance-name* specifies the name of the VPN instance.	The value must be an existing VPN instance name.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Route statistics include:

- Total number of routes that are added or deleted by the protocol
- Number of active or inactive routes that are tagged for deletion but not deleted

Example

Display statistics about routes in the MRT routing table.

```
<HUAWEI> display mrt routing-table statistics
Proto    total      active     added      deleted    freed
         routes     routes     routes     routes     routes
MSTATIC  1          0          1          0          0
```


Table 8-95 Description of the **display mrt routing-table statistics** command output

Item	Description
Proto	Routing protocol.
total routes	Total number of routes in the routing table.
active routes	Number of active routes in the routing table.
added routes	Number of active and inactive routes added in the routing table.
deleted routes	Number of routes to be deleted from the routing table.
freed routes	Number of routes that are permanently deleted from the routing table.

8.7.7 display mrt routing-table vpn-instance

Function

The **display mrt routing-table vpn-instance** command displays the MRT routing table of a VPN instance.

Format

display mrt routing-table vpn-instance *vpn-instance-name* [*ip-address* [*mask* | *mask-length*] [**longer-match**]] [**verbose**]

Parameters

Parameter	Description	Value
vpn-instance-name	Specifies a VPN instance. *vpn-instance-name* specifies the name of the VPN instance.	The value must be an existing VPN instance name.
ip-address	Specifies a destination IP address.	The address is in dotted decimal notation.
mask	Specifies mask.	The mask is in dotted decimal notation.
mask-length	Specifies mask length.	The value is a decimal integer that ranges from 0 to 32.
longer-match	Displays only routes that match the specified network or mask.	-
verbose	Displays detailed information about active and inactive routes.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can specify different parameters to view the specific routing information.

Example

Display the MRT routing table of the IPv4 VPN instance named vpn1.

```
<HUAWEI> display mrt routing-table vpn-instance vpn1
Route Flags: R - relay, D - download to fib
------------------------------------------------------------------------------
Routing Tables: MSR
         Destinations : 1        Routes : 1

Destination/Mask  Proto  Pre  Cost      Flags NextHop         Interface

 10.5.5.1/32      MSR    255  0           R   10.1.1.1        Vlanif100
```

Table 8-96 Description of the **display mrt routing-table vpn-instance** command output

Item	Description
Route Flags	Route flag that identifies the attribute of a route. • R: indicates an iterated route. • D: indicates that the route is downloaded to the FIB table.
Routing Tables: MSR	MRT routing table.
Destinations	Total number of destination networks or hosts.
Routes	Total number of routes.
Destination/Mask	Address and mask length of the destination network or host.
Proto	Protocol through which routes are learned.
Pre	Route preference.
Cost	Route cost.
Flags	Route flags in the header of the routing table.
NextHop	Next hop of a route.
Interface	Outbound interface to a reachable next hop.

8.7.8 display mtrace statistics

Function

The **display mtrace statistics** command displays statistics about multicast trace (Mtrace) packets.

Format

display mtrace statistics

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

To collect statistics about Mtrace traffic generated in a certain period, clear the original statistics.

Example

Display statistics about the current Mtrace traffic.

```
<HUAWEI> display mtrace statistics
Mtrace statistics:
 Type          Send        Receive       Invalid
 Query         10          5             0
 Request       20          4             0
 Response      3           7             1
```

Table 8-97 Description of the **display mtrace statistics** command output

Item	Description
Type	Indicates the types of Mtrace packets. The types are as follows: • Query: IGMP-Tracert-Query packets. • Request: IGMP-Tracert-Request packets. • Response: IGMP-Tracert-Response packets.
Send	Indicates the number of sent packets.
Receive	Indicates the number of received packets.
Invalid	Indicates the number of invalid packets.

8.7.9 display multicast boundary

Function

The **display multicast boundary** command displays the multicast boundary configured on an interface.

Format

display multicast [**vpn-instance** *vpn-instance-name* | **all-instance**] **boundary** [*group-address* [*mask* | *mask-length*]] [**interface** *interface-type interface-number*]

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Specifies a VPN instance. *vpn-instance-name* specifies the name of the VPN instance.	The value must be an existing VPN instance name.
all-instance	Specifies all the instances.	-
group-address	Specifies a multicast group address.	The address is in dotted decimal notation. The value ranges from 224.0.1.0 to 239.255.255.255.
mask	Specifies the mask of the multicast group address.	The mask is in dotted decimal notation.
mask-length	Specifies the mask length of the multicast group address.	The value is a decimal integer that ranges from 4 to 32.
interface *interface-type interface-number*	Specifies the type and the number of an interface. The parameter is used to specify an interface.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

This command enables you to check the boundary of a PIM-SM network. When some hosts cannot receive multicast data, you can use this command to check whether the problem is caused by multicast boundary configuration.

Example

Display the boundaries configured on all the interfaces.

```
<HUAWEI> display multicast boundary
Multicast boundary information
Total 1 Multicast IPv4 boundary
 Interface          Boundary
 Vlanif100           225.1.1.0/24
```

Table 8-98 Description of the **display multicast boundary** command output

Item	Description
Multicast boundary information of	multicast boundary information.
Total 1 Multicast IPv4 boundary	Total number of multicast boundaries configured on a switch.
Interface	Interface configured with a multicast boundary.
Boundary	Information about the multicast boundary address.

8.7.10 display multicast forwarding-table

Function

The **display multicast forwarding-table** command displays the multicast forwarding table.

Format

display multicast [**vpn-instance** *vpn-instance-name* | **all-instance**] **forwarding-table** [*group-address* [**mask** { *group-mask* | *group-mask-length* }] | *source-address* [**mask** { *source-mask* | *source-mask-length* }] | **incoming-interface** { *interface-type interface-number* | **register** } | **outgoing-interface** { **include** | **exclude** | **match** } { *interface-type interface-number* | **register** | **none** } | { **statistics** | **verbose** }] *

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Specifies a VPN instance. *vpn-instance-name* specifies the name of the VPN instance.	The value must be an existing VPN instance name.
all-instance	Indicates all the instances.	-
group-address	Specifies a multicast group address.	The address is in dotted decimal notation and ranges from 224.0.1.0 to 239.255.255.255.
mask	Specifies the mask of a multicast address or source address.	-
group-mask	Specifies the mask of the multicast group address.	The mask is in dotted decimal notation.
group-mask-length	Specifies the mask length of the multicast group address.	The value is a decimal integer that ranges from 4 to 32.
source-address	Specifies the mask of the multicast source address.	The mask is in dotted decimal notation.
source-mask	Specifies the mask of the multicast source address.	The mask is in dotted decimal notation.
source-mask-length	Specifies the mask length of the multicast source address.	The value is a decimal integer that ranges from 0 to 32.
incoming-interface	Indicates the inbound interface of a multicast forwarding entry.	-
interface-type interface-number	Specifies the type and the number of an interface.	-
register	Indicates the register interface of PIM-SM.	-
outgoing-interface	Indicates the outbound interface of a multicast forwarding entry.	-

Parameter	Description	Value
include	Displays the (S, G) entry list that contains the specified downstream interface.	-
exclude	Displays the (S, G) entry list that does not contain the specified downstream interface.	-
match	Displays the (S, G) entry list that matches the specified interface and the (S, G) entries have only one specified interface.	-
none	Indicates that the downstream interface list is null.	-
verbose	Displays the detailed information about the multicast forwarding table.	-
statistics	Displays the statistics about the multicast forwarding table.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

During multicast routing and forwarding, routing information generated by multicast routing protocols is saved in a multicast routing table. The switch selects the optimal multicast routes from the routing table according to multicast routing and forwarding policies, and then delivers the selected multicast routes to the multicast forwarding table to guide multicast data forwarding.

You can use the **display multicast forwarding-table** command to check whether multicast forwarding entries have been generated and whether multicast data can be forwarded normally.

Example

Display the multicast forwarding table.

```
<HUAWEI> display multicast forwarding-table
Multicast Forwarding Table of VPN-Instance: public net
```



```
Total 1 entry, 1 matched

00001. (10.10.10.2, 225.0.0.1)
    MID: 0, Flags: ACT
    Uptime: 00:08:32, Timeout in: 00:03:26
    Incoming interface: Vlanif10
    List of 1 outgoing interfaces:
      1:  Vlanif20
          Activetime: 00:23:15
    Matched 154 packets(15378 bytes), Wrong If 0 packets
    Forwarded 154 packets(15378 bytes)
```

Table 8-99 Description of the **display multicast forwarding-table** command output

Item	Description
Multicast Forwarding Table of VPN-Instance: public net	VPN instance to which the multicast forwarding table corresponds. **public net** indicates the public network instance.
Total 1 entry, 1 matched	Total number of forwarding entries and number of eligible forwarding entries.
00001	Sequence number of the (S, G) entry.
(10.10.10.2, 225.0.0.1)	(S, G) entry in the multicast forwarding table.
MID	Uniquely identifies the multicast forwarding entry in the MFIB table. MID is used to rapidly search the multicast forwarding table.

Item	Description
Flags	Indicates the status flag of the (S, G) entry. ● ACT: indicates that an active event is triggered. ● DUM: indicates a dummy entry. ● MISS: indicates that the nocache time needs to be reported. ● DROP: indicates packet dropping. ● LTH: indicates that the traffic volume is below the threshold. ● DEL: indicates a deleted entry. ● RST: indicates that registration of the known timer is started. ● 2SYNC: indicates that the entry is contained in the MFIB table but it does not exist on the device. ● 2ADD: indicates that the entry existing on the device has not been added to the MFIB table. ● CLR: indicates that the MFIB table is resetting. ● L2FWD: indicates that the device forwards Layer 2 traffic in multicast mode. ● 2ACK: indicates that the VPN instance is waiting for the ACK message from the slave main control board. ● 2RSED: indicates that the entry is waiting for retransmission. ● BKCLR: indicates that the MFIB table on the slave main control board is resetting. ● 2DEL: indicates that the entry deleted from the device has not been removed from the MFIB table. ● PDEL: indicates that the entry does not exist on the device. ● A denotes addition; D denotes deletion; I denotes upstream update; R denotes RP update; P denotes PMBR; F denotes flag. ● S denotes SPT; E denotes encapsulation group update; US denotes status update; CS denotes status clearing.
Uptime	Period duration of the (S, G) entry.
Timeout in	Remaining time of the (S, G) entry.
Incoming interface	Upstream interface of the (S, G) entry.
List of 1 outgoing interfaces	Downstream interface list. The contents of the downstream interface list are as follows: ● Name and number of the outbound interface ● The existing time of outbound interface

Item	Description
Matched 154 packets(15378 bytes)	Number of multicast packets and bytes matching the (S, G) entry. **NOTE** Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S can provide the accurate counter values.
Wrong If 0 packets	Number of multicast packets matching the (S, G) entry but are not forwarded. **NOTE** Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S can provide the accurate counter values.
Forwarded 154 packets(15378 bytes)	Number of packets and bytes forwarded by the (S, G) entry. **NOTE** Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S can provide the accurate counter values.

8.7.11 display multicast forwarding-table optimization-mode configuration

Function

The **display multicast forwarding-table optimization-mode configuration** command displays the configuration of the optimization mode in which Layer 3 multicast forwarding entries are stored.

NOTE

Only the S6720-EI, S6735-S and S6720S-EI support this command.

Format

display multicast forwarding-table optimization-mode configuration [**slot** *slot-id*]

Parameters

Parameter	Description	Value
slot *slot-id*	*slot-id* specifies the slot that uses the multicast optimization mode. If no slot ID is specified, configurations of all slots are displayed.	The value is an integer and must be the slot ID of a running slot.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

This command is used to display the configuration of the optimization mode in which Layer 3 multicast forwarding entries are stored. The configuration helps you select a slot based on your storage requirement.

Example

Display the configuration of the optimization modes.

```
<HUAWEI> display multicast forwarding-table optimization-mode configuration
Multicast forwarding-table optimization mode :
Slot      Mode
-------------------------
2         Normal mode
4         Normal mode
5         Rich MCast mode
```

Table 8-100 Description of the **display multicast forwarding-table optimization-mode configuration** command output

Item	Description
Multicast forwarding-table optimization mode	When the multicast optimization mode is enabled.
slot	Slot ID.
mode	Storage Mode. The following storage modes are available: • Normal: The ARP cache table or ND cache table and multicast forwarding table share hardware resources, without affecting hardware resources allocated to the routing table. • Rich MCast mode: also known as multicast optimization mode. The system allocates hardware resources preferentially to the multicast forwarding table. The ARP/ND cache table and routing table share hardware resources.

8.7.12 display multicast routing-table

Function

The **display multicast routing-table** command displays information about a multicast routing table.

Format

display multicast [**vpn-instance** *vpn-instance-name* | **all-instance**] **routing-table** [*group-address* [**mask** { *group-mask* | *group-mask-length* }] | *source-address* [**mask** { *source-mask* | *source-mask-length* }] | **incoming-interface** { *interface-type interface-number* | **register** } | **outgoing-interface** { **include** | **exclude** | **match** } { *interface-type interface-number* | **register** | **none** }] * [**outgoing-interface-number** [*number*]]

display multicast routing-table [*group-address* [**mask** { *group-mask* | *group-mask-length* }] | *source-address* [**mask** { *source-mask* | *source-mask-length* }] | **incoming-interface** { *interface-type interface-number* | **register** } | **outgoing-interface** { **include** | **exclude** | **match** } { *interface-type interface-number* | **vpn-instance** *vpn-instance-name* | **register** | **none** }] * [**outgoing-interface-number** [*number*]]

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Specifies a VPN instance. *vpn-instance-name* specifies the name of the VPN instance.	The value must be an existing VPN instance name.
all-instance	Specifies all the instances.	-
group-address	Indicates the multicast group address.	The address is in dotted decimal notation. The value ranges from 224.0.1.0 to 239.255.255.255.
mask { *group-mask* | *group-mask-length* }	Indicates the mask of the multicast group address.	• *group-mask*: The address is in dotted decimal notation. The value ranges from 240.0.0.0 to 255.255.255.255. • *group-mask-length*: The value is an integer that ranges from 4 to 32
source-address	Indicates the multicast source address.	The address is in dotted decimal notation.

Parameter	Description	Value
mask { *source-mask* | *source-mask-length* }	Indicates the mask of the specified source address.	• *source-mask*: The address is in dotted decimal notation. The value ranges from 0.0.0.0 to 255.255.255.255. • *source-mask-length*: The value is an integer that ranges from 0 to 32
incoming-interface	Indicates the upstream interface of a multicast routing entry.	-
interface-type interface-number	Indicates the type and the number of an interface.	-
register	Indicates the register interface of a multicast routing entry.	-
outgoing-interface	Indicates the downstream interface of a multicast routing entry.	-
include	Indicates the (S, G) entries whose downstream interface list contains specified downstream interfaces.	-
exclude	Indicates the (S, G) entries whose downstream interface list does not contain specified downstream interfaces.	-
match	Indicates (S, G) entries whose the downstream interface list contains only one interface that is the same as a specified downstream interface.	-
none	Indicates that the downstream interface list is null.	-

Parameter	Description	Value
outgoing-interface-number	Indicates the number of downstream interfaces of multicast routing entries.	-
number	Specifies the number of downstream interfaces.	The value is an integer that ranges from 0 to 2048.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The **display multicast routing-table** command is used to display the information of a multicast routing table.

Example

Display the corresponding routing entry of a multicast group in the multicast routing table.

```
<HUAWEI> display multicast routing-table
Multicast routing table of VPN-Instance: public net
 Total 1 entry
 00001. (192.168.0.2, 227.0.0.1)
      Uptime: 00:00:28
      Upstream Interface: Vlanif10
      List of 2 downstream interfaces
        1:  Vlanif20
        2:  Vlanif30
```

Table 8-101 Description of the **display multicast routing-table** command output

Item	Description
Multicast routing table of VPN-Instance	VPN instance to which the multicast routing information corresponds. **public net** indicates the public network instance.
Total 1 entry	Number of eligible routing entries.
00001	Sequence number of the (S, G) entry.
(192.168.0.2, 227.0.0.1)	(S, G) entry in the multicast routing table.
Uptime	Time that elapsed since the (S, G) entry was generated.

Item	Description
Upstream Interface	Upstream interface of the (S, G) entry.
List of 2 downstream interfaces	Downstream interface list.

Display the number of downstream interfaces of the multicast routing entries.

```
<HUAWEI> display multicast routing-table outgoing-interface-number
Multicast routing table
 Total 2 entries

 00001. (10.1.1.22, 232.1.1.1)
      Uptime: 00:00:07
      Upstream Interface: Vlanif10
      List of 20 downstream interfaces

 00002. (10.1.1.22, 232.1.2.1)
      Uptime: 00:00:07
      Upstream Interface: Vlanif20
      List of 20 downstream interfaces
```

Table 8-102 Description of the display multicast routing-table outgoing-interface-number command output

Item	Description
List of 20 downstream interfaces	Number of downstream interfaces in multicast routing entries.

8.7.13 display multicast routing-table static

Function

The **display multicast routing-table static** command displays the multicast static routes.

Format

display multicast routing-table [**vpn-instance** *vpn-instance-name*] **static** [**config**] [*source-address* { *mask* | *mask-length* }]

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Specifies a VPN instance. *vpn-instance-name* specifies the name of the VPN instance.	The value must be an existing VPN instance name.
config	Displays the configuration of the multicast static routes.	-

Parameter	Description	Value
source-address	Specifies a multicast source address.	The address is in dotted decimal notation.
mask	Specifies the mask of the multicast source address.	The mask is in dotted decimal notation.
mask-length	Specifies the mask length of the multicast source address.	The value is an integer that ranges from 0 to 32.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

To check whether multicast RPF static routes are configured successfully, run the **display multicast routing-table static** command.

If the multicast static route configured on the local switch cannot be displayed, use the **ip rpf-route-static** command to configure multicast static routes.

Example

Display all multicast static routes on the switch.

```
<HUAWEI> display multicast routing-table static
Multicast Routing Table
Routes : 1

 Mroute 10.1.0.0/24
        Interface = Vlanif100       RPF Neighbor = 10.1.2.2
        Matched routing protocol = ospf, process-id = 100, Route-policy = none
        Preference = 1, Order = 1
 Running Configuration = ip rpf-route-static 10.1.0.0 24 ospf 100 10.1.2.2 order 1
```

Table 8-103 Description of the **display multicast routing-table static** command output

Item	Description
Multicast Routing Table	Multicast routing table.
Routes	Number of routes.
Mroute	Source address and mask length of a multicast route.
Interface	Outbound interface of the reachable multicast source.
RPF Neighbor	Neighbor IP address through which the source address is reachable.

Item	Description
Matched routing protocol	Matching unicast route type, which can be: • IS-IS • RIP • OSPF • BGP • Unicast static route
process-id	Process ID of a routing protocol.
Route-policy	Routing policy. The source address of a route must match the routing policy.
Preference	Preference of a route.
Order	Order of a route.
Running Configuration	Command line for configuring a static route.

8.7.14 display multicast rpf-info

Function

The **display multicast rpf-info** command displays the Reverse Path Forwarding (RPF) routes of a specified IPv4 multicast source or source/group.

Format

display multicast [**vpn-instance** *vpn-instance-name* | **all-instance**] **rpf-info** *source-address* [*group-address*] [**rpt** | **spt**]

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Specifies a VPN instance. *vpn-instance-name* specifies the name of the VPN instance.	The value must be an existing VPN instance name.
all-instance	Indicates all the instances.	-
source-address	Specifies the address of a multicast source, used to display the information of RPF routing corresponding to the source.	The address is in dotted decimal notation.

Parameter	Description	Value
group-address	Specifies the multicast group address, used to display the information of RPF routing corresponding to the source/group.	The address is in dotted decimal notation and ranges from 224.0.1.0 to 239.255.255.255.
rpt	Displays the RPF routing information corresponding to a specified source or source/group on the shared RP-tree.	-
spt	Displays the RPF routing information corresponding to a specified source or source/group on the shortest path tree.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The RPF route with the *source-address* as the destination address is an optimal route selected from unicast routes, multicast static routes, MBGP routes, and MIGP routes. You can use the **display multicast rpf-info** command to check the RPF route to the specified source or source-group.

Example

Display all RPF routes to the source address 192.168.0.1.

```
<HUAWEI> display multicast rpf-info 192.168.0.1
 VPN-Instance: public net
 RPF information about source: 192.168.0.1
    RPF interface: Vlanif100, RPF neighbor: 10.1.5.2
    Referenced route/mask: 192.168.0.0/24
    Referenced route type: unicast
    Route selection rule: preference-preferred
    Load splitting rule: disable
```

Table 8-104 Description of the **display multicast rpf-info** command output

Item	Description
RPF information about source	Multicast source to which the multicast RPF path belongs.
RPF interface	RPF interface.
RPF neighbor	RPF neighbor.
Referenced route/mask	Referenced route and its mask.

Item	Description
Referenced route type	Referenced route types: • unicast: unicast routes • MBGP: MBGP routes • mstatic: multicast static routes • MIGP: MIGP routes
Route selection rule	RPF route selection rules: • preference-preferred: selecting routes based on the preference of the routing protocols • longest-match: selecting routes based on the longest matching rule
Load splitting rule	Load splitting rules: • disable: load splitting disabled. • balance-preferred: load balancing preferred. • stable-preferred: stable-preferred load splitting. • source: load splitting based on source addresses. • group: load splitting based on group addresses. • source-group: load splitting based source and group addresses.

8.7.15 ip rpf-route-static

Function

The **ip rpf-route-static** command configures a multicast static route.

The **undo ip rpf-route-static** command deletes a multicast static route.

By default, no multicast static route is configured.

Format

ip rpf-route-static [**vpn-instance** *vpn-instance-name*] *source-address* { *mask* | *mask-length* } [**isis** *process-id* | **ospf** *process-id* | **rip** *process-id* | **bgp** | **static**] [**route-policy** *route-policy-name*] { *interface-type interface-number* | *gateway-address* } [**preference** *preference*] [**order** *order-number*]

undo ip rpf-route-static [**vpn-instance** *vpn-instance-name*] { *source-address* { *mask* | *mask-length* } [**isis** *process-id* | **ospf** *process-id* | **rip** *process-id* | **bgp** | **static**] [**route-policy** *route-policy-name*] | **all** }

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Specifies a VPN instance. *vpn-instance-name* specifies the name of the VPN instance.	The value must be an existing VPN instance name.
source-address	Specifies the address of a multicast source.	The address is in dotted decimal notation.
mask	Indicates the address mask of the multicast source.	The address mask is in dotted decimal notation.
mask-length	Specifies the mask length of the multicast source address.	The value is a decimal integer that ranges from 0 to 32.
isis *process-id*	Specifies that matched routes must be generated by the IS-IS protocol. *process-id* indicates the IS-IS process ID.	The value is a decimal integer that ranges from 1 to 65535.
ospf *process-id*	Specifies that matched routes must be generated by the OSPF protocol. *process-id* indicates the OSPF process ID.	The value is a decimal integer that ranges from 1 to 65535.
rip *process-id*	Specifies that matched routes must be generated by the RIP protocol. *process-id* indicates the RIP process ID.	The value is a decimal integer that ranges from 1 to 65535.
bgp	Specifies that matched routes must be generated by the BGP protocol.	-
static	Specifies that matched routes must be static routes.	-
route-policy *route-policy-name*	Indicates the matching rule of multicast static routes. *route-policy-name* specifies the name of a route matching rule.	The name is a string of 1 to 40 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Parameter	Description	Value
interface-type interface-number	Specifies the type and the number of an interface, used to specify an interface.	-
gateway-address	Specifies the address of the gateway.	-
order *order-number*	Indicates the configuration order of routes in the same network segment.	The value is a decimal integer that ranges from 1 to 100.
preference *preference*	Indicates the preference of routes. The greater the value is, the lower the preference is.	The value is a decimal integer that ranges from 1 to 255. By default, it is 1.
all	Indicates all multicast static routes in the multicast static routing table.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A multicast static route specifies an RPF interface or RPF neighbor for multicast packets from a specified multicast source. You can configure a multicast static route to:

- Change an RPF route.

  If you want an interface to receive multicast data packets from a specified multicast source but the interface is not the RPF interface for the multicast source, configure a multicast static route to specify this interface as the RPF interface for the multicast source. When the switch receives multicast data packets from the multicast source, it performs an RPF check using the configured RPF route. Packets sent from the source to the switch through other interfaces fail the RPF check.
- Connect RPF routes.

  If the unicast route on a network segment is incomplete, multicast packets cannot be forwarded due to the lack of an RPF route. For example, when two adjacent devices run different routing protocols and the routing protocols do

not import routes from each other, packets cannot be forwarded between the two devices. In this case, you can configure RPF static routes on the devices. The devices can perform RPF checks using the specified RPF interfaces so that multicast packets can be forwarded successfully.

Precautions

- If you specify a protocol type in the **ip rpf-route-static** command, the switch compares the configured multicast static route with the unicast routes of the specified protocol. If protocol types of the optimal unicast route and the multicast static route are different, the switch selects the optimal unicast route as the RPF route.
- A multicast static route is identified by three elements: *source-address* { *mask* | *mask-length* }, protocol type, and *route-policy-name*. Two multicast static routes are considered different as long as one element has different values in the two routes. A maximum of eight multicast static routes can be configured on a network segment.
- If the next-hop interface of a multicast static route is a P2P interface, you can specify the next-hop interface in the command. If the next-hop interface is not a P2P interface, you must specify the next-hop address.
- A multicast static route may not take effect after you configure it using the **ip rpf-route-static**, because the specified interface is Down. After configuring a multicast static route, you are advised to run the **display multicast routing-table static** command to check whether the route is configured successfully and takes effect.

Example

Configure a multicast static route.

```
<HUAWEI> system-view
[HUAWEI] ip rpf-route-static 10.0.0.0 255.0.0.0 rip 1 route-policy map1 10.10.0.1
```

8.7.16 mtrace

Function

The **mtrace** command detects the multicast path or RPF path from a multicast source to the querier or to a destination host. The querier indicates the switch on which the **mtrace** command is executed.

Format

mtrace -gw *last-hop-router* **-r** *receiver* [**-g** *group*] [[**-mr** | **-ur** *resp-dest*] | **-a** *source-ip-address* | **-l** [[*stat-times*] [**-st** *stat-int*]] | **-m** *max-ttl* | **-q** *nqueries* | **-ts** *ttl* | **-tr** *ttl* | **-v** | **-w** *timeout* | **-vpn-instance** *vpn-instance-name*] * **source** *source-address*

mtrace -b -r *receiver* **-g** *group* [[**-mr** | **-ur** *resp-dest*] | **-a** *source-ip-address* | **-l** [[*stat-times*] [**-st** *stat-int*]] | **-m** *max-ttl* | **-q** *nqueries* | **-ts** *ttl* | **-tr** *ttl* | **-v** | **-w** *timeout* | **-vpn-instance** *vpn-instance-name*] * **source** *source-address*

mtrace -d -r *receiver* [**-g** *group*] [[**-mr** | **-ur** *resp-dest*] | **-a** *source-ip-address* | **-l** [[*stat-times*] [**-st** *stat-int*]] | **-m** *max-ttl* | **-q** *nqueries* | **-ts** *ttl* | **-tr** *ttl* | **-v** | **-w** *timeout* | **-vpn-instance** *vpn-instance-name*] * **source** *source-address*

mtrace -r *receiver* [**-g** *group*] [[**-mr** | **-ur** *resp-dest*] | **-l** [[*stat-times*] [**-st** *stat-int*]] | **-m** *max-ttl* | **-q** *nqueries* | **-ts** *ttl* | **-tr** *ttl* | **-v** | **-w** *timeout* | **-vpn-instance** *vpn-instance-name*] * **source** *source-address*

mtrace [**-g** *group*] [[**-mr** | **-ur** *resp-dest*] | **-l** [[*stat-times*] [**-st** *stat-int*]] | **-m** *max-ttl* | **-q** *nqueries* | **-ts** *ttl* | **-tr** *ttl* | **-v** | **-w** *timeout* | **-vpn-instance** *vpn-instance-name*] * **source** *source-address*

Parameters

Parameter	Description	Value
-l	Performs Mtrace tracking for multiple times, collects traffic statistics and rate, uses detailed display mode, and ignores the configuration of **-v**.	If **-l** is not specified, Mtrace tracking is performed once.
stat-times	Indicates the number of times for Mtrace tracking.	The value is an integer that ranges from 2 to 65535. If **-l** is specified while *stat-times* is not specified, Mtrace tracking stops after it is performed 65535 times.
-st *stat-int*	Sets the interval at which the rate is calculated during cyclic query.	The value is an integer that ranges from 10 to 60, in seconds. The default value is 10. To configure **-st**, configure **-l** first. In addition, the cyclic count must be greater than or equal to 2.
-m *max-ttl*	Specifies the maximum number of hops to be traced.	The value is an integer that ranges from 1 to 255. The default value is 255.
-mr	Indicates that the response address is specified as the traced multicast group address.	The **-mr** is applicable only when the querier resides in a multicast distribution tree.
-q *nqueries*	Sets the number of retry times of mtrace.	The value is an integer that ranges from 1 to 65535. The default value is 3.

Parameter	Description	Value
-tr *ttl*	Specifies the TTL value of the IGMP Tracert Response messages sent in multicast mode.	The value is an integer that ranges from 1 to 255. The default value is 30.
-ts *ttl*	Sets the maximum number of hops to be traced in hop-by-hop mode.	The value is an integer that ranges from 1 to 255. The default value is 30. When Mtrace in max-hop mode fails, Mtrace automatically enters the hop-by-hop mode. The number of hops increases by one each time a new hop is traced.
-ur *resp-dest*	Specifies the response address as a unicast address. The value of *resp-dest* must be a local interface address. **NOTE** If neither **-mr** nor **-ur** *resp-dest* is specified, multicast address 224.0.1.32 is used as the response address.	-
-v	Sets the detailed mode and exports time and statistics.	-
-vpn-instance *vpn-instance-name*	Specifies the name of a VPN instance.	The value must be an existing VPN instance name.
-w *timeout*	Specifies the timeout period to wait for an IGMP Tracert Response message.	The value is an integer that ranges from 1 to 60, in seconds. The default value is 3.
-g *group*	Specifies the multicast group address to be traced.	The address cannot be a reserved group address.
-gw *last-hop-router*	Specifies the last-hop switch address, which ensures that unicast packets can be transmitted between the querier and the last-hop switch. After this parameter is specified, the initiating mode of Mtrace is specified as last-hop.	-

Parameter	Description	Value
-d	Indicates that unicast packets can be transmitted between the querier and the destination host. After this parameter is specified, the initiating mode of Mtrace is specified as destination.	-
-r *receiver*	Specifies the destination host address.	The value is in dotted decimal notation.
-a *source-ip-address*	Specifies the source address of an IGMP Tracert Query message. The value of *source-ip-address* must be a local interface address. **NOTE** When you need to detect the multicast path or the RPF path from the multicast source to the querier, **-a** is not supported.	The value is in dotted decimal notation.
-b	Indicates that the querier is directly connected to the destination host, but whether the querier is the last-hop switch is unknown. After this parameter is specified, the initiating mode of Mtrace is specified as all-router. **NOTE** After a VPN or RPF is specified, the initiating mode of Mtrace cannot be specified as all-router.	-
source *source-address*	Specifies the multicast source address.	The value is in dotted decimal notation.

Views

All views

Default Level

0: Visit level

Usage Guidelines

Usage Scenario

During multicast troubleshooting and routine maintenance, you can run the **mtrace** command to collect traffic information for locating faulty nodes, which

helps reduce configuration errors, perform cyclic tracert, and collect statistics on multicast flow rates.

The **mtrace** command format varies according to the types of paths.

- **mtrace source** *source-address*: detects the RPF path from the multicast source to the querier.
- **mtrace -g** *group* **source** *source-address*: detects the multicast path from the multicast source to the querier.

  The corresponding (S, G) entry must exist on the querier.
- **mtrace** [**-gw** *last-hop-router* | **-d**] **-r** *receiver* **source** *source-address*: detects the RPF path from the multicast source to the destination host.
  - The querier is directly connected to the destination host, or the querier can ping the last-hop switch or detonation host in unicast mode.
  - When multiple switches are connected to the specified host, RPF paths from different switches can be different. You can specify the last-hop switch using **-gw** *last-hop-router* to uniquely define an RPF path.
- **mtrace** [**-b** | **-gw** *last-hop-router* | **-d**] **-r** *receiver* **-g** *group* **source** *source-address*: detects the multicast path from the multicast source to the destination host.

  The corresponding (S, G) entry must exist on the querier. In addition, one of the following conditions must be met:
  - The querier is directly connected to the destination host.
  - The querier can ping the last-hop switch or the destination host in unicast mode.
  - The querier resides in the multicast path from the multicast source to the destination host. For example, the querier is the first hop switch.

When running the **mtrace** [**-b** | **-gw** *last-hop-router* | **-d**] **-r** *receiver* **-g** *group* **source** *source-address* command to detect the multicast path from a multicast source to a destination host, specify **-gw** *last-hop-router*, **-b** or **-d**, which helps implement tracking quickly and accurately.

- **-b**: indicates that the querier is directly connected to the destination host.
- **-gw** *last-hop-router*: specifies the last-hop switch address. Unicast packets can be transmitted between the querier and the last-hop switch.
- **-d**: indicates that unicast packets can be transmitted between the querier and the destination host.
- If none of the preceding three parameters are specified, Mtrace fails unless the querier resides in the multicast path from the multicast source to the destination host.

Precautions

- According to draft-fenner-traceroute-ipm-01, the Router Alert option needs to be carried in the IGMP Tracert Query messages that are sent to the destination address in unicast mode and in the IGMP Tracert Response messages that sent in response in multicast mode. However, manufacturers have not reached an agreement on this issue. Packets sent from a Huawei switch carry the Router Alert option. If Huawei switches need to communicate with devices that do not support the Router Alert option, use **-gw** to specify the last-hop address and **-ur** to specify the unicast response address.

- The parameter **vpn-instance** is used on the PE to initiate a multicast VPN probe.
- If the destination address of an IGMP Tracert Response message is a multicast address, the device sends the message to all PIM-enabled interfaces (except the interface that receives the message). The message is then looped back on the ring network until the TTL value becomes 0, upon which time the message is discarded.

Example

- Detect the RPF path from a multicast source to the querier.

Detect the RPF path from the multicast source 10.1.0.1 to the querier 10.1.5.1.

```
<HUAWEI> mtrace source 10.1.0.1
 Press Ctrl+C to break multicast traceroute facility
 From the receiver(10.1.5.1), trace reverse path to source (10.1.0.1) according to RPF rules

 Num  Reverse-Path    FwdTTL Protocol
  0   10.1.5.1
 -1   10.1.5.1        1      PIM
 -2   10.1.2.1        1      PIM
  In maximum-hop mode, received the response message, and multicast traceroute finished.
```

Detect the RPF path from the multicast source 10.1.0.1 to the querier 10.1.5.1. The unicast response address is 10.1.5.1, and the maximum number of hops to be traced in hop-by-hop mode is 2.

```
<HUAWEI>mtrace -ur 10.1.5.1 -ts 2 source 10.1.0.1
 Press Ctrl+C to break multicast traceroute facility
 From the receiver(10.1.5.1), trace reverse path to source (10.1.0.1) accordin
g to RPF rules *  *  *
 Switch from max hop mode to hop-by-hop mode
 In hop-by-hop mode, current probe hops is: 1
 Num  Reverse-Path    FwdTTL Protocol
  0   10.1.5.1
 -1   10.1.5.1        1      PIM
 In hop-by-hop mode, current probe hops is: 2
 Num  Reverse-Path    FwdTTL Protocol
  0   10.1.5.1
 -1   10.1.5.1        1      PIM
 -2   10.1.2.1        1      PIM
  In hop-by-hop mode, the current trace hops is equal to the specified max hops,
 hops is 2,and multicast traceroute finished.
```

- Detect the multicast path from a multicast source to the querier.

Detect the multicast path from the multicast source 10.1.0.1 to the querier 10.1.5.1. The group address is 225.0.0.1, the cyclic count is 2, and the interval at which the rate is calculated is 10s.

```
<HUAWEI> mtrace -g 225.0.0.1 -l 2 -st 10 source 10.1.0.1
 Press Ctrl+C to break multicast traceroute facility
 From the receiver(10.1.5.1), trace (10.1.0.1, 225.0.0.1)'s reverse path according to multicast routing-table
 In calculating-rate mode, current statistic times is: 1

 -1 10.1.5.1
   Incoming Interface Address: 10.1.5.1 Input packets rate: 0
   Outgoing Interface Address: 0.0.0.0 Output packets rate: 0xffffffff
   Forwarding Cache (10.1.0.1, 225.0.0.1) Forwarding packets rate: 0

 -2 10.1.2.1
   Incoming Interface Address: 10.1.2.1 Input packets rate: 0
   Outgoing Interface Address: 10.1.5.2 Output packets rate: 0
   Forwarding Cache (10.1.0.1, 225.0.0.1) Forwarding packets rate: 0
```



```
-3 10.1.0.1
  Incoming Interface Address: 10.1.0.1 Input packets rate: 0
  Outgoing Interface Address: 10.1.2.2 Output packets rate: 0
  Forwarding Cache (10.1.0.1, 225.0.0.1) Forwarding packets rate: 0
**********************************************************
 In calculating-rate mode, reach the demanded number of statistic,and multicast
 traceroute finished.
```

- Detect the RPF path from the multicast source to the destination host.

Detect the RPF path from the multicast source 10.1.0.1 to the destination host 10.1.6.4. The last hop address is 10.1.6.3, unicast packets can be transmitted, and the time and statistics are displayed in detail.

```
<HUAWEI> mtrace -gw 10.1.6.3 -r 10.1.6.4 -v source 10.1.0.1
 Press Ctrl+C to break multicast traceroute facility
 From the receiver(10.1.6.4), trace reverse path to source (10.1.0.1) according to RPF rules

 Num  Reverse-Path    FwdTTL Protocol
  0   10.1.6.4
 -1   10.1.5.1        1      PIM
  Incoming Interface Address: 10.1.5.1
  Outgoing Interface Address: 10.1.6.3
  Previous-Hop Router Address: 10.1.5.2
  Input packet count on incoming interface: 0
  Output packet count on outgoing interface: 0
  Total number of packets for this source-group pair: 0xffffffff
  Forwarding TTL: 1
  Forwarding Code: NO_ERROR
 -2   10.1.2.1        1      PIM
  Incoming Interface Address: 10.1.2.1
  Outgoing Interface Address: 10.1.5.2
  Previous-Hop Router Address: 10.1.2.2
  Input packet count on incoming interface: 0
  Output packet count on outgoing interface: 0
  Total number of packets for this source-group pair: 0xffffffff
  Forwarding TTL: 1
  Forwarding Code: NO_ERROR
 -3   10.1.0.1        1      PIM
  Incoming Interface Address: 10.1.0.1
  Outgoing Interface Address: 10.1.2.2
  Previous-Hop Router Address: 0.0.0.0
  Input packet count on incoming interface: 0
  Output packet count on outgoing interface: 0
  Total number of packets for this source-group pair: 0xffffffff
  Forwarding TTL: 1
  Forwarding Code: NO_ERROR
 In maximum-hop mode, received the response message, and multicast traceroute finished.
```

- Detect the multicast path from the multicast source to the destination host.

Detect the multicast path from the multicast source 10.1.0.1 to the destination 225.0.0.1. The destination host address is 10.1.6.4, the querier is directly connected to the destination host, the response address is the default value 224.0.1.32, and the TTL value of a Response packet is 5.

```
<HUAWEI> mtrace -b -r 10.1.6.4 -g 225.0.0.1 -tr 5 source 10.1.0.1
 Press Ctrl+C to break multicast traceroute facility
 From the receiver(10.1.6.4), trace (10.1.0.1, 225.0.0.1)'s reverse path according to multicast routing-table

 Num  Reverse-Path    FwdTTL Protocol
  0   10.1.6.4
 -1   10.1.5.1        1      PIM
 -2   10.1.2.1        1      PIM
 -3   10.1.0.1        1      PIM
 In maximum-hop mode, received the response message, and multicast traceroute finished.
```

Detect the multicast path from the multicast source 10.1.0.1 to the destination 225.0.0.1. The destination host address is 10.1.6.4, the last hop address is 10.1.6.3,

unicast packets are reachable, the number of cyclic times is 2, and the interval at which the rate is calculated is 12s.

```
<HUAWEI> mtrace -gw 10.1.6.3 -r 10.1.6.4 -g 225.0.0.1 -l 2 -st 12 source 10.1.0.1
 Press Ctrl+C to break multicast traceroute facility
 From the receiver(10.1.6.4), trace (10.1.0.1, 225.0.0.1)'s reverse path according to multicast routing-table
 In calculating-rate mode, current statistic times is: 1

 -1 10.1.5.1
   Incoming Interface Address: 10.1.5.1 Input packets rate: 0
   Outgoing Interface Address: 10.1.6.3 Output packets rate: 0
   Forwarding Cache (10.1.0.1, 225.0.0.1) Forwarding packets rate: 0

 -2 10.1.2.1
   Incoming Interface Address: 10.1.2.1 Input packets rate: 0
   Outgoing Interface Address: 10.1.5.2 Output packets rate: 0
   Forwarding Cache (10.1.0.1, 225.0.0.1) Forwarding packets rate: 0

 -3 10.1.0.1
   Incoming Interface Address: 10.1.0.1 Input packets rate: 0
   Outgoing Interface Address: 10.1.2.2 Output packets rate: 0
   Forwarding Cache (10.1.0.1, 225.0.0.1) Forwarding packets rate: 0
 ************************************************************
  In calculating-rate mode, reach the demanded number of statistic, and multicast
 traceroute finished.
```

Table 8-105 Description of the **mtrace** command output

Item	Description
Press Ctrl+C to break multicast traceroute facility	The ongoing Mtrace test is terminated after you press **Ctrl+C**.
From the receiver (10.1.6.4), trace reverse path to source (10.1.0.1) according to RPF rules	The RPF path from destination host 10.1.6.4 to multicast source 10.1.0.1 is detected.
From the receiver (10.1.6.4), trace (10.1.0.1, 225.0.0.1)'s reverse path according to multicast routing-table	The transmission path of multicast data (10.1.0.1, 225.0.0.1) from the destination host 10.1.6.4 to the source is tested.
Num	Number of traced hops.
Reverse-Path	Reverse path of multicast traffic.
FwdTTL	Minimum TTL value for multicast packet forwarding.
Protocol	Multicast routing protocol used on the switch.
-1 10.1.5.1 1 PIM	The address of the last hop is 10.1.5.1, the minimum TTL value for multicast forwarding is 1, and the multicast routing protocol used on the switch is PIM.
In calculating-rate mode, current statistic times is: 1	The rate is calculated for the first time in the calculating rate mode.

Item	Description
-1 10.1.5.1	Last hop with the address as 10.1.5.1 in calculating rate mode.
Incoming Interface Address: 10.1.5.1 Input packets rate: 0	Multicast inbound interface address and the inbound packet rate on the inbound interface in calculating rate mode.
Outgoing Interface Address: 0.0.0.0 Output packets rate: 0xffffffff	Multicast outbound interface address and the outbound packet rate on the outbound interface in calculating rate mode.
Forwarding Cache (10.1.0.1, 225.0.0.1) Forwarding packets rate: 0	Rate for a switch to forward multicast packets of the (S, G) entry in calculating rate mode.
In maximum-hop mode, received the response message, and multicast traceroute finished.	IGMP Tracert Response messages are received in maximum hop tracking mode.
In calculating-rate mode, reach the demanded number of statistic, and multicast traceroute finished.	Mtrace is complete in calculating rate mode when the required number of calculating times is reached.

8.7.17 mtrace query-policy

Function

The **mtrace query-policy** command enables a device to filter IGMP-Tracert-Query packets in unicast mode based on the source address of these packets.

The **undo mtrace query-policy** command cancels the filtering of IGMP-Tracert-Query packets.

By default, the switch does not filter IGMP-Tracert-Query packets.

Format

mtrace query-policy [*basic-acl-number*]

undo mtrace query-policy

Parameters

Parameter	Description	Value
basic-acl-number	Specifies the number of the basic ACL. This ACL defines the address range of a trusted querier. According to this ACL, the last hop switch rejects the IGMP-Tracert-Query packets sent by an invalid querier.	The value is an integer ranging from 2000 to 2999.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

The source address of IGMP-Tracert-Query packets in unicast mode is the local interface address. Before you create an ACL rule, create an ACL.

Run this command on the switch that is connected to the host.

- This command takes effect only on the last hop switch, which is not the querier.
- This command filters only the IGMP-Tracert-Query packets encapsulated in unicast IP packets.
- This command is not applicable to the tracking initiated from the querier.

When you run the **mtrace query-policy** command on the last hop switch, note the following points:

- If *basic-acl-number* is not specified, the last hop switch does not reject IGMP-Tracert-Query packets in unicast mode.
- If *basic-acl-number* is specified but the ACL is not defined on the switch, the last hop switch rejects any IGMP-Tracert-Query packet in unicast mode.
- If *basic-acl-number* is specified and this ACL is defined on the switch, only the IGMP-Tracert-Query packets allowed by the ACL can be received.

Example

Apply the querier filtering rules to the last hop switch.

```
<HUAWEI> system-view
[HUAWEI] mtrace query-policy 2000
```

8.7.18 multicast boundary

Function

The **multicast boundary** command configures a multicast boundary for a single administrative range.

The **undo multicast boundary** command deletes the configured multicast boundary.

By default, no multicast boundary is configured on an interface.

Format

multicast boundary *group-address* { *mask* | *mask-length* }

undo multicast boundary { *group-address* { *mask* | *mask-length* } | **all** }

Parameters

Parameter	Description	Value
group-address	Specifies the address of a multicast group, used to specify a multicast group and configure the forwarding range of the multicast packets for the group.	The address is in dotted decimal notation and ranges from 224.0.1.0 to 239.255.255.255.
mask	Indicates the mask of a specified group address.	The mask is in dotted decimal notation.
mask-length	Indicates the mask length of a specified group address.	The value is an integer that ranges from 4 to 32.
all	Deletes all the multicast boundaries configured on an interface.	-

Views

GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, VLANIF interface view, loopback interface view, tunnel interface view, VBDIF interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Data of some multicast groups needs to be forwarded within a specified range. For example, each BSR administrative domain serves a specific group address range, and data packets sent from multicast sources to these groups need to be forwarded within the matching administrative domain. After a multicast boundary is configured for specified multicast groups on an interface, multicast packets sent to these groups cannot be forwarded through the interface. This restricts multicast forwarding within a range.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command.

Precautions

To configure the boundary for different multicast groups, you can repeat the command on the same interface.

A and B are the forwarding boundary sets of the multicast group range to be configured, and B is a subset of A. If A is first configured on an interface, B cannot be configured. If you configure A on the interface that has been configured with B, B is replaced by A.

Example

Configure VLANIF100 as the boundary of group 239.2.0.0/16.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] multicast boundary 239.2.0.0 16
```

Configure GE0/0/1 as the boundary of group 239.2.0.0/16.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] multicast boundary 239.2.0.0 16
```

8.7.19 multicast cpu-forward disable

Function

The **multicast cpu-forward disable** command disables software forwarding for multicast packets.

The **undo multicast cpu-forward disable** command restores the default configuration.

By default, software forwarding for multicast packets is enabled.

Format

multicast cpu-forward disable

undo multicast cpu-forward disable

Parameters

None.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In most cases, the switch forwards packets based on software before the hardware forwarding is completed. Then, the switch forwards packets based on hardware. Soft forwarding for multicast packets must be disabled on the switch to prevent packet loss and disorder caused by the low forwarding speed and first packet cache mechanism of soft forwarding.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command.

Example

Disable software forwarding for multicast packets.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] multicast cpu-forward disable
```

8.7.20 multicast forwarding-table downstream-limit

Function

The **multicast forwarding-table downstream-limit** command sets the maximum number of downstream nodes of an entry in the multicast forwarding table.

The **undo multicast forwarding-table downstream-limit** command restores the default setting.

By default, the maximum number of downstream nodes of an entry is 128.

Format

multicast forwarding-table downstream-limit *limit*

undo multicast forwarding-table downstream-limit

Parameters

Parameter	Description	Value
limit	Indicates the maximum number of downstream nodes of an entry in the forwarding table.	The value of ranges from 0 to 128.

Views

System view, VPN instance view, VPN IPv4 address family view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the switch receives a multicast packet, it copies the packet for each downstream node in the matching multicast forwarding entry. If the switch has a large number of multicast forwarding entries or each entry has many downstream nodes, many system resources are consumed. To reduce the load on the switch, limit the maximum number of downstream nodes in each multicast forwarding entry.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command.

Precautions

If the configured number is smaller than the current number, the excessive downstream nodes are not deleted immediately, and must be deleted by the multicast routing protocol. In addition, no new downstream node can be added to the entry in the forwarding table.

Example

Set the maximum number of downstream nodes of an entry in the forwarding table to 32.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] multicast forwarding-table downstream-limit 32
```

8.7.21 multicast forwarding-table route-limit

Function

The **multicast forwarding-table route-limit** command sets the limit on the number of entries in the multicast forwarding table.

The **undo multicast forwarding-table route-limit** command restores the default value of the limit.

The following lists the maximum number of entries allowed in the multicast forwarding table of each model by default:

- S5720-LI, S5720S-LI: 1022
- S5731-S, S5731S-S, S5720I-SI: 1024
- S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735-S, S500, S5735S-S, S5735-S-I: 1500
- S5735S-H, S5736-S, S6720S-S: 1536
- S5731-H, S5731S-H, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, S6730S-S: 4096

Format

multicast forwarding-table route-limit *limit*

undo multicast forwarding-table route-limit

Parameters

Parameter	Description	Value
limit	Specifies the limit on the number of entries in the multicast forwarding table.	The value is an integer that ranges from 0 to *The maximum number of entries allowed in the multicast forwarding table by default.* **NOTE** The value range of S5731-H, S5731S-H, S5732-H, S6730S-H, and S6730-H are expanded after the high specification mode is configured for multicast forwarding using the **set multicast forwarding-table super-mode** command. The actual value range depends on the specification of the device.

Views

System view, VPN instance view, VPN IPv4 address family view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Excessive multicast forwarding entries will exhaust the memory of the switch. To prevent this problem, use the **multicast forwarding-table route-limit** command to limit the number of entries in the multicast forwarding table.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command.

Precautions

NOTICE

If you set the limit on the number of entries in the multicast forwarding table after multicast services are deployed on a switch, ensure that the limit is greater than or equal to the number of current forwarding entries. Otherwise, faults may occur.

It is recommended that you set this limit based on the actual network environment before deploying multicast services on the switch.

If the configured limit is smaller than the number of existing entries, the excessive entries are not deleted immediately. The configured limit takes effect in the following cases:

- Entries are added to the multicast forwarding table after the existing entries age out.
- The **reset multicast forwarding-table all** command is run.

Example

Set the limit on the number of the entries in the forwarding table to 60.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] multicast forwarding-table route-limit 60
```

8.7.22 multicast invalid-packet

Function

The **multicast invalid-packet** command sets the maximum number of invalid multicast protocol packets that can be stored on the switch.

The **undo multicast invalid-packet** command deletes the set maximum number of invalid multicast protocol packets that can be stored on the switch.

By default, the switch can save a maximum of 10 invalid packets for each specific multicast protocol.

Format

multicast invalid-packet { **igmp** | **mdt** | **msdp** | **pim** } **max-count** *max-number*

undo multicast invalid-packet { **igmp** | **mdt** | **msdp** | **pim** }

Parameters

Parameter	Description	Value
igmp	Sets the maximum number of invalid IGMP messages.	-
mdt	Sets the maximum number of invalid multicast VPN messages.	-
msdp	Sets the maximum number of invalid MSDP messages.	-
pim	Sets the maximum number of invalid PIM messages.	-
max-count *max-number*	Sets the maximum number of invalid multicast protocol packets that can be stored on a device.	The value is an integer ranging from 1 to 100.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

If multicast entries fail to be generated or peer relationships fail to be set up, you can enable the switch to store invalid multicast protocol packets and view statistics and details of the invalid multicast protocol packets. Based on the command output, you can locate and rectify faults.

Example

Set the maximum number of invalid IGMP messages that can be stored on the switch to 20.

```
<HUAWEI> system-view
[HUAWEI] multicast invalid-packet igmp max-count 20
```

8.7.23 multicast load-splitting

Function

The **multicast load-splitting** command enables load splitting among multicast routes.

The **undo multicast load-splitting** command restores the default configuration.

By default, load splitting among multicast routes is disabled.

Format

multicast load-splitting { **balance-preferred** | **stable-preferred** | **group** | **source** | **source-group** }

undo multicast load-splitting

Parameters

Parameter	Description	Value
balance-preferred	Indicates balance-preferred load splitting. This policy is applicable to the scenario where hosts frequently join or leave groups, which requires automatic load adjustment.	-
stable-preferred	Indicates stable-preferred load splitting. This policy is applicable to stable multicast networking.	-

Parameter	Description	Value
group	Indicates group address-based load splitting. This policy is applicable to the scenario of one source to multiple groups.	-
source	Indicates source address-based load splitting. This policy is applicable to the scenario of multiple sources to one group.	-
source-group	Indicates source and group addresses-based load splitting. This policy is applicable to the scenario of multiple sources to multiple groups.	-

Views

System view, VPN instance view, VPN IPv4 address family view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

By default, if there are multiple equal-cost routes to a multicast source, the switch applies the following route selection rules during RPF check:

- If the equal-cost routes are in the same routing table, for example, a unicast routing table, multicast static routing table, or MBGP routing table, the switch selects the route with the largest next-hop address as the RPF route.
- If the equal-cost routes are in different routing tables, the switch selects the route with the highest preference. If the routes have the same preference, the switch selects the route with the longest mask length. If the routes have the same preference and mask length, the switch uses certain algorithm to select a route as the RPF route.

No matter which rule is used, the switch selects only one route as the RPF route. To enable multicast data to be forwarded through multiple paths, run the **multicast load-splitting** command to configure multicast load splitting. After multicast load splitting is configured, the switch uses the specified load splitting policy to distribute multicast data among multiple paths. This function improves quality of multicast forwarding.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command.

Follow-up Procedure

Because the forwarding capabilities of equal-cost routes are different from the actual load distribution situation on the equal-cost routes, even load splitting cannot meet network requirements in some scenarios. Then, you can run the

multicast load-splitting weight command to configure the multicast load splitting weight on the interface to realize unbalanced load splitting.

Precautions

The five load splitting policies are mutually exclusive. It is recommended that you use a fixed load splitting policy based on the actual situation on your network. The **balance-preferred** or **stable-preferred** policy is preferred.

If PIM-DM is enabled in the current public network instance, the **balance-preferred** or **stable-preferred** policy cannot be used.

Example

Configure group address-based load splitting.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] multicast load-splitting group
```

8.7.24 multicast load-splitting weight

Function

The **multicast load-splitting weight** command sets the multicast load splitting weight for an interface.

The **undo multicast load-splitting weight** command restores the default setting.

By default, the multicast load splitting weight of an interface is 1.

Format

multicast load-splitting weight *weight-value*

undo multicast load-splitting weight

Parameters

Parameter	Description	Value
weight-value	Specifies the multicast load splitting weight of an interface.	The value is an integer that ranges from 0 to 32.

Views

GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, VLANIF interface view, loopback interface view, VBDIF interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When a stable-preferred or balance-preferred multicast splitting policy is configured, you can run this command to set load splitting weights for interfaces to realize unbalanced load splitting. The larger weight value an interface has, the more multicast routing entries have it as the upstream interface.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command.

Precautions

This command is applicable only when the multicast load splitting policy is set to stable-preferred or balance-preferred.

When the multicast load splitting weight on an interface is 0, the routes that have this interface as the upstream interface do not take part in load splitting.

Example

Set the multicast load splitting weight on VLANIF100 to 10.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] multicast load-splitting weight 10
```

Set the multicast load splitting weight on GE0/0/1 to 10.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] multicast load-splitting weight 10
```

8.7.25 multicast load-splitting-timer

Function

The **multicast load-splitting-timer** command sets a load splitting timer.

The **undo multicast load-splitting-timer** command restores the default setting.

By default, the value of a load splitting timer is 1800 seconds.

Format

multicast load-splitting-timer *interval*

undo multicast load-splitting-timer

Parameters

Parameter	Description	Value
interval	Specifies the value of the load splitting timer.	The value is an integer ranging from 10 to 1800, in seconds.

Views

System view, VPN instance view, VPN IPv4 address family view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In stable-preferred load splitting or balance-preferred load splitting mode, entries may not be well-balanced among paths because of the addition or deletion of entries, change of load splitting weights of the paths, or change of equal-cost routes. In such a case, the device will balance entries after a certain waiting time to reduce the impact of frequent changes on the system.

Currently, setting a load splitting timer to change the waiting time before balancing entries is supported.

- If the network is stable, for example, when entries are not deleted or added frequently or equal-cost routes are not changed frequently, set the load splitting timer value to a smaller value so that entries can be balanced rapidly. The recommended value is 300 to 600 seconds.
- If the network is not stable, for example, when entries are deleted or added frequently or equal-cost routes are changed frequently, set the load splitting timer value to a larger value to reduce the impact of frequent entry changes on the system and network stability. The recommended value is 1200 to 1800 seconds.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command.

Example

Set a load splitting timer to 100 seconds.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] multicast load-splitting-timer 100
```


8.7.26 multicast longest-match

Function

The **multicast longest-match** command configures the switch to select the RPF route based on the longest matching rule.

The **undo multicast longest-match** command restores the default configuration.

By default, the switch selects the route with the highest preference as the RPF route.

Format

multicast longest-match

undo multicast longest-match

Parameters

None

Views

System view, VPN instance view, VPN IPv4 address family view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

By default, the switch selects the RPF route based on route preference. This command changes the route selection policy used by the switch during RPF check. After you run this command, the switch selects the RPF route with the longest mask. If multiple routes have the same mask length, the switch selects the route with the highest preference.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command.

Example

Select routes according to the longest match on the switch.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] multicast longest-match
```


8.7.27 multicast routing-enable

Function

The **multicast routing-enable** command enables the multicast routing function.

The **undo multicast routing-enable** command restores the default configuration.

By default, the multicast routing function is disabled.

Format

multicast routing-enable

undo multicast routing-enable

Parameters

None

Views

System view, VPN instance view, VPN IPv4 address family view

NOTE

Only the following models support the VPN instance view and VPN IPv4 address family view: S5731-H, S5731S-H, S5732-H, S5731-S, S5731S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S, S6720-EI, S6735-S and S6720S-EI

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Before configuring Layer 3 multicast, you must enable the multicast routing function globally. Layer 3 multicast protocols (such as PIM and IGMP) and other Layer 3 multicast functions can be configured only after multicast routing is enabled.

Precautions

Multicast functions (Layer 2 and Layer 3 multicast) and the flow control function (configured using the **flow-control** command) are mutually exclusive on the following models: S2730S-S, S5735-L-I, S5735-L1, S300, S5735-L, S5735S-L1, S5735S-L, S5735S-L-M, S500, S5735-S, S5735S-S, S5735-S-I

NOTICE

The **undo multicast routing-enable** command deletes all multicast configurations of the public network instance or VPN instance. After this command is run, multicast services that are running on the instance will be interrupted. To restore the multicast services, you must run the deleted multicast commands again.

Example

Enable multicast routing globally.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
```

8.7.28 multicast ttl-check disable

Function

The **multicast ttl-check disable** command disables a switch from checking the TTL value of multicast packets.

The **undo multicast ttl-check disable** command enables a switch to check the TTL value of multicast packets again.

By default, a switch checks the TTL value of multicast packets.

NOTE

This command is supported only on the following models: S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S.

Format

multicast ttl-check disable

undo multicast ttl-check disable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

In V200R019C10 and later versions, when multicast packets between a multicast source and receiver are forwarded across VLANs, the multicast packets with a TTL value less than or equal to 1 will be discarded by default.

In versions earlier than V200R019C10, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S do not discard multicast packets whose TTL value is less than or equal to 1. After the switch software version is upgraded to V200R019C10 or later, however, if you want a switch not to discard multicast packets whose TTL value is less than or equal to 1, run the **multicast ttl-check disable** command to disable the switch from checking the TTL value of multicast packets.

The **multicast ttl-check disable** command does not apply to the following scenarios:

- This command is not applicable to multicast packets on a VPN. A switch always discards multicast packets on a VPN if their TTL value is less than or equal to 1.
- This command does not apply when a multicast source and receiver are in the same VLAN, in which case, the switch does not check the TTL value of multicast packets between them.
- When the forwarding mode of multicast packets is changed to MAC address-based forwarding, the switch does not check the TTL value of multicast packets.

Example

Disable a switch from checking the TTL value of multicast packets.

```
<HUAWEI> system-view
[HUAWEI] multicast ttl-check disable
```

8.7.29 ping multicast

Function

The **ping multicast** command enables a device to detect the reserved members in the network segment, simulates the common group traffic, triggers the establishment of a distribution tree, and checks whether the network can normally bear multicast services.

Format

ping multicast [**-c** *count* | **-h** *ttl-value* | **-i** *interface-type interface-number* | **-m** *time* | **-p** *pattern* | **-q** | **-s** *packetsize* | **-t** *timeout* | **-tos** *tos-value* | **-v**] * *host*

Parameters

Parameter	Description	Value
-c *count*	Specifies the number of times for sending ICMP Echo Request messages.	The value is an integer that ranges from 1 to 65535. The default value is 5.
-h *ttl-value*	Sets the TTL value of an ICMP Echo Request message.	The value is an integer that ranges from 1 to 255. The default value is 255.
-i *interface-type interface-number*	Sets the outgoing interface that sends ICMP Echo Request messages. • When the MPing destination group address is a reserved multicast group address, **-i** must be specified. • When the MPing destination group address is a common multicast group address, **-i** cannot be specified.	-
-m *time*	Specifies the time to wait before sending the next ICMP Echo Request message. Each time the source sends an ICMP Echo Request message using the **ping multicast** command, the source waits a period of time (2000 ms by default) before sending the next ICMP Echo Request message. You can set the time to wait before sending the next ICMP Echo Request message using the parameter *time*. In the case of poor network condition, the value should be equal to or larger than 2000, in milliseconds.	The value is an integer that ranges from 1 to 10000, in milliseconds. The default value is 2000.
-p *pattern*	Specifies the padding byte of ICMP Echo Request messages. After the padding byte of the ICMP Echo Request message is set, the destination host can identify a certain ICMP Echo Reply message.	The value ranges from 0 to FFFFFFFF, in the hexadecimal format. By default, the padding starts from 0x01, and continues in ascending order.

Parameter	Description	Value
-q	Indicates that only statistics are displayed. When **-q** is specified in the **ping multicast** command, only the number of sent and received packets, packet loss rate, and the minimum, average, and maximum RTTs are displayed.	By default, all information is displayed.
-s *packetsize*	Sets the length of an ICMP Echo Request message, excluding the IP or ICMP header.	The value is an integer that ranges from 20 to 8100, in bytes. The default value is 56.
-t *timeout*	Specifies the timeout period to wait for an ICMP Echo Reply message after an ICMP Echo Request message is sent. After the **ping multicast** command is run, the source sends an ICMP Echo Request message to a destination and waits for an ICMP Echo Reply message. If the destination, after receiving the ICMP Echo Request message, returns an ICMP Echo Reply message to the source within the period specified by the parameter *timeout*, the destination is reachable. If the destination does not return an ICMP Echo Reply message within the specified period, the source displays a message indicating that the message times out. Normally, the source receives an ICMP Echo Reply message within 1 to 10 seconds after sending an ICMP Echo Request message. If the transmission speed is low, properly prolong the timeout period.	The value is an integer that ranges from 0 to 65535, in milliseconds. The default value is 2000.
-tos *tos-value*	Specifies the ToS value of the sent ICMP Echo Request messages.	The value is an integer that ranges from 0 to 255. The default value is 196.

Parameter	Description	Value
-v	Displays all received ICMP Echo Reply messages. ● If **-v** is not specified, the system displays the received ICMP Echo Reply messages of the user. ● If **-v** is specified, the system displays all received ICMP Echo Reply messages.	By default, only ICMP Echo Reply messages of the user are displayed.
host	Specifies the destination address of an ICMP Echo Request message, also called the MPing destination group address.	It includes reserved group addresses and common group addresses.

Views

All views

Default Level

0: Visit level

Usage Guidelines

Usage Scenario

The **ping multicast** command is used to check a multicast network in the following scenarios:

Scenario 1: When configuring the destination group address *host* as a reserved group address, you can run the **ping multicast** command to check which reserved multicast members reside on the network segment of the outbound interface. In this scenario, the TTL of an ICMP Echo Request message cannot be set.

The reserved multicast group identifies a group of network devices (reserved multicast members) that match certain conditions. When the reserved multicast members receive ICMP Echo Request messages with the destination addresses as the reserved group addresses, they return ICMP Echo Reply messages. Common reserved group addresses are as follows:

- 224.0.0.1: indicates all systems in the subnet.
- 224.0.0.2: indicates all routers in the subnet.
- 224.0.0.5: indicates OSPF IGP routers.
- 224.0.0.13: indicates PIM routers.

NOTE

In this scenario, **-i** must be specified in the **ping multicast** command.

Scenario 2: When setting the destination group address *host* as a common group address, you can run the **ping multicast** command to implement the following functions:

- Simulates the multicast traffic and triggers a series of protocol processes. By viewing the multicast routing information on the switch, check whether the protocol running status is normal and whether the multicast distribution tree is correctly established.
- Check multicast members in the network and calculate the TTL value and the RTT from the MPing initiator to multicast members. This function requires that the host support MPing and is implemented by calculating the number of ICMP Echo Reply messages sent by the destination host. MPing is performed continuously at a certain interval to calculate the network delay and route jitter.

NOTE

In this scenario, **-i** cannot be specified in the **ping multicast** command.

You can specify different parameters in **ping multicast** command for different scenarios:

- On an unstable network, you can run the **ping multicast -c** *count* **-t** *timeout* *host* command to check the quality of the multicast network. By analyzing the packet loss rate and average delay in the command output, you can evaluate the network quality. If the network is unreliable, set the packet transmission count (**-c**) and timeout (**-t**) to the upper limits. This makes the test result accurate.
- You can run the **ping multicast -s** *packetsize host* to set the size of a multicast probe packet. In this way, you can check the quality of the multicast network by simulating real service datagrams. The path MTU is then obtained through multiple probes.

Prerequisites

Before running the **ping multicast** command, ensure that the ICMP module is working properly.

Configuration Impact

If an intermediate device is disabled from responding to ICMP messages, detection on this node fails.

Precautions

If a fault occurs in the MPing process, you can press **Ctrl+C** to terminate the MPing operation.

Example

Perform MPing, specify the reserved multicast group address as 224.0.0.5 and the outbound interface as VLANIF 100, and detect the OSPF IGP router in the network segment.

```
<HUAWEI> ping multicast -i vlanif 100 224.0.0.5
MULTICAST PING 224.0.0.5 : 56 data bytes, press Ctrl+C to break
Reply from 10.1.1.5 : bytes=56 Sequence=1 TTL =255 time=30ms
Reply from 10.1.1.5 : bytes=56 Sequence=2 TTL =255 time=10ms
Reply from 10.1.1.5 : bytes=56 Sequence=3 TTL =255 time=10ms
Reply from 10.1.1.5 : bytes=56 Sequence=4 TTL =255 time=20ms
```



```
Reply from 10.1.1.5 : bytes=56 Sequence=5 TTL =255 time=10ms
Destination multicast address 224.0.0.5
--- Multicast ping statistics ---
5 Request packet(s) transmitted
5 Reply packet(s) received
0.00% packet loss
Round-trip min/avg/max = 10/16/40 ms
```

Specify the padding field of **-p**.

```
<HUAWEI> ping multicast -i vlanif 100 -p 12345678 224.0.0.5
MULTICAST PING 224.0.0.5 : 56 data bytes, press Ctrl+C to break
The padding string: 12345678
Reply from 10.1.1.5 : bytes=56 Sequence=1 TTL =255 time=30ms
Reply from 10.1.1.5 : bytes=56 Sequence=2 TTL =255 time=10ms
Reply from 10.1.1.5 : bytes=56 Sequence=3 TTL =255 time=10ms
Reply from 10.1.1.5 : bytes=56 Sequence=4 TTL =255 time=20ms
Reply from 10.1.1.5 : bytes=56 Sequence=5 TTL =255 time=10ms
Destination multicast address 224.0.0.5
--- Multicast ping statistics ---
5 Request packet(s) transmitted
5 Reply packet(s) received
0.00% packet loss
Round-trip min/avg/max = 10/16/40 ms
```

Table 8-106 Description of the ping multicast command output

Item	Description
MULTICAST PING 224.0.0.5	The destination group address of MPing is 224.0.0.5.
56 data bytes	The length of the sent ICMP Echo Request message is 56 bytes.
press Ctrl+C to break	The ongoing MPing test can be terminated by pressing **Ctrl+C**.
The padding string: 12345678	The padding string is 12345678. If **-p** is not specified, the padding character string is not displayed.
Reply from 10.1.1.5: bytes=56 Sequence=1 TTL=255 time=30ms	The ICMP Echo Reply message sent from 10.1.1.5 is received. The message carries the following information: ● bytes=56: indicates the length of the ICMP Echo Reply message. ● Sequence=1: indicates the sequence number of the ICMP Echo Reply message. ● TTL=255: indicates the TTL value of the ICMP Echo Reply message. ● time=30ms: indicates the RTT, in milliseconds. If no ICMP Echo Reply message is received after the timeout period, "Request time out" is displayed.
Destination multicast address 224.0.0.5	The destination group address is 224.0.0.5.

Item	Description
--- Multicast ping statistics --- 5 Request packet(s) transmitted 5 Reply packet(s) received 0.00% packet loss Round-trip min/avg/max = 10/16/40 ms	Statistics collected after the Ping test on the destination host. The statistics are as follows: • Number of sent ICMP Echo Request messages: 5 • Number of received ICMP Echo Reply messages: 5 • Percentage of non-Reply messages against total sent messages: 0.00% • The minimum RTT is 10 ms, the average RTT is 16 ms, and the maximum RTT is 40 ms.

8.7.30 reset mtrace statistics

Function

The **reset mtrace statistics** command clears statistics about Mtrace packets.

Format

reset mtrace statistics

Parameters

None

Views

User view

Default Level

3: Management level

Usage Guidelines

To collect statistics about Mtrace traffic generated in a certain period, reset the original statistics.

Example

Clear statistics about the current Mtrace traffic.

```
<HUAWEI> reset mtrace statistics
```


8.7.31 reset multicast forwarding-table

Function

The **reset multicast forwarding-table** command clears the entries of the multicast forwarding table.

Format

reset multicast [**vpn-instance** *vpn-instance-name* | **all-instance**] **forwarding-table all**

reset multicast [**vpn-instance** *vpn-instance-name* | **all-instance**] **forwarding-table** { *group-address* [**mask** { *group-mask* | *group-mask-length* }] | *source-address* [**mask** { *source-mask* | *source-mask-length* }] | **incoming-interface** { *interface-type interface-number* | **register** } } *

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Specifies a VPN instance. *vpn-instance-name* indicates the name of the VPN instance.	The value must be an existing VPN instance name.
all-instance	Indicates all the instances.	-
all	Indicates all forwarding entries of multicast forwarding tables.	-
group-address	Specifies the address of a multicast group.	The address is in dotted decimal notation and ranges from 224.0.1.0 to 239.255.255.255.
mask	Specifies the mask of a multicast group address or source address.	-
group-mask	Specifies the address mask of a multicast group.	The address mask is in dotted decimal notation.
group-mask-length	Specifies the mask length of a multicast group address.	The value is an integer that ranges from 4 to 32.
source-address	Specifies the address of a multicast source.	The address is in dotted decimal notation.
source-mask	Specifies the address mask of a multicast source.	The address mask is in dotted decimal notation.
source-mask-length	Specifies the mask length of the multicast source address.	The value is an integer that ranges from 0 to 32.
incoming-interface	Indicates the upstream interface of the forwarding entry.	-

Parameter	Description	Value
interface-type interface-number	Specifies the type and the number of an interface, used to specify an interface.	-
register	Indicates the register interface in PIM-SM.	-

Views

User view

Default Level

3: Management level

Usage Guidelines

NOTICE

After you run this command to delete information from the multicast forwarding table, multicast data will be interrupted for a period. Confirm the action before you use the command.

The time interval before you run the **reset multicast forwarding-table** command again must be longer than 30 seconds.

Example

Delete the multicast forwarding entries of the group 225.5.4.3 from the forwarding table.

```
<HUAWEI> reset multicast forwarding-table 225.5.4.3
```

8.7.32 reset multicast routing-table

Function

The **reset multicast routing-table** command clears the entries in the multicast routing table. The corresponding forwarding entries in the forwarding table are deleted at the same time.

Format

reset multicast [**vpn-instance** *vpn-instance-name* | **all-instance**] **routing-table all**

reset multicast [**vpn-instance** *vpn-instance-name* | **all-instance**] **routing-table** { *group-address* [**mask** { *group-mask* | *group-mask-length* }] | *source-address* [**mask** { *source-mask* | *source-mask-length* }] | **incoming-interface** { *interface-type interface-number* | **register** } } *

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Specifies a VPN instance. *vpn-instance-name* indicates the name of the VPN instance.	The value must be an existing VPN instance name.
all-instance	Indicates all the instances.	-
all	Indicates all entries in the multicast routing table.	-
group-address	Specifies the address of the specified group.	The address is in dotted decimal notation and ranges from 224.0.1.0 to 239.255.255.255.
mask	Indicates the address mask of a multicast group or source.	-
group-mask	Specifies the address mask of a multicast group.	The address mask is in dotted decimal notation.
group-mask-length	Specifies the mask length of a multicast group address.	The value is an integer that ranges from 4 to 32.
source-address	Specifies the address of a specified source.	The address is in dotted decimal notation.
source-mask	Specifies the address mask of a multicast source, in dotted decimal notation.	The address mask is in dotted decimal notation.
source-mask-length	Specifies the mask length of the multicast source address.	The value is an integer that ranges from 0 to 32.
incoming-interface	Specifies the incoming interface of a multicast entry.	-
interface-type interface-number	Specifies the type and the number of an interface, used to specify an interface.	-
register	Indicates the register interface of PIM-SM.	-

Views

User view

Default Level

3: Management level

Usage Guidelines

NOTICE

After you run this command to delete information from the multicast routing table, the matching entries in the multicast forwarding table are also deleted. As a result, multicast forwarding will be interrupted for a period. Confirm the action before you use the command.

Example

Delete the entries of the group 225.5.4.3 from the multicast routing table.

```
<HUAWEI> reset multicast routing-table 225.5.4.3
```

8.7.33 set multicast forwarding-table enhance-mode

Function

The **set multicast forwarding-table enhance-mode** command sets the multicast forwarding mode to enhanced forwarding. In this forwarding mode, the device generates dummy entries (Layer 3 multicast dummy forwarding entries) for multicast packets that fail RPF check, even if Layer 2 multicast is disabled on the device.

The **undo set multicast forwarding-table enhance-mode** command disables enhanced forwarding for multicast traffic on the device. After this command is run, the device no longer generates dummy entries (Layer 3 multicast dummy forwarding entries) for multicast packets that fail RPF check, if Layer 2 multicast is disabled on the device.

By default, a device forwards multicast traffic in enhanced mode.

Format

set multicast forwarding-table enhance-mode

undo set multicast forwarding-table enhance-mode

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If Layer 2 multicast is not enabled on a device using the **igmp-snooping enable (VLAN view)** command, the device cannot generate dummy entries for multicast packets that fail the RPF check, so such packets cannot match any multicast entries. As a result, a large number of unknown multicast packets will be continuously sent to the CPU, causing high CPU usage. To prevent such a problem, you can run the **set multicast forwarding-table enhance-mode** command to set the multicast forwarding mode to enhanced forwarding. In this forwarding mode, the device generates dummy entries for multicast packets that fail RPF check, even if Layer 2 multicast is disabled on the device. The dummy entries guide Layer 3 multicast traffic forwarding, preventing high CPU usage caused by continuous sending of unknown multicast traffic.

Precautions

This command takes effect only for multicast packets in a VLAN.

Example

Set multicast forwarding mode to enhanced forwarding.

```
<HUAWEI> system-view
[HUAWEI] set multicast forwarding-table enhance-mode
```

8.7.34 set multicast forwarding-table optimization-mode

Function

The **set multicast forwarding-table optimization-mode** command configures the multicast optimization mode in which the Layer 3 forwarding entries are stored on a switch.

The **undo set multicast forwarding-table optimization-mode** command restores the default storage mode.

By default, a switch uses the normal storage mode.

NOTE

Only the S6720-EI, S6735-S and S6720S-EI support this command.

Format

set multicast forwarding-table optimization-mode [**slot** *slot-id*]

undo set multicast forwarding-table optimization-mode [**slot** *slot-id*]

Parameters

Parameter	Description	Value
slot *slot-id*	*slot-id* specifies the slot that uses the multicast optimization mode. If no slot ID is specified, storage modes of all slots are configured to be the multicast optimization mode.	The value is an integer and must be the slot ID of a running slot.

Views

System view

Default Level

3: Management level

Usage Guidelines

Applicable Environment

In most cases, the Layer 3 forwarding entries are stored in normal mode. The ARP cache table, ND cache table, and multicast forwarding table share hardware resources, without affecting hardware resources allocated to the routing table.

This command optimizes storage resources of Layer 3 forwarding entries through preferential allocation of hardware resources preferentially to the multicast forwarding table. The ARP cache table, ND cache table, and routing table share hardware resources. Run this command if either of the following situations occurs:

- A large number of ARP prefix entries and multicast forwarding entries exist in the system at the same time.
- A large number of ND prefix entries and multicast forwarding entries exist in the system at the same time.

Precautions

Note the following points when running this command:

- If the multicast optimization modes on a switch are configured or deleted, the system prompts the user to save the configurations and then restart the device. If the device configuration is not saved, the new storage mode does not take effect after the restart.
- This function can be implemented on an IPv6 network only when a switch with an extended entry register is available. In addition, the storage mode of the register must be set to IPv6 mode. For details on how to configure the extended entry register, see **assign resource-mode** in "Device Management Commands > Hardware Configuration Commands".

NOTICE

When the user configures this mode or restores the default mode, the system will prompt the user to restart the device or a specified slot. If the system receives no response, the configuration times out, and the system view is displayed. The system does not restart. The restart can cause the network to crash for a short period. In most cases, this command is not recommended.

Example

Configure the storage mode to be the multicast optimization mode for a switch.

```
<HUAWEI> system-view
[HUAWEI] set multicast forwarding-table optimization-mode
```

8.7.35 set multicast forwarding-table super-mode

Function

The **set multicast forwarding-table super-mode** command configures the high specification mode for multicast forwarding. In the high specification mode, the number of multicast entries can reach the maximum value supported by the switch, which is much more than the default limit.

The **undo set multicast forwarding-table super-mode** command restores the default configuration.

By default, the common specification mode is used for multicast forwarding after Layer 3 multicast is configured. In this mode, the number of multicast entries cannot exceed the default limit defined on the switch.

NOTE

Only the S5731-H, S5731S-H, S5732-H, S6730S-H, and S6730-H support this command.

Format

set multicast forwarding-table super-mode

undo set multicast forwarding-table super-mode

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After Layer 3 multicast is enabled, the common specification mode is used for multicast forwarding by default. This mode can meet requirements of most multicast service scenarios. In some large-scale multicast applications, a network has a large number of multicast sources to provide many channels for multicast users. In these applications, the number of multicast entries may exceed the default limit defined on a multicast device. When this occurs, some multicast entries cannot be generated. As a result, some users cannot receive the multicast data they request.

The **set multicast forwarding-table super-mode** command configures the high specification mode to increase the number of entries used for multicast forwarding. In high specification mode, the number of multicast entries supported by the switch is much larger than the default limit on the number of multicast entries. This mode maximizes a device's capability to support large-scale multicast applications.

Precautions

After you run this command:

- This command can only increase the number of Layer 3 multicast forwarding entries, but cannot increase the number of Layer 2 multicast forwarding entries. In scenarios when both Layer 2 and Layer 3 multicast services are configured, the number of Layer 3 multicast forwarding entries is limited by the number of Layer 2 multicast forwarding entries. Therefore, this command cannot increase the number of multicast forwarding entries if both Layer 2 and Layer 3 multicast services are configured.
- Restart the switch for the configuration to take effect.
- The default value of the IGMP general query interval changes from 60s to 120s. You can set the IGMP general query interval using the **igmp timer query** or **timer query (IGMP view)** command.
- The default value of the IGMP robustness variable changes from 2 to 3. You can set the robustness variable using the **igmp robust-count** or **robust-count (IGMP view)** command.
- The default value of the other querier present interval changes from 125s to 245s. You can set the other querier present interval using the **igmp timer other-querier-present** or **timer other-querier-present (IGMP view)** command.
- The default value of the MLD robustness variable changes from 2 to 3. You can set the robustness variable using the **mld robust-count** or **robust-count (MLD view)** command.
- The default interval for sending PIM-DM State-Refresh messages changes from 60s to 255s. On an IPv4 multicast network, run the **state-refresh-interval (IPv4)** command to set the interval for sending PIM-DM State-Refresh messages. On an IPv6 network, run the **state-refresh-interval (IPv6)** command to set the interval for sending PIM-DM State-Refresh messages.
- The default interval for sending PIM Join-Prune messages changes from 210s to 300s. On an IPv4 multicast network, run the **holdtime join-prune (IPv4)** or **pim holdtime join-prune** command to set the interval for sending PIM

Join-Prune messages. On an IPv6 network, run the **holdtime join-prune (IPv6)** or **pim ipv6 holdtime join-prune** command to set the interval for sending PIM Join-Prune messages.

- Run the **car** command to change the rate limit for IGMP/MLD messages sent to the CPU according to the actual situations of multicast services.
- More system resources are consumed in the high specification mode. If the number of multicast protocol packets sent to the switch increases sharply in a short time, the CPU usage of the switch becomes high.
- It is recommended that you set the same general query interval on all the IGMP/MLD-enabled interfaces of a switch. For an IGMP-enabled interface, run the **igmp timer query** command in the interface view to set the general query interval. For an MLD-enabled interface, run the **mld timer query** command in the interface view to set the general query interval. This configuration prevents IGMP/MLD-enabled interfaces from sending Query messages at the same time, so that the switch does not have to process a large number of Report messages in a short time, which could cause a high CPU usage.
- In a stack, if member interfaces of an Eth-trunk interface are located on member switches that support different numbers of multicast forwarding entries, the maximum number of multicast forwarding entries supported by the Eth-Trunk interface depends on the member switch that supports the fewest multicast forwarding entries. Multicast forwarding entries supported by an Eth-Trunk interface meet either of the following conditions:
  - The outbound interface of the multicast forwarding entries is the Eth-Trunk interface that has been switched to the Layer 3 mode using the **undo portswitch** command.
  - The Eth-Trunk interface belongs to the VLANs corresponding to the VLANIF interfaces of the multicast forwarding entries.

Example

Configure the high specification mode for multicast forwarding.

```
<HUAWEI> system-view
[HUAWEI] set multicast forwarding-table super-mode
Warning: This command will modify some default multicast settings and has limitations
in a few special scenarios. Use the command according to product manual.Continue? [Y/N]:y
```

8.7.36 set multicast-hash-mode

Function

The **set multicast-hash-mode** command specifies a hash algorithm for multicast forwarding.

The **undo multicast-hash-mode** command restores the default hash algorithm for multicast forwarding.

By default, the crc-32-lower algorithm is used.

NOTE

Only the S6720-EI, S6735-S and S6720S-EI support support this command.

Format

set multicast-hash-mode { **crc-32-upper** | **crc-32-lower** | **lsb** | **crc-16-upper** | **crc-16-lower** }

undo set multicast-hash-mode { **crc-32-upper** | **crc-32-lower** | **lsb** | **crc-16-upper** | **crc-16-lower** }

Parameters

Parameter	Description
crc-32-upper	
crc-32-lower	
lsb	
crc-16-upper	
crc-16-lower	

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To improve multicast forwarding performance, the switch uses a hash algorithm to learn multicast addresses. If multiple addresses match a key value, a hash conflict occurs. A large number of hash conflicts will cause failures to learn some multicast addresses. When such a problem occurs, use an appropriate hash algorithm to reduce hash conflicts.

Precautions

- An appropriate hash algorithm can reduce but not eliminate hash conflicts.
- MAC addresses are distributed on a network randomly, so the system cannot determine the best hash algorithm. The default hash algorithm is the best algorithm in most cases, so changing the hash algorithm is not recommended.
- After changing the hash algorithm, restart the switch for the configuration to take effect.

Example

Set the hash algorithm for multicast forwarding to crc-32-upper.
<HUAWEI> **system-view**
[HUAWEI] **set multicast-hash-mode crc-32-upper**

8.8 IPv6 Multicast Route Management Commands

8.8.1 Command Support

Product	Support
S1700	Not supported.
S300	Supported.
S500	Supported.
S2700	Supported.
S5700	Supported except S5731-L and S5731S-L.
S6700	Supported.

8.8.2 display multicast ipv6 boundary

Function

The **display multicast ipv6 boundary** command displays the multicast boundary configured on an interface.

Format

display multicast ipv6 boundary [*ipv6-group-address ipv6-group-mask-length* | **scope** *scope-id*] [**interface** *interface-type interface-number*]

Parameters

Parameter	Description	Value
ipv6-group-address	Specifies an IPv6 multicast group address to display the corresponding multicast routing table.	The address is a 32-digit hexadecimal number, in the format X:X:X:X:X:X:X:X. An IPv6 multicast address starts with FF.
ipv6-group-mask-length	Specifies the mask length of the IPv6 multicast group address.	The value is an integer that ranges from 8 to 128.

Parameter	Description	Value
scope *scope-id*	Specifies a scope ID.	The value is an integer that ranges from 3 to 15.
interface *interface-type interface-number*	Specifies the type and number of an interface.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

This command enables you to check the boundary of a PIM-SM (IPv6) network. When some hosts cannot receive multicast data, you can use this command to check whether the problem is caused by multicast boundary configuration.

Example

Display the boundaries configured on all the interfaces.

```
<HUAWEI> display multicast ipv6 boundary
IPv6 multicast boundary information
Total 1 Multicast IPv6 boundary
 Interface            Boundary
 Vlanif100            FF02::/64
```

Table 8-107 Description of the display multicast ipv6 boundary command output

Item	Description
IPv6 multicast boundary information	IPv6 multicast boundary.
Total 1 Multicast IPv6 boundary	Total number of IPv6 multicast boundaries.
Interface	Name of the interface configured with multicast boundary.
Boundary	Multicast group with the interface as the boundary.

8.8.3 display multicast ipv6 forwarding-table

Function

The **display multicast ipv6 forwarding-table** command displays the IPv6 multicast forwarding table.

Format

display multicast ipv6 forwarding-table [*ipv6-source-address* [*ipv6-source-mask-length*] | *ipv6-group-address* [*ipv6-group-mask-length*] | **incoming-interface** { *interface-type interface-number* | **register** } | **outgoing-interface** { { **exclude** | **include** | **match** } { *interface-type interface-number* | **register** | **none** } } | { **statistics** | **verbose** }] *

Parameters

Parameter	Description	Value
ipv6-source-address	Specifies the IPv6 address of a multicast source.	The address is a 32-digit hexadecimal number, in the format X:X:X:X:X:X:X:X.
ipv6-source-mask-length	Specifies the mask length of the multicast source address.	The value is an integer that ranges from 0 to 128.
ipv6-group-address	Specifies the IPv6 address of a multicast group.	The address is a 32-digit hexadecimal number, in the format X:X:X:X:X:X:X:X. An IPv6 multicast address starts with FF.
ipv6-group-mask-length	Specifies the mask length of a multicast group address.	The value is an integer that ranges from 8 to 128.
incoming-interface	Indicates the incoming interface of an IPv6 multicast forwarding entry.	-
interface-type interface-number	Specifies the type and number of an interface.	-
register	Indicates the register interface of PIM-SM.	-
outgoing-interface	Indicates the outgoing interface of an IPv6 multicast forwarding entry.	-
exclude	Indicates that the downstream interface list does not contain the route forwarding entries of a specified interface.	-

Parameter	Description	Value
include	Indicates that the downstream interface list contains the route forwarding entries of a specified interface.	-
match	Indicates that the downstream interface list matches the route forwarding entries of a specified interface.	The downstream interface list contains only one eligible interface. After **match** is configured, the route forwarding entries of a null downstream interface list are displayed if the outgoing interface is not specified.
none	Displays the (S, G) entry without a downstream interface.	-
statistics	Displays the statistics of the multicast forwarding table.	-
verbose	Displays the detailed information about the multicast forwarding table.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

During IPv6 multicast routing and forwarding, routing information generated by IPv6 multicast routing protocols is saved in an IPv6 multicast routing table. The switch selects the optimal multicast routes from the routing table according to multicast routing and forwarding policies, and then delivers the selected multicast routes to the IPv6 multicast forwarding table to guide multicast data forwarding.

You can use the **display multicast ipv6 forwarding-table** command to check whether IPv6 multicast forwarding entries have been generated and whether multicast data can be forwarded normally.

Example

Display the IPv6 multicast forwarding table.


```
<HUAWEI> display multicast ipv6 forwarding-table
IPv6 Multicast Forwarding Table
Total 2 entries, 2 matched

00001. (FC00:AA::123, FF33::)
    MID: 0, Flags: ACT
    Uptime: 00:01:03, Timeout in: 00:02:27
    Incoming interface: Vlanif10
    List of 1 outgoing interfaces:
      1: LoopBack0
        Activetime: 00:23:15
    Matched 0 packets(0 bytes), Wrong If 0 packets
    Forwarded 0 packets(0 bytes)

00002. (FC00:AA::123, FF34::)
    MID: 1, Flags: ACT
    Uptime: 00:00:03, Timeout in: 00:03:27
    Incoming interface: Vlanif20
    List of 1 outgoing interfaces:
      1: LoopBack0
        Activetime: 00:23:15
    Matched 0 packets(0 bytes), Wrong If 0 packets
    Forwarded 0 packets(0 bytes)
```

Table 8-108 Description of the **display multicast ipv6 forwarding-table** command output

Item	Description
IPv6 Multicast Forwarding Table	IPv6 multicast forwarding table.
Total 2 entries, 2 matched	Total forwarding entries and total eligible forwarding entries.
00001	Number of the (S, G) entry.
(FC00:AA::123, FF33::)	(S, G) entry in the multicast routing table.
MID	Unique multicast forwarding entry in the MFIB table. MID is used to rapidly search the multicast forwarding table.

Item	Description
Flags	Status flag of the (S, G) entry. • ACT: indicates that an active event is triggered. • DUM: indicates a dummy entry. • MISS: indicates that the nocache time needs to be reported. • DROP: indicates packet dropping. • LTH: indicates that the traffic volume is below the threshold. • DEL: indicates a deleted entry. • RST: indicates that registration of the known timer is started. • 2IODEL: indicates that an entry is deleted from the MFIB table, and the update needs to be synchronized to the IO board. • 2PDEL: indicates that an entry is deleted from the device, and the update needs to be synchronized to the IO board. • 2SYNC: indicates that the entry is contained in the MFIB table but it does not exist on the device. • 2ADD: indicates that the entry existing on the device has not been added to the MFIB table. • CLR: indicates that the MFIB table is resetting. • L2FWD: indicates that the device forwards Layer 2 traffic in multicast mode. • NORPF: indicates that the device does not perform RPF check. • 2ACK: indicates that the VPN instance is waiting for the ACK message from the slave main control board. • 2RSED: indicates that the entry is waiting for retransmission. • IOACK: indicates that the VPN instance has received the ACK message from the device. • SACK: indicates that the VPN instance has received the ACK message forwarded by software.

Item	Description
	• BKCLR: indicates that the MFIB table on the slave main control board is resetting. • EXTR: indicates an extranet entry. • 2DEL: indicates that the entry deleted from the device has not been removed from the MFIB table. • PDEL: indicates that the entry does not exist on the device. • A denotes addition; D denotes deletion; I denotes upstream update; R denotes RP update; P denotes PMBR; F denotes flag. • S denotes SPT; E denotes encapsulation group update; US denotes status update; CS denotes status clearing.
Uptime	Period during which the (S, G) entry exists.
Timeout in	Remaining time of the (S, G) entry.
Incoming interface	Incoming interface of the (S, G) entry.
List of 1 outgoing interfaces: 1: LoopBack0	Outgoing interface list, including the outgoing interface number and name.
Activetime	Existing time of the outgoing interface of the (S, G) entry.
Matched 0 packets(0 bytes)	Bytes of multicast packets matching the (S, G) entry. **NOTE** Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S can provide the accurate counter values.
Wrong If 0 packets	Number of multicast packets matching the (S, G) entry but are not forwarded. **NOTE** Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S can provide the accurate counter values.

Item	Description
Forwarded 0 packets(0 bytes)	Number of packets and bytes forwarded by the (S, G) entry. **NOTE** Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S can provide the accurate counter values.

8.8.4 display multicast forwarding-table optimization-mode configuration

Function

The **display multicast forwarding-table optimization-mode configuration** command displays the configuration of the optimization mode in which Layer 3 multicast forwarding entries are stored.

NOTE

Only the S6720-EI, S6735-S and S6720S-EI support this command.

Format

display multicast forwarding-table optimization-mode configuration [**slot** *slot-id*]

Parameters

Parameter	Description	Value
slot *slot-id*	*slot-id* specifies the slot that uses the multicast optimization mode. If no slot ID is specified, configurations of all slots are displayed.	The value is an integer and must be the slot ID of a running slot.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

This command is used to display the configuration of the optimization mode in which Layer 3 multicast forwarding entries are stored. The configuration helps you select a slot based on your storage requirement.

Example

Display the configuration of the optimization modes.

```
<HUAWEI> display multicast forwarding-table optimization-mode configuration
Multicast forwarding-table optimization mode :
Slot      Mode
-------------------------
2         Normal mode
4         Normal mode
5         Rich MCast mode
```

Table 8-109 Description of the **display multicast forwarding-table optimization-mode configuration** command output

Item	Description
Multicast forwarding-table optimization mode	When the multicast optimization mode is enabled.
slot	Slot ID.
mode	Storage Mode. The following storage modes are available: • Normal: The ARP cache table or ND cache table and multicast forwarding table share hardware resources, without affecting hardware resources allocated to the routing table. • Rich MCast mode: also known as multicast optimization mode. The system allocates hardware resources preferentially to the multicast forwarding table. The ARP/ND cache table and routing table share hardware resources.

8.8.5 display multicast ipv6 routing-table

Function

The **display multicast ipv6 routing-table** command displays information about an IPv6 multicast routing table.

Format

display multicast ipv6 routing-table [*ipv6-source-address* [*ipv6-source-mask-length*] | *ipv6-group-address* [*ipv6-group-mask-length*] | **incoming-interface** { *interface-type interface-number* | **register** } | **outgoing-interface** { **exclude** | **include** | **match** } { *interface-type interface-number* | **register** | **none** }] * [**outgoing-interface-number** [*number*]]

Parameters

Parameter	Description	Value
ipv6-source-address	Specifies the IPv6 address of a multicast source.	The address is a 32-digit hexadecimal number, in the format X:X:X:X:X:X:X:X.
ipv6-source-mask-length	Specifies the mask length of a multicast source address.	The value is an integer that ranges from 0 to 128.
ipv6-group-address	Specifies the IPv6 address of a multicast group.	The address is a 32-digit hexadecimal number, in the format X:X:X:X:X:X:X:X. An IPv6 multicast address starts with FF.
ipv6-group-mask-length	Specifies the mask length of an IPv6 multicast group address.	The value is an integer that ranges from 8 to 128.
incoming-interface	Indicates the incoming interface of a multicast forwarding entry.	-
interface-type interface-number	Specifies the type and number of an interface.	-
register	Indicates the register interface of IPv6 PIM-SM.	-
outgoing-interface	Indicates the outgoing interface of a multicast forwarding entry.	-
include	Displays the (S, G) entries whose downstream interface list contains specified outgoing interfaces.	-
exclude	Displays the (S, G) entries whose downstream interface list does not contain specified outgoing interfaces.	-
match	Displays (S, G) entries whose the downstream interface list contains only one interface that is the same as a specified outgoing interface.	If no interface is specified, the (S, G) entry with the null downstream interface list is displayed.
none	Displays the routing entry without a downstream interface.	-
outgoing-interface-number	Displays the number of the outgoing interfaces of multicast routing entries.	-
number	Specifies the number of outgoing interfaces.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display multicast ipv6 routing-table** command to view the IPv6 multicast routing table, including the multicast source address, multicast group address, upstream interface, and downstream interface list.

Example

Display the corresponding routing entry of a multicast group in the IPv6 multicast routing table.

```
<HUAWEI> display multicast ipv6 routing-table
IPv6 multicast routing table
 Total 1 entry

 00001. (FC00::2, FFE3::1)
      Uptime: 00:00:14
      Upstream Interface: Vlanif10
      List of 1 downstream interface
        1:  Vlanif20
```

Table 8-110 Description of the display multicast ipv6 routing-table command output

Item	Description
IPv6 multicast routing table	IPv6 multicast routing table.
Total 1 entry	Number of routing entries that meet the query condition.
00001	Sequence number of the (S, G) entry.
(FC00::2, FFE3::1)	(S, G) entry in the IPv6 multicast routing table.
Uptime	Period during which the (S, G) entry exists.
Upstream Interface	Upstream interface of the (S, G) entry.
List of 1 downstream interface	Downstream interface list.

Display the number of downstream interfaces of the IPv6 multicast routing entries.

```
<HUAWEI> display multicast ipv6 routing-table outgoing-interface-number
IPv6 multicast routing table
 Total 2 entries

 00001. (FC00::55, FF33::1)
      Uptime: 00:00:05
```



```
    Upstream Interface: Vlanif10
    List of 2 downstream interfaces

00002. (FC00::55, FF33::2)
    Uptime: 00:00:05
    Upstream Interface: Vlanif20
    List of 2 downstream interfaces
```

Table 8-111 Description of the display multicast ipv6 routing-table outgoing-interface-number command output

Item	Description
List of 2 downstream interfaces	Number of the outgoing interfaces of IPv6 multicast routing entries.

8.8.6 display multicast ipv6 rpf-info

Function

The **display multicast ipv6 rpf-info** command displays the Reverse Path Forwarding (RPF) routes of a specified IPv6 multicast source or source/group.

Format

display multicast ipv6 rpf-info *ipv6-source-address* [*ipv6-group-address*] [**rpt** | **spt**]

Parameters

Parameter	Description	Value
ipv6-source-address	Specifies the IPv6 address of a multicast source, used to display the information of RPF routing corresponding to the source.	The address is a 32-digit hexadecimal number, in the format X:X:X:X:X:X:X:X.
ipv6-group-address	Specifies the IPv6 address of a multicast group, used to display the information of RPF routing corresponding to the group.	The address is a 32-digit hexadecimal number, in the format X:X:X:X:X:X:X:X. An IPv6 multicast address starts with FF.
rpt	Displays the RPF routing information corresponding to a specified source or group on the RPT.	-
spt	Displays the RPF routing information corresponding to a specified source or group on the SPT.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The RPF route with the *ipv6-source-address* as the destination address is an optimal route selected from IPv6 unicast routes. You can use the **display multicast ipv6 rpf-info** command to check the RPF route to the specified source or source-group.

Example

Display all RPF routes to the source address FC00::101.

```
<HUAWEI> display multicast ipv6 rpf-info fc00::101
 VPN-Instance: public net
 RPF information about source: FC00::101
    RPF interface: Vlanif100
    Referenced route/mask: FC00::/64
    Referenced route type: unicast
    Load splitting rule: disabled
```

Table 8-112 Description of the display multicast ipv6 rpf-info command output

Item	Description
RPF information about source	Indicates the multicast source to which RPF information belongs.
RPF interface	Indicates the RPF interface.
Referenced route/mask	Indicates the referenced route and its mask.
Referenced route type	Indicates the referenced route type.
Load splitting rule	Load splitting rules: • disable: load splitting disabled. • balance-preferred: load balancing preferred. • stable-preferred: stable-preferred load splitting. • source: source address-based load splitting. • group: group address-based load splitting. • source-group: source and group addresses-based load splitting.

8.8.7 multicast ipv6 boundary

Function

The **multicast ipv6 boundary** command configures a multicast boundary on an interface.

The **undo multicast ipv6 boundary** command deletes the configured multicast boundary.

By default, no multicast boundary is configured on an interface.

Format

multicast ipv6 boundary { *ipv6-group-address ipv6-group-mask-length* | **scope** *scope-id* }

undo multicast ipv6 boundary { *ipv6-group-address ipv6-group-mask-length* | **all** | **scope** }

Parameters

Parameter	Description	Value
ipv6-group-address	Specifies a multicast group address.	The address is a 32-digit hexadecimal number, in the format X:X:X:X:X:X:X:X. An IPv6 multicast address starts with FF.
ipv6-group-mask-length	Specifies the mask length of an IPv6 multicast group address.	The value is an integer that ranges from 8 to 128.
scope *scope-id*	Specifies a scope ID.	The value is an integer that ranges from 3 to 15.
all	Deletes all the multicast boundaries configured on an interface.	-

Views

GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, VLANIF interface view, loopback interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Data of some multicast groups needs to be forwarded within a specified range. For example, each BSR administrative domain serves a specific group address range, and data packets sent from multicast sources to these groups need to be forwarded within the matching administrative domain. After a multicast boundary is configured for specified multicast groups on an interface, multicast packets sent

to these groups cannot be forwarded through the interface. This restricts multicast forwarding within a range.

Prerequisites

IPv6 multicast routing has been enabled globally using the **multicast ipv6 routing-enable** command in the system view.

Precautions

To configure the boundary for different multicast groups, you can repeat the command on the same interface.

A and B are the forwarding boundary sets of the multicast group range to be configured, and B is a subset of A. If A is first configured on an interface, B cannot be configured. If you configure A on the interface that has been configured with B, B is replaced by A.

Example

Configure VLANIF100 as the boundary of group FF02::101/16.

```
<HUAWEI> system-view
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] ipv6 enable
[HUAWEI-Vlanif100] multicast ipv6 boundary FF02::101 16
```

Configure GE0/0/1 as the boundary of group FF02::101/16.

```
<HUAWEI> system-view
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] ipv6 enable
[HUAWEI-GigabitEthernet0/0/1] multicast ipv6 boundary FF02::101 16
```

8.8.8 multicast ipv6 cpu-forward disable

Function

The **multicast ipv6 cpu-forward disable** command disables software forwarding for IPv6 multicast packets.

The **undo multicast ipv6 cpu-forward disable** command restores the default configuration.

By default, software forwarding for IPv6 multicast packets is enabled.

Format

multicast ipv6 cpu-forward disable

undo multicast ipv6 cpu-forward disable

Parameters

None.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In most cases, the switch forwards packets based on software before the hardware forwarding is completed. Then, the switch forwards packets based on hardware. Soft forwarding for multicast packets must be disabled on the switch to prevent packet loss and disorder caused by the low forwarding speed and first packet cache mechanism of soft forwarding.

Prerequisites

IPv6 multicast routing has been enabled using the **multicast ipv6 routing-enable** command in the system view.

Example

Disable software forwarding for IPv6 multicast packets.

```
<HUAWEI> system-view
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] multicast ipv6 cpu-forward disable
```

8.8.9 multicast ipv6 forwarding-table downstream-limit

Function

The **multicast ipv6 forwarding-table downstream-limit** command sets the maximum number of downstream nodes of an entry in the IPv6 multicast forwarding table.

The **undo multicast ipv6 forwarding-table downstream-limit** command restores the default setting.

By default, the maximum number of downstream nodes of an entry is 128.

Format

multicast ipv6 forwarding-table downstream-limit *limit*

undo multicast ipv6 forwarding-table downstream-limit

Parameters

Parameter	Description	Value
limit	Indicates the maximum number of downstream nodes of an entry in the forwarding table.	The value is an integer that ranges from 0 to 128.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the switch receives a multicast packet, it copies the packet for each downstream node in the matching IPv6 multicast forwarding entry. If the switch has a large number of IPv6 multicast forwarding entries or each entry has many downstream nodes, many system resources are consumed. To reduce the load on the switch, limit the maximum number of downstream nodes in each IPv6 multicast forwarding entry.

Prerequisites

IPv6 multicast routing has been enabled globally using the **multicast ipv6 routing-enable** command in the system view.

Precautions

If the configured number is smaller than the current number, the excessive downstream nodes are not deleted immediately, and must be deleted by the IPv6 multicast routing protocol. In addition, no new downstream node can be added to the entry in the forwarding table.

Example

In the system view, set the maximum number of downstream nodes of an entry in the IPv6 multicast forwarding table to 32.

```
<HUAWEI> system-view
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] multicast ipv6 forwarding-table downstream-limit 32
```

8.8.10 multicast ipv6 forwarding-table route-limit

Function

The **multicast ipv6 forwarding-table route-limit** command sets the limits on the number of entries in the IPv6 multicast forwarding table.

The **undo multicast ipv6 forwarding-table route-limit** command restores the default value of the limit.

The following lists the maximum number of entries allowed in the IPv6 multicast forwarding table of each model by default:

- S5720-LI, S5720S-LI: 496
- S5735S-H, S5736-S, S6720S-S: 512
- S5731-S, S5731S-S, S5720I-SI 1024
- S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735S-S, S5735-S-I: 1500
- S5732-H, S6730-H, S6730S-H: 2048
- S6730-S, S6730S-S, S5731-H, S5731S-H, S6735-S, S6720-EI, S6720S-EI: 4096

Format

multicast ipv6 forwarding-table route-limit *limit*

undo multicast ipv6 forwarding-table route-limit

Parameters

Parameter	Description	Value
limit	Specifies the limit on the number of entries in the IPv6 multicast forwarding table.	The value is an integer that ranges from 0 to *The maximum number of entries allowed in the multicast forwarding table by default.* **NOTE** The value range of S5731-H, S5731S-H, S5732-H, S6730S-H, and S6730-H are expanded after the high specification mode is configured for multicast forwarding using the **set multicast forwarding-table super-mode** command. The actual value range depends on the specification of the device.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Excessive IPv6 multicast forwarding entries will exhaust the memory of the switch. To prevent this problem, use the **multicast ipv6 forwarding-table route-limit** command to limit the number of entries in the IPv6 multicast forwarding table.

Prerequisites

IPv6 multicast routing has been enabled globally using the **multicast ipv6 routing-enable** command in the system view.

Precautions

NOTICE

If the limit on the number of entries in the IPv6 multicast forwarding table is set after multicast services are deployed on a switch, ensure that this limit is greater than or equal to the number of existing forwarding entries. Otherwise, faults may occur.

It is recommended that you set the limit based on the actual network environment before deploying multicast services on the switch.

If the newly-configured limit on the number of entries is smaller than the number of existing entries, the excessive entries are not deleted immediately. The configured limit takes effect in the following cases:

- Entries are added to the IPv6 multicast forwarding table after the existing entries age out.
- The **reset multicast ipv6 forwarding-table all** command is executed.

Example

Set the limit on the number of the entries in the IPv6 forwarding table to 1024.

```
<HUAWEI> system-view
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] multicast ipv6 forwarding-table route-limit 1024
```

8.8.11 multicast ipv6 invalid-packet

Function

The **multicast ipv6 invalid-packet** command sets the maximum number of invalid IPv6 multicast protocol packets that can be stored on the switch.

The **undo multicast ipv6 invalid-packet** command deletes the set maximum number of invalid IPv6 multicast protocol packets that can be stored on the switch.

By default, the switch can save a maximum of 10 invalid packets for each specific IPv6 multicast protocol.

Format

multicast ipv6 invalid-packet { **mld** | **pim** } **max-count** *max-number*

undo multicast ipv6 invalid-packet { **mld** | **pim** }

Parameters

Parameter	Description	Value
mld	Sets the maximum number of invalid MLD messages.	-
pim	Sets the maximum number of invalid PIM (IPv6) messages.	-
max-count *max-number*	Sets the maximum number of invalid IPv6 multicast protocol packets that can be stored on a device.	The value is an integer that ranges from 1 to 100.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

If IPv6 multicast entries fail to be generated or peer relationships fail to be set up, you can enable the switch to store invalid IPv6 multicast protocol packets and view statistics and details of the invalid IPv6 multicast protocol packets. Based on the command output, you can locate and rectify faults.

Example

Set the maximum number of invalid MLD messages that can be stored on the switch to 20.

```
<HUAWEI> system-view
[HUAWEI] multicast ipv6 invalid-packet mld max-count 20
```

8.8.12 multicast ipv6 load-splitting

Function

The **multicast ipv6 load-splitting** command enables load splitting among IPv6 multicast routes.

The **undo multicast ipv6 load-splitting** command restores the default configuration.

By default, load splitting among IPv6 multicast routes is disabled.

Format

multicast ipv6 load-splitting { **balance-preferred** | **stable-preferred** | **group** | **source** | **source-group** }

undo multicast ipv6 load-splitting

Parameters

Parameter	Description	Value
balance-preferred	Indicates balance-preferred load splitting. This policy is applicable to the scenario where hosts frequently join or leave groups, which requires automatic load adjustment.	-
group	Indicates group address-based load splitting. This policy is applicable to the scenario of one source to multiple groups.	-
source	Indicates source address-based load splitting. This policy is applicable to the scenario of multiple sources to one group.	-
source-group	Indicates source and group addresses-based load splitting. This policy is applicable to the scenario of multiple sources to multiple groups.	-
stable-preferred	Indicates stable-preferred load splitting. This policy is applicable to stable multicast networking.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

By default, if there are multiple equal-cost routes to a multicast source, the device selects the route with the largest next-hop address as the RPF route. To enable multicast data to be forwarded through multiple paths, run this command to configure multicast load splitting. After multicast load splitting is configured, the device uses the specified load splitting policy to distribute multicast data among multiple paths. This function improves quality of multicast forwarding.

Prerequisites

IPv6 multicast routing has been enabled globally using the **multicast ipv6 routing-enable** command in the system view.

Follow-up Procedure

Because the forwarding capabilities of equal-cost routes are different from the actual load distribution situation on the equal-cost routes, even load splitting cannot meet network requirements in some scenarios. In this case, you can run the **multicast ipv6 load-splitting weight** command to configure the IPv6 multicast load splitting weight on the interface to realize unbalanced load splitting.

Precautions

The five load splitting policies are mutually exclusive. It is recommended that you use a fixed load splitting policy based on the actual situation on your network. The **balance-preferred** or **stable-preferred** policy is preferred.

If PIM-DM (IPv6) is enabled on the switch, the **balance-preferred** or **stable-preferred** policy cannot be used.

Example

Configure stable-preferred load splitting in the system view.

```
<HUAWEI> system-view
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] multicast ipv6 load-splitting stable-preferred
```

8.8.13 multicast ipv6 load-splitting weight

Function

The **multicast ipv6 load-splitting weight** command sets the IPv6 multicast load splitting weight for an interface.

The **undo multicast ipv6 load-splitting weight** command restores the default setting.

By default, the IPv6 multicast load splitting weight of an interface is 1.

Format

multicast ipv6 load-splitting weight *weight-value*

undo multicast ipv6 load-splitting weight

Parameters

Parameter	Description	Value
weight-value	Specifies the IPv6 multicast load splitting weight of an interface.	The value is an integer that ranges from 0 to 32.

Views

GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, VLANIF interface view, loopback interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When a stable-preferred or balance-preferred multicast splitting policy is configured, you can run this command to set load splitting weights for interfaces to realize unbalanced load splitting. The larger weight value an interface has, the more IPv6 multicast routing entries have it as the upstream interface.

Prerequisites

IPv6 multicast routing has been enabled globally using the **multicast ipv6 routing-enable** command in the system view.

Precautions

This command is applicable only when the IPv6 multicast load splitting policy is set to stable-preferred or balance-preferred.

When the IPv6 multicast load splitting weight on an interface is 0, the routes with this interface as the upstream interface do not take part in load splitting.

Example

Set the IPv6 multicast load splitting weight on VLANIF100 to 10.

```
<HUAWEI> system-view
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] ipv6 enable
[HUAWEI-Vlanif100] multicast ipv6 load-splitting weight 10
```

Set the IPv6 multicast load splitting weight on GE0/0/1 to 10.

```
<HUAWEI> system-view
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] ipv6 enable
[HUAWEI-GigabitEthernet0/0/1] multicast ipv6 load-splitting weight 10
```

8.8.14 multicast ipv6 load-splitting-timer

Function

The **multicast ipv6 load-splitting-timer** command sets an IPv6 multicast load splitting timer.

The **undo multicast ipv6 load-splitting-timer** command restores the default setting.

By default, the value of the IPv6 multicast load splitting timer is 1800 seconds.

Format

multicast ipv6 load-splitting-timer *interval*

undo multicast ipv6 load-splitting-timer

Parameters

Parameter	Description	Value
interval	Specifies the value of the IPv6 multicast load splitting timer.	The value is an integer that ranges from 10 to 1800, in seconds.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In stable-preferred load splitting or balance-preferred load splitting mode, entries may not be well-balanced among paths because of the addition or deletion of entries, change of load splitting weights of the paths, or change of equal-cost routes. In such a case, the device will balance entries after a certain waiting time to reduce the impact of frequent changes on the system.

Currently, setting a load splitting timer to change the waiting time before balancing entries is supported.

- If the network is stable, for example, when entries are not deleted or added frequently or equal-cost routes are not changed frequently, set the load splitting timer value to a smaller value so that entries can be balanced rapidly. The recommended value is 300 to 600 seconds.
- If the network is not stable, for example, when entries are deleted or added frequently or equal-cost routes are changed frequently, set the load splitting timer value to a larger value to reduce the impact of frequent entry changes on the system and network stability. The recommended value is 1200 to 1800 seconds.

Prerequisites

IPv6 multicast routing has been enabled globally using the **multicast ipv6 routing-enable** command in the system view.

Example

Set the IPv6 multicast load splitting timer to 100 seconds.

```
<HUAWEI> system-view
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] multicast ipv6 load-splitting-timer 100
```


8.8.15 multicast ipv6 routing-enable

Function

The **multicast ipv6 routing-enable** command enables the IPv6 multicast routing function.

The **undo multicast ipv6 routing-enable** command restores the default configuration.

By default, the IPv6 multicast routing function is disabled.

Format

multicast ipv6 routing-enable

undo multicast ipv6 routing-enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Before configuring Layer 3 IPv6 multicast, you must enable the IPv6 multicast routing function globally. Layer 3 IPv6 multicast protocols (such as PIM (IPv6) and MLD) and other Layer 3 IPv6 multicast functions can be configured only after IPv6 multicast routing is enabled.

Precautions

Multicast functions (Layer 2 and Layer 3 multicast) and the flow control function (configured using the **flow-control** command) are mutually exclusive on the following models: S2730S-S, S5735-L-I, S5735-L1, S300, S5735-L, S5735S-L1, S5735S-L, S5735S-L-M, S500, S5735-S, S5735S-S, S5735-S-I

NOTICE

The **undo multicast ipv6 routing-enable** command deletes all IPv6 multicast configurations of the device. If IPv6 multicast services are running on the device, the IPv6 multicast services are interrupted when this command is executed. To restore IPv6 multicast services on the instance, you must re-configure the corresponding commands.

Example

Enable IPv6 multicast routing globally.

```
<HUAWEI> system-view
[HUAWEI] multicast ipv6 routing-enable
```

8.8.16 multicast ttl-check disable

Function

The **multicast ttl-check disable** command disables a switch from checking the TTL value of multicast packets.

The **undo multicast ttl-check disable** command enables a switch to check the TTL value of multicast packets again.

By default, a switch checks the TTL value of multicast packets.

NOTE

This command is supported only on the following models: S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S.

Format

multicast ttl-check disable

undo multicast ttl-check disable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

In V200R019C10 and later versions, when multicast packets between a multicast source and receiver are forwarded across VLANs, the multicast packets with a TTL value less than or equal to 1 will be discarded by default.

In versions earlier than V200R019C10, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S do not discard multicast packets whose TTL value is less than or equal to 1. After the switch software version is upgraded to V200R019C10 or later, however, if you want a switch not to discard multicast packets whose TTL value is less than or equal to 1, run the **multicast ttl-check disable** command to disable the switch from checking the TTL value of multicast packets.

The **multicast ttl-check disable** command does not apply to the following scenarios:

- This command is not applicable to multicast packets on a VPN. A switch always discards multicast packets on a VPN if their TTL value is less than or equal to 1.
- This command does not apply when a multicast source and receiver are in the same VLAN, in which case, the switch does not check the TTL value of multicast packets between them.
- When the forwarding mode of multicast packets is changed to MAC address-based forwarding, the switch does not check the TTL value of multicast packets.

Example

Disable a switch from checking the TTL value of multicast packets.

```
<HUAWEI> system-view
[HUAWEI] multicast ttl-check disable
```

8.8.17 reset multicast ipv6 forwarding-table

Function

The **reset multicast ipv6 forwarding-table** command clears the entries of the IPv6 multicast forwarding table.

Format

reset multicast ipv6 forwarding-table all

reset multicast ipv6 forwarding-table { *ipv6-group-address* [*ipv6-group-mask-length*] | *ipv6-source-address* [*ipv6-source-mask-length*] | **incoming-interface** { *interface-type interface-number* | **register** } } *

Parameters

Parameter	Description	Value
all	Resets all the multicast forwarding caches (MFCs) in the multicast forwarding table.	-
ipv6-group-address	Specifies the IPv6 address of a multicast group.	The address is a 32-digit hexadecimal number, in the format X:X:X:X:X:X:X:X. An IPv6 multicast address starts with FF.
ipv6-group-mask-length	Specifies the mask length of a multicast group address.	The value is an integer that ranges from 8 to 128.

Parameter	Description	Value
ipv6-source-address	Specifies the IPv6 address of a multicast source.	The address is a 32-digit hexadecimal number, in the format X:X:X:X:X:X:X:X.
ipv6-source-mask-length	Specifies the mask length of a multicast source address.	The value is an integer that ranges from 0 to 128.
incoming-interface	Indicates the incoming interface of a forwarding entry.	-
interface-type interface-number	Specifies the type and number of an interface.	-
register	Indicates the register interface of IPv6 PIM.	-

Views

User view

Default Level

3: Management level

Usage Guidelines

NOTICE

After you run this command to delete information from the IPv6 multicast forwarding table, multicast data will be interrupted for a period. Confirm the action before you use the command.

Example

Delete all the IPv6 multicast forwarding entries.

```
<HUAWEI> reset multicast ipv6 forwarding-table all
```

8.8.18 reset multicast ipv6 routing-table

Function

The **reset multicast ipv6 routing-table** command clears the entries in the IPv6 multicast routing table. The corresponding forwarding entries in the forwarding table are deleted at the same time.

Format

reset multicast ipv6 routing-table all

reset multicast ipv6 routing-table { *ipv6-group-address* [*ipv6-group-mask-length*] | *ipv6-source-address* [*ipv6-source-mask-length*] | **incoming-interface** { *interface-type interface-number* | **register** } } *

Parameters

Parameter	Description	Value
all	Resets all routing entries in the multicast core routing table.	-
ipv6-group-address	Specifies the IPv6 address of a multicast group.	The address is a 32-digit hexadecimal number, in the format X:X:X:X:X:X:X:X. An IPv6 multicast address starts with FF.
ipv6-group-mask-length	Specifies the mask length of an IPv6 multicast group address.	The value is an integer that ranges from 8 to 128.
ipv6-source-address	Specifies the IPv6 address of a multicast source.	The address is a 32-digit hexadecimal number, in the format X:X:X:X:X:X:X:X.
ipv6-source-mask-length	Specifies the mask length of a multicast source address.	The value is an integer that ranges from 0 to 128.
incoming-interface	Indicates the incoming interface of a routing entry.	-
interface-type interface-number	Specifies the type and number of an interface.	-
register	Indicate the register interface of IPv6 PIM.	-

Views

User view

Default Level

3: Management level

Usage Guidelines

NOTICE

After you run this command to delete information from the IPv6 multicast routing table, the matching entries in the IPv6 multicast forwarding table are also deleted. As a result, multicast forwarding will be interrupted for a period. Confirm the action before you use the command.

Example

Delete the entries of the group FF02::101 from the IPv6 multicast routing table.

```
<HUAWEI> reset multicast ipv6 routing-table FF02::101
```

8.8.19 set multicast forwarding-table optimization-mode

Function

The **set multicast forwarding-table optimization-mode** command configures the multicast optimization mode in which the Layer 3 forwarding entries are stored on a switch.

The **undo set multicast forwarding-table optimization-mode** command restores the default storage mode.

By default, a switch uses the normal storage mode.

NOTE

Only the S6720-EI, S6735-S and S6720S-EI support this command.

Format

set multicast forwarding-table optimization-mode [**slot** *slot-id*]

undo set multicast forwarding-table optimization-mode [**slot** *slot-id*]

Parameters

Parameter	Description	Value
slot *slot-id*	*slot-id* specifies the slot that uses the multicast optimization mode. If no slot ID is specified, storage modes of all slots are configured to be the multicast optimization mode.	The value is an integer and must be the slot ID of a running slot.

Views

System view

Default Level

3: Management level

Usage Guidelines

Applicable Environment

In most cases, the Layer 3 forwarding entries are stored in normal mode. The ARP cache table, ND cache table, and multicast forwarding table share hardware resources, without affecting hardware resources allocated to the routing table.

This command optimizes storage resources of Layer 3 forwarding entries through preferential allocation of hardware resources preferentially to the multicast forwarding table. The ARP cache table, ND cache table, and routing table share hardware resources. Run this command if either of the following situations occurs:

- A large number of ARP prefix entries and multicast forwarding entries exist in the system at the same time.
- A large number of ND prefix entries and multicast forwarding entries exist in the system at the same time.

Precautions

Note the following points when running this command:

- If the multicast optimization modes on a switch are configured or deleted, the system prompts the user to save the configurations and then restart the device. If the device configuration is not saved, the new storage mode does not take effect after the restart.
- This function can be implemented on an IPv6 network only when a switch with an extended entry register is available. In addition, the storage mode of the register must be set to IPv6 mode. For details on how to configure the extended entry register, see **assign resource-mode** in "Device Management Commands > Hardware Configuration Commands".

NOTICE

When the user configures this mode or restores the default mode, the system will prompt the user to restart the device or a specified slot. If the system receives no response, the configuration times out, and the system view is displayed. The system does not restart. The restart can cause the network to crash for a short period. In most cases, this command is not recommended.

Example

Configure the storage mode to be the multicast optimization mode for a switch.

```
<HUAWEI> system-view
[HUAWEI] set multicast forwarding-table optimization-mode
```

8.8.20 set multicast forwarding-table super-mode

Function

The **set multicast forwarding-table super-mode** command configures the high specification mode for multicast forwarding. In the high specification mode, the number of multicast entries can reach the maximum value supported by the switch, which is much more than the default limit.

The **undo set multicast forwarding-table super-mode** command restores the default configuration.

By default, the common specification mode is used for multicast forwarding after Layer 3 multicast is configured. In this mode, the number of multicast entries cannot exceed the default limit defined on the switch.

NOTE

Only the S5731-H, S5731S-H, S5732-H, S6730S-H, and S6730-H support this command.

Format

set multicast forwarding-table super-mode

undo set multicast forwarding-table super-mode

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After Layer 3 multicast is enabled, the common specification mode is used for multicast forwarding by default. This mode can meet requirements of most multicast service scenarios. In some large-scale multicast applications, a network has a large number of multicast sources to provide many channels for multicast users. In these applications, the number of multicast entries may exceed the default limit defined on a multicast device. When this occurs, some multicast entries cannot be generated. As a result, some users cannot receive the multicast data they request.

The **set multicast forwarding-table super-mode** command configures the high specification mode to increase the number of entries used for multicast forwarding. In high specification mode, the number of multicast entries supported by the switch is much larger than the default limit on the number of multicast entries. This mode maximizes a device's capability to support large-scale multicast applications.

Precautions

After you run this command:

- This command can only increase the number of Layer 3 multicast forwarding entries, but cannot increase the number of Layer 2 multicast forwarding entries. In scenarios when both Layer 2 and Layer 3 multicast services are configured, the number of Layer 3 multicast forwarding entries is limited by the number of Layer 2 multicast forwarding entries. Therefore, this command cannot increase the number of multicast forwarding entries if both Layer 2 and Layer 3 multicast services are configured.
- Restart the switch for the configuration to take effect.

- The default value of the IGMP general query interval changes from 60s to 120s. You can set the IGMP general query interval using the **igmp timer query** or **timer query (IGMP view)** command.
- The default value of the IGMP robustness variable changes from 2 to 3. You can set the robustness variable using the **igmp robust-count** or **robust-count (IGMP view)** command.
- The default value of the other querier present interval changes from 125s to 245s. You can set the other querier present interval using the **igmp timer other-querier-present** or **timer other-querier-present (IGMP view)** command.
- The default value of the MLD robustness variable changes from 2 to 3. You can set the robustness variable using the **mld robust-count** or **robust-count (MLD view)** command.
- The default interval for sending PIM-DM State-Refresh messages changes from 60s to 255s. On an IPv4 multicast network, run the **state-refresh-interval (IPv4)** command to set the interval for sending PIM-DM State-Refresh messages. On an IPv6 network, run the **state-refresh-interval (IPv6)** command to set the interval for sending PIM-DM State-Refresh messages.
- The default interval for sending PIM Join-Prune messages changes from 210s to 300s. On an IPv4 multicast network, run the **holdtime join-prune (IPv4)** or **pim holdtime join-prune** command to set the interval for sending PIM Join-Prune messages. On an IPv6 network, run the **holdtime join-prune (IPv6)** or **pim ipv6 holdtime join-prune** command to set the interval for sending PIM Join-Prune messages.
- Run the **car** command to change the rate limit for IGMP/MLD messages sent to the CPU according to the actual situations of multicast services.
- More system resources are consumed in the high specification mode. If the number of multicast protocol packets sent to the switch increases sharply in a short time, the CPU usage of the switch becomes high.
- It is recommended that you set the same general query interval on all the IGMP/MLD-enabled interfaces of a switch. For an IGMP-enabled interface, run the **igmp timer query** command in the interface view to set the general query interval. For an MLD-enabled interface, run the **mld timer query** command in the interface view to set the general query interval. This configuration prevents IGMP/MLD-enabled interfaces from sending Query messages at the same time, so that the switch does not have to process a large number of Report messages in a short time, which could cause a high CPU usage.
- In a stack, if member interfaces of an Eth-trunk interface are located on member switches that support different numbers of multicast forwarding entries, the maximum number of multicast forwarding entries supported by the Eth-Trunk interface depends on the member switch that supports the fewest multicast forwarding entries. Multicast forwarding entries supported by an Eth-Trunk interface meet either of the following conditions:
  - The outbound interface of the multicast forwarding entries is the Eth-Trunk interface that has been switched to the Layer 3 mode using the **undo portswitch** command.
  - The Eth-Trunk interface belongs to the VLANs corresponding to the VLANIF interfaces of the multicast forwarding entries.

Example

Configure the high specification mode for multicast forwarding.

```
<HUAWEI> system-view
[HUAWEI] set multicast forwarding-table super-mode
Warning: This command will modify some default multicast settings and has limitations
in a few special scenarios. Use the command according to product manual.Continue? [Y/N]:y
```

8.8.21 set multicast-hash-mode

Function

The **set multicast-hash-mode** command specifies a hash algorithm for multicast forwarding.

The **undo multicast-hash-mode** command restores the default hash algorithm for multicast forwarding.

By default, the crc-32-lower algorithm is used.

NOTE

Only the S6720-EI, S6735-S and S6720S-EI support support this command.

Format

set multicast-hash-mode { **crc-32-upper** | **crc-32-lower** | **lsb** | **crc-16-upper** | **crc-16-lower** }

undo set multicast-hash-mode { **crc-32-upper** | **crc-32-lower** | **lsb** | **crc-16-upper** | **crc-16-lower** }

Parameters

Parameter	Description
crc-32-upper	
crc-32-lower	
lsb	
crc-16-upper	
crc-16-lower	

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To improve multicast forwarding performance, the switch uses a hash algorithm to learn multicast addresses. If multiple addresses match a key value, a hash conflict occurs. A large number of hash conflicts will cause failures to learn some multicast addresses. When such a problem occurs, use an appropriate hash algorithm to reduce hash conflicts.

Precautions

- An appropriate hash algorithm can reduce but not eliminate hash conflicts.
- MAC addresses are distributed on a network randomly, so the system cannot determine the best hash algorithm. The default hash algorithm is the best algorithm in most cases, so changing the hash algorithm is not recommended.
- After changing the hash algorithm, restart the switch for the configuration to take effect.

Example

Set the hash algorithm for multicast forwarding to crc-32-upper.
<HUAWEI> **system-view**
[HUAWEI] **set multicast-hash-mode crc-32-upper**

8.9 VLAN-based IGMP Snooping Configuration Commands

8.9.1 Command Support

Commands provided in this section and all the parameters in the commands are supported by all switch models (except the S5731-L and S5731S-L), unless otherwise specified. For details, see specific commands.

8.9.2 dhcp-snooping user-offline remove igmp-snooping

Function

The **dhcp-snooping user-offline remove igmp-snooping** command enables the switch to delete the IGMP snooping entries of DHCP snooping users immediately after the users go offline.

The **undo dhcp-snooping user-offline remove igmp-snooping** command restores the default configuration.

By default, the switch does not delete the IGMP snooping entries of DHCP snooping users immediately after the users go offline.

Format

dhcp-snooping user-offline remove igmp-snooping

undo dhcp-snooping user-offline remove igmp-snooping

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

By default, when IGMP snooping is enabled for DHCP snooping users, the switch does not delete the IGMP snooping entry of a user immediately after the user goes offline. The multicast flow requested by the user is still transmitted until the IGMP snooping entry of the user is aged out.

The **dhcp-snooping user-offline remove igmp-snooping** command enables the switch to delete the IGMP snooping entry of a DHCP snooping user immediately after the user goes offline, terminating the multicast flow requested by the user.

Prerequisites

IGMP snooping has been enabled globally using the **igmp-snooping enable (system view)** command.

Example

Enable the system to delete IGMP snooping entries of DHCP snooping users immediately after the users go offline.

```
<HUAWEI> system-view
[HUAWEI] igmp-snooping enable
[HUAWEI] dhcp-snooping user-offline remove igmp-snooping
```

8.9.3 display igmp-snooping

Function

The **display igmp-snooping** command displays the IGMP snooping running parameters.

Format

display igmp-snooping [**vlan** [*vlan-id*]]

Parameters

Parameter	Description	Value
vlan [*vlan-id*]	Displays the IGMP snooping running parameters in a specified VLAN. If this parameter is not specified, the system displays the IGMP running parameters in all VLANs with IGMP snooping configured.	The value is an integer that ranges from 1 to 4094.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

You can use this command to view the IGMP snooping running parameters.

To view the IGMP snooping configuration, run the **display igmp-snooping configuration** command.

Precautions

This command can display the IGMP snooping running parameters in a VLAN only when at least one interface in the VLAN is in Up state and IGMP snooping enabled in the VLAN. To enable IGMP snooping in a VLAN, run the **igmp-snooping enable (VLAN view)** command.

Example

Display the IGMP snooping running parameters.

```
<HUAWEI> display igmp-snooping
  IGMP Snooping Information for VLAN 3
    IGMP Snooping is Enabled
    IGMP Version is Set to default 2
    IGMP Query Interval is Set to default 125s
    IGMP Max Response Interval is Set to default 10s
    IGMP Robustness is Set to default 2
    IGMP Last Member Query Interval is Set to default 1s
    IGMP Router Port Aging Interval is Set to 180s or holdtime in hello
    IGMP Filter Group-Policy is not set
    IGMP Prompt Leave Disable
    IGMP Host-based Prompt Leave Disable
    IGMP Router Alert is Not Required
    IGMP Send Router Alert Enable
```



```
  IGMP Proxy Disable
  IGMP Report Suppress Disable
  IGMP Suppress Time is set to default 10 seconds
  IGMP Querier Disable
  IGMP Router Port Learning Enable
  IGMP SSM-Mapping Disable
  IGMP Limit Action Disable
  IGMP Suppress-dynamic-join Disable
IGMP Snooping Information for VLAN 4
  IGMP Snooping is Enabled
  IGMP Version is 3
  IGMP snooping version 3 uses ASM-SSM mode
  IGMP Query Interval is Set to default 125s
  IGMP Max Response Interval is Set to default 10s
  IGMP Robustness is Set to default 2
  IGMP Last Member Query Interval is Set to default 1s
  IGMP Router Port Aging Interval is Set to 180s or holdtime in hello
  IGMP Filter Group-Policy is not set
  IGMP Prompt Leave Disable
  IGMP Host-based Prompt Leave Disable
  IGMP Router Alert is Not Required
  IGMP Send Router Alert Enable
  IGMP Proxy Disable
  IGMP Report Suppress Disable
  IGMP Suppress Time is set to default 10 seconds
  IGMP Querier Disable
  IGMP Router Port Learning Enable
  IGMP SSM-Mapping Disable
  IGMP Limit Action Disable
  IGMP Suppress-dynamic-join Disable
```

Table 8-113 Description of the **display igmp-snooping** command output

Item	Description
IGMP Snooping Information for VLAN 3	The following information displayed is the IGMP snooping running parameters in VLAN 3.
IGMP Snooping is Enabled	IGMP snooping is enabled in the VLAN. By default, IGMP snooping is disabled in a VLAN. IGMP snooping can be enabled in a VLAN using the **igmp-snooping enable (VLAN view)** command.
IGMP Version is Set to default 2 IGMP Version is 3	Version of IGMP messages that can be processed in the VLAN. The default version is 2, indicating that both IGMPv1 and IGMPv2 messages can be processed. This parameter is configured using the **igmp-snooping version** command.
IGMP snooping version 3 uses ASM-SSM mode	The ASM-SSM model is used for IGMPv3. This parameter is configured using the **igmp-snooping version** command.
IGMP Query Interval is Set to default 125s	Interval at which IGMP General Query messages are sent. In this example, the default value (125 seconds) is displayed. This parameter is configured using the **igmp-snooping query-interval** command.

Item	Description
IGMP Max Response Interval is Set to default 10s	Maximum response time for IGMP General Query messages. In this example, the default value (10 seconds) is displayed. This parameter is configured using the **igmp-snooping max-response-time** command.
IGMP Robustness is Set to default 2	IGMP robustness variable. In this example, the default value 2 is displayed. This parameter is configured using the **igmp-snooping robust-count** command.
IGMP Last Member Query Interval is Set to default 1s	Interval at which IGMP Group-Specific Query messages are sent. In this example, the default value (1 second) is displayed. This parameter is configured using the **igmp-snooping lastmember-queryinterval** command.
IGMP Router Port Aging Interval is Set to 180s or holdtime in hello	Aging time of a router port. In this example, the default value (180 seconds or the holdtime value contained in PIM Hello messages) is displayed. This parameter is configured using the **igmp-snooping router-aging-time** command.
IGMP Filter Group-Policy is not set	Multicast group policy. In this example, the default configuration is displayed. That is, no policy is configured. A multicast group policy is configured using the **igmp-snooping group-policy** command.
IGMP Prompt Leave Disable	The fast leave function is disabled for interfaces in the VLAN (default configuration). The fast leave function can be enabled using the **igmp-snooping prompt-leave** command.
IGMP Host-based Prompt Leave Disable	The host-based fast leave function is disabled (default configuration). The host-based fast leave function can be enabled using the **igmp-snooping host-based prompt-leave** command.
IGMP Router Alert is Not Required	The switch does not require that the IGMP messages received from the VLAN contain the Router-Alert option in the IP header (default configuration). The switch can be configured to discard IGMP messages without the Router-Alert option using the **igmp-snooping require-router-alert** command.

Item	Description
IGMP Send Router Alert Enable	The switch sends the IGMP messages with the Router-Alert option to the VLAN (default configuration). The switch can be configured to send IGMP messages with the Router-Alert option using the **igmp-snooping send-router-alert** command.
IGMP Router Port Learning Enable	Router port learning is enabled (default configuration). Router port learning can be enabled using the **igmp-snooping router-learning** command.
IGMP Proxy Disable	IGMP snooping proxy is disabled (default configuration). IGMP snooping proxy can be enabled using the **igmp-snooping proxy** command.
IGMP Report Suppress Disable	IGMP message suppression is disabled (default configuration). IGMP message suppression can be enabled using the **igmp-snooping report-suppress** command.
IGMP Suppress Time is set to default 10 seconds	IGMP message suppression time. In this example, the default value (10 seconds) is displayed. This parameter is configured using the **igmp-snooping suppress-time** command.
IGMP Querier Disable	IGMP snooping querier is disabled (default configuration). IGMP snooping querier can be enabled using the **igmp-snooping querier enable** command.
IGMP SSM-Mapping Disable	IGMP snooping SSM mapping is disabled (default configuration). IGMP snooping SSM mapping can be enabled using the **igmp-snooping ssm-mapping enable** command.
IGMP Limit Action Disable	Layer 2 multicast entry overwriting is disabled (default configuration). Layer 2 multicast entry overwriting can be enabled using the **igmp-snooping limit-action** command.
IGMP Suppress-dynamic-join Disable	Report and Leave messages received in the VLAN can be forwarded to the upstream multicast device with static multicast groups configured (default configuration). This function can be disabled using the **igmp-snooping static-group suppress-dynamic-join** command.

8.9.4 display igmp-snooping configuration

Function

The **display igmp-snooping configuration** command displays the IGMP snooping configuration.

Format

display igmp-snooping [**vlan** [*vlan-id*]] **configuration**

Parameters

Parameter	Description	Value
vlan [*vlan-id*]	Displays the IGMP snooping configuration in a specified VLAN. If this parameter is not specified, the system displays the IGMP snooping configuration in all VLANs.	The value is an integer that ranges from 1 to 4094.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

This command displays only the IGMP snooping configuration so that you can check whether the IGMP snooping configuration made in the system is proper.

To check all IGMP snooping running parameters, run the **display igmp-snooping** command.

Prerequisites

The IGMP snooping configuration in a VLAN can be displayed as long as IGMP snooping parameters have been configured in the VLAN, no matter whether the VLAN contains interfaces in Up state.

Global IGMP snooping must be enabled using the **igmp-snooping enable (system view)** command before any IGMP snooping configuration is performed.

Example

Display the IGMP snooping configuration in all VLANs.

```
<HUAWEI> display igmp-snooping configuration
 IGMP Snooping Configuration for VLAN 7
    igmp-snooping enable
    igmp-snooping version 3
    igmp-snooping ssm-mapping enable
    igmp-snooping ssm-policy 2000
    igmp-snooping ssm-mapping 232.1.1.0 255.255.255.0 10.1.2.1
```

8.9.5 display igmp-snooping port-info

Function

The **display igmp-snooping port-info** command displays information about multicast group member ports.

Format

display igmp-snooping port-info [**vlan** *vlan-id* [**group-address** *group-address*]] [**verbose**]

Parameters

Parameter	Description	Value
vlan *vlan-id*	Displays information about multicast group member ports in a specified VLAN. If this parameter is not specified, the system displays multicast group member ports in all VLANs.	The value is an integer ranging from 1 to 4094.
group-address *group-address*	Displays information about member ports of a specified multicast group. If this parameter is not specified, the system displays member ports of all multicast groups.	The value ranges from 224.0.1.0 to 239.255.255.255, in dotted decimal notation.
verbose	Displays detailed information about multicast group member ports. If this parameter is not specified, the system displays the summary of multicast group member ports.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

When the switch with IGMP snooping enabled receives IGMP messages exchanged between hosts and a Layer 3 device, the switch maintains a Layer 2 multicast forwarding table based on information in the messages. The **display igmp-snooping port-info** command shows member ports in the Layer 2 multicast forwarding table. According to the command output, you can know which downlink ports of the switch have multicast users connected, and control multicast services conveniently.

Precautions

This command can display information about multicast group member ports in a VLAN only when IGMP snooping has been enabled in the VLAN using the **igmp-snooping enable (VLAN view)** command, and at least one interface in the VLAN is in Up state. If interfaces in the VLAN are dynamic group member ports, the command can display information about these member ports only after they receive IGMP Report messages and before their aging time expires.

Example

Display information about multicast group member ports in VLAN 7.

```
<HUAWEI> display igmp-snooping port-info vlan 7
--------------------------------------------------------------------------------
                        (Source, Group)  Port                        Flag
           Flag: S:Static    D:Dynamic    M: Ssm-mapping
--------------------------------------------------------------------------------
 VLAN 7, 2 Entry(s)
                         (*, 225.0.0.1)  GE0/0/1                     -D-
                                         1 port(s) include
                   (1.1.1.1, 225.0.0.1)  GE0/0/1                      -D-
                                         1 port(s) exclude
--------------------------------------------------------------------------------
```


Table 8-114 Description of the **display igmp-snooping port-info** command output

Item	Description
(Source, Group)	(S, G) entry, specifying the multicast source and multicast group. Multicast data is sent from multicast source S to group G. If S is displayed as *, multicast data may be sent from any multicast source. If S is displayed as an IP address, multicast data is sent from this IP address.
Port	Member port. **include** and **exclude** indicate the multicast source filtering mode.
Flag	Type of a member port, which can be: • S: static member port, which is configured using the **l2-multicast static-group** command • D: dynamic member port learned through IGMP snooping • M: member port established through SSM mapping
VLAN *x*, *x* Entry(s)	VLAN ID and the number of entries in the VLAN.

Display detailed information about all multicast group member ports.

```
<HUAWEI> display igmp-snooping port-info verbose

The port information of Group 225.0.0.1 on VLAN
100:
   Time of this group has been up : 00:00:55

  The port information of (0.0.0.0, 225.0.0.1):
    Time of this source has been up : 00:00:55
    Port Table on this source(0.0.0.0):
    List of ports in include mode:
      No.1
        Port name : GE0/0/1
        Time of this port has been up as a host-port : 00:00:55
        Remain time of port expire as dynamic host-port :
00:03:33
        Host-port flags : Dynamic
    There are 1 port(s) in include mode.

  The port information of (1.1.1.1, 225.0.0.1):
    Time of this source has been up : 00:00:55
    Port Table on this source(1.1.1.1):
    List of ports in exclude mode:
      No.1
        Port name : GE0/0/1
        Time of this port has been up as a host-port : 00:00:55
        Remain time of port expire as dynamic host-port :
00:03:33
        Host-port flags : Dynamic
    There are 1 port(s) in exclude mode.
```


Table 8-115 Description of the display igmp-snooping port-info verbose command output

Item	Description
The port information of Group *xxx*	Information about member ports of multicast group in VLAN.
Time of this group has been up	Time that elapsed since the multicast group was set up.
The port information of *xxx*	Information about member ports of a specified (S, G).
Time of this source has been up	Time that elapsed since the multicast source was set up.
Port Table on this source	List of member ports of the specified multicast source.
List of ports in include mode	Information about member ports that join a multicast group in INCLUDE mode.
List of ports in exclude mode	Information about member ports that join a multicast group in EXCLUDE mode.
No.1	First member port.
Port name	Type and number of the first member port.
Time of this port has been up as a host-port	Time that elapsed since the first member port was bound to a source or (S, G).
Remain time of port expire as dynamic host-port	Remaining aging time of the first member port. This field displays "NA" for a static member port. The aging time of a dynamic member port is calculated using the following formula: Aging time = Robustness variable x General query interval + Maximum response time for General Query messages. The robustness variable is configured using the **igmp-snooping robust-count** command. The general query interval is configured using the **igmp-snooping query-interval** command. The maximum response time for General Query messages is configured using the **igmp-snooping max-response-time** command.
Version2-host-present-timer-expiry	Aging time of the IGMPv2 host.
Version1-host-present-timer-expiry	Aging time of the IGMPv1 host.

Item	Description
Host-port flags	Type of a member port, which can be: • Static: static member • Dynamic: dynamic member port learned through IGMP snooping • Mapping: member port established through SSM mapping
There are *x* port(s) in include mode	Number of member ports that join a multicast group in INCLUDE mode.
There are *x* port(s) in exclude mode	Number of member ports that join a multicast group in EXCLUDE mode.

8.9.6 display igmp-snooping host-tracking

Function

The **display igmp-snooping host-tracking** command displays information about group member hosts.

Format

display igmp-snooping host-tracking [**vlan** *vlan-id* [**group-address** *group-address*]] [**interface** *interface-type interface-number*]

Parameters

Parameter	Description	Value
vlan *vlan-id*	Displays information about group member hosts in a specified VLAN. If this parameter is not specified, the command displays information about group member hosts in all VLANs.	The value is an integer that ranges from 1 to 4094.
group-address *group-address*	Displays information about member hosts of a specified multicast group. If this parameter is not specified, the command displays information about member hosts of all multicast groups.	The value ranges from 224.0.1.0 to 239.255.255.255, in dotted decimal notation.

Parameter	Description	Value
interface *interface-type interface-number*	Displays information about group member hosts on a specified interface. If this parameter is not specified, the command displays information about group member hosts on all interfaces. • *interface-type* specifies the interface type. • *interface-number* specifies the interface number.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

IGMP snooping creates and maintains a Layer 2 multicast forwarding table by listening to IGMP messages exchanged between hosts and an upstream Layer 3 device. You can use this command to view information about member hosts in the Layer 2 multicast forwarding table. The command output shows which hosts under group member ports are using multicast services, helping you manage multicast services.

Precautions

If no forwarding entry is available for a member host, the command does not display information about this host.

Example

Display information about group member hosts.

```
<HUAWEI> display igmp-snooping host-tracking
-------------------------------------------------------------------------------
VLAN                (Source, Group)      Interface       Reporter        Mode
-------------------------------------------------------------------------------
100                   (*, 225.0.0.2)     GE0/0/1         192.51.100.1    Include
100                (192.1.1.1,225.0.0.1) GE0/0/1         10.10.5.2       Exclude
-------------------------------------------------------------------------------
```


Table 8-116 Description of the **display igmp-snooping host-tracking** command output

Item	Description
VLAN	VLAN ID.
(Source, Group)	(S, G) entry, indicating that data is sent from multicast source S to group G. If Source is displayed as *, multicast data may be sent from any multicast source. If Source is displayed as an IP address, multicast data is sent from this IP address.
Interface	Group member interface.
Reporter	Host IP address.
Mode	Mode in which an interface filters multicast traffic specified by (S,G) entries. • Include: The interface receives multicast traffic specified by (S,G) entries. • Exclude: The interface does not receive multicast traffic specified by (S,G) entries.

8.9.7 display igmp-snooping qinq-port-info

Function

The **display igmp-snooping qinq-port-info** command displays multicast group membership on a QinQ or dot1q termination sub-interface.

Format

display igmp-snooping qinq-port-info interface *interface-type interface-number* [**group-address** *group-address*]

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Displays multicast group membership of a specified interface.	-

Parameter	Description	Value
group-address *group-address*	Displays group membership of a specified multicast group. If this parameter is not specified, the command displays group membership of all multicast groups on the specified interface.	The value ranges from 224.0.1.0 to 239.255.255.255, in dotted decimal notation.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

This command is used to check group membership on a QinQ or dot1q termination sub-interface.

Example

Display group membership of all multicast groups on QinQ termination sub-interface GE0/0/18.1.

```
<HUAWEI> display igmp-snooping qinq-port-info interface GigabitEthernet 0/0/18.1
Interface GigabitEthernet0/0/18.1, 1 Group(s)
 (Source,Group)                  PE-VID/CE-VID LiveTime          Flag
 ------------------------------------------------------------------------------
 (*,225.0.0.1)                   1001/0        --                S-
 (*,225.0.0.2)                   1001/0        00:00:23          -D-
```

Table 8-117 Description of the **display igmp-snooping qinq-port-info** command output

Item	Description
Interface GigabitEthernet0/0/18.1, 1 Group(s)	Group membership on a termination sub-interface.
(Source, Group)	(S, G) entry. If S is displayed as *, multicast data may be sent from any multicast source. If S is displayed as an IP address, multicast data is sent from this IP address.

Item	Description
PE-VID/CE-VID	Outer VLAN ID and inner VLAN ID.
LiveTime	Time elapsed since the group is discovered, in any of the following formats: ● If the time is shorter than or equal to 24 hours, the format is hh:mm:ss. ● If the time is longer than 24 hours but shorter than or equal to one week, the format is day:hour. ● If the time is longer than one week, the format is week:day. -- indicates that the group Up time is not obtained.
Flag	Type of a member port, which can be: ● S: static member port, which is configured using the **igmp static-group** command ● D: dynamic member port learned through IGMP snooping ● M: member port established through SSM mapping

8.9.8 display igmp-snooping querier

Function

The **display igmp-snooping querier** command displays whether the IGMP snooping querier function is enabled in a VLAN.

Format

display igmp-snooping querier vlan [*vlan-id*]

Parameters

Parameter	Description	Value
vlan [*vlan-id*]	Displays whether the IGMP snooping querier function is enabled in a specified VLAN. If *vlan-id* is not specified, the system displays status of the IGMP snooping querier function in all VLANs.	The value is an integer that ranges from 1 to 4094.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

You can configure an IGMP snooping querier on the switch to send IGMP Query messages in place of the upstream Layer 3 device in the following situations:

- The Layer 3 device cannot send IGMP messages for some reasons, for example, IGMP is not enabled on the Layer 3 device.
- The Layer 3 device uses static multicast forwarding entries and does not need to learn multicast forwarding entries.

You can use the **display igmp-snooping querier** command to check in which VLANs the IGMP snooping querier function is enabled.

Precautions

The querier function is disabled in a VLAN by default after IGMP snooping is enabled in the VLAN. To enable the querier function, run the **igmp-snooping querier enable** command.

Example

Display the status of the IGMP snooping querier function in all VLANs.

```
<HUAWEI> display igmp-snooping querier vlan
 VLAN            Querier-state
------------------------------------------------
 10              Enable
 20              Disable
 30              Disable
------------------------------------------------
 total entry 3
```

Table 8-118 Description of the **display igmp-snooping querier vlan** command output

Item	Description
VLAN	VLAN ID.
Querier-state	Querier status in a VLAN. • Disable: The IGMP snooping querier function is disabled in the VLAN. • Enable: The IGMP snooping querier function is enabled in the VLAN.
total entry 3	Number of VLANs in which the querier status is displayed.

8.9.9 display igmp-snooping router-port

Function

The **display igmp-snooping router-port** command displays information about the router ports in a specified VLAN, including static and dynamic router ports.

Format

display igmp-snooping router-port vlan [*vlan-id*]

Parameters

Parameter	Description	Value
vlan [*vlan-id*]	Displays information about the router ports in a specified VLAN. If *vlan-id* is not specified, the command displays router ports in all VLANs.	The value is an integer that ranges from 1 to 4094.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

A router port connects the switch to an upstream Layer 3 multicast device. The router port can be statically configured or dynamically generated after the interface receives an IGMP Query message or a PIM Hello message.

You can run the **display igmp-snooping router-port** command to view the type, name, lifetime, and aging time of a router port.

Precautions

This command can display information about router ports in a VLAN only when IGMP snooping has been enabled in the VLAN using the **igmp-snooping enable (VLAN view)** command, and at least one interface in the VLAN is in Up state.

Example

Display information about router ports in VLAN 2.

```
<HUAWEI> display igmp-snooping router-port vlan 2
Port Name               UpTime    Expires   Flags
```



```
--------------------------------------------------------------------
VLAN 2, 2 router-port(s)
GE0/0/1                 03:28:16    00:01:20    DYNAMIC
GE0/0/2                 2d:10h      --          STATIC
```

Table 8-119 Description of the display igmp-snooping router-port command output

Item	Description
Port Name	Type and number of a router port.
UpTime	Time that elapsed since the interface became a router port.
Expires	Aging time of the router port. ● The aging time is displayed for a dynamic router port. This parameter is configured using the **igmp-snooping router-aging-time** command. ● For a static router port, "--" is displayed, indicating that the static router does not age.
Flags	Type of the router port, which can be: ● STATIC: static router port configured using the **igmp-snooping static-router-port** command. ● DYNAMIC: dynamic router port

8.9.10 display igmp-snooping statistics

Function

The **display igmp-snooping statistics** command displays IGMP snooping statistics.

Format

display igmp-snooping statistics vlan [*vlan-id*]

Parameters

Parameter	Description	Value
vlan [*vlan-id*]	Displays IGMP snooping statistics in a specified VLAN. • If *vlan-id* is not specified, the system displays IGMP snooping statistics in all VLANs. • If *vlan-id* is specified, the system displays statistics about IGMP messages in the specified VLAN, but does not display the counts of IGMP snooping events that occur in the VLAN.	The value is an integer that ranges from 1 to 4094.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

After completing IGMP snooping configuration, you can use the **display igmp-snooping statistics** command to view IGMP snooping statistics, including the number of IGMP messages sent, number of IGMP messages received, number of PIM Hello messages received in each VLAN, and number of Layer 2 events that have occurred in all VLANs. Layer 2 events include changes in interface status, changes in VLAN status, changes in VLAN member interfaces (interfaces join or leave VLANs), and MSTP events. When a multicast fault occurs, the IGMP snooping statistics help you identify the cause of the fault.

Precautions

This command displays IGMP snooping statistics only when IGMP snooping has been enabled globally using the **igmp-snooping enable (VLAN view)** command.

Example

Display IGMP snooping statistics in all VLANs.

```
<HUAWEI> display igmp-snooping statistics vlan
 IGMP Snooping Events Counter
```



```
    Recv VLAN Up Event Times      3
    Recv VLAN Down Event Times    0
    Recv VLAN Del Event Times     0
    Recv Port Up Event Times      2
    Recv Port Down Event Times    0
    Recv Port Del Event Times     0
    Recv Port Inc Event Times     0
    Recv Port Exc Event Times     0
    Recv MSTP Block Event Times   0
    Recv MSTP Forward Event Times 0
    Recv LINK Change Event Times  0
 IGMP Snooping Packets Counter
   Statistics for VLAN 10
    Recv V1 Report          0
    Recv V2 Report          0
    Recv V3 Report          0
    Recv V1 Query           0
    Recv V2 Query           0
    Recv V3 Query           0
    Recv General Query      0
    Recv Leave              0
    Recv Pim Hello          0
    Send Query(S=0)         0
    Send Query(S!=0)        0
    Suppress Report         0
    Suppress Leave          0
    Proxy Send General Query              0
    Proxy Send Group-Specific Query       0
    Proxy Send Group-Source-Specific Query 0
```

Display IGMP snooping statistics in VLAN 10.

```
<HUAWEI> display igmp-snooping statistics vlan 10
 IGMP Snooping Packets Counter
   Statistics for VLAN 10
    Recv V1 Report  16
    Recv V2 Report  8768
    Recv V3 Report  0
    Recv V1 Query   0
    Recv V2 Query   2243
    Recv V3 Query   0
    Recv Leave      215
    Recv Pim Hello  0
    Send Query(S=0) 0
    Send Query(S!=0)529
    Suppress Report         0
    Suppress Leave          0
    Proxy Send General Query              0
    Proxy Send Group-Specific Query       0
    Proxy Send Group-Source-Specific Query 0
```

Table 8-120 Description of the display igmp-snooping statistics command output

Item	Description
IGMP Snooping Events Counter	Statistics on IGMP snooping events, including changes in interface status, changes in VLAN status, interfaces joining or leaving VLANs, and MSTP events.
Recv VLAN Up Event Times	Number of VLAN Up events.
Recv VLAN Down Event Times	Number of VLAN Down events.
Recv VLAN Del Event Times	Number of VLAN deletion events.

Item	Description
Recv Port Up Event Times	Number of interface Up events.
Recv Port Down Event Times	Number of interface Down events.
Recv Port Del Event Times	Number of interface deletion events.
Recv Port Inc Event Times	Number of times interfaces join VLANs.
Recv Port Exc Event Times	Number of times interfaces leave VLANs.
Recv MSTP Block Event Times	Number of times static groups fail to be created on interfaces that are blocked by MSTP and cannot forward multicast packets.
Recv MSTP Forward Event Times	Number of times static groups are successfully created on interfaces that are in MSTP forwarding state and can forward multicast packets normally.
Recv LINK Change Event Times	Number of link status change events.
IGMP Snooping Packets Counter	Statistics on IGMP Snooping packets.
Statistics for VLAN 10	Packet statistics in VLAN 10.
Recv V1 Report	Number of IGMPv1 Report messages received.
Recv V2 Report	Number of IGMPv2 Report messages received.
Recv V3 Report	Number of IGMPv3 Report messages received.
Recv V1 Query	Number of IGMPv1 Query messages received.
Recv V2 Query	Number of IGMPv2 Query messages received.
Recv V3 Query	Number of IGMPv3 Query messages received.
Recv General Query	Interval for sending IGMP General Query messages.
Recv Leave	Number of IGMP Leave messages received.
Recv Pim Hello	Number of PIM Hello messages received.
Send Query(S=0)	Number of IGMP Query messages sent with the source address 0.0.0.0.
Send Query(S!=0)	Number of IGMP Query messages sent with source addresses other than 0.0.0.0.
Suppress Report	Number of duplicate IGMP Report messages dropped.
Suppress Leave	Number of duplicate IGMP Leave messages dropped.

Item	Description
Proxy Send General Query	Number of General Query messages sent by the IGMP snooping proxy.
Proxy Send Group-Specific Query	Number of Group-Specific Query messages sent by the IGMP snooping proxy.
Proxy Send Group-Source-Specific Query	Number of Group-Source-Specific Query messages sent by the IGMP snooping proxy.

8.9.11 display l2-multicast forwarding-mode

Function

The **display l2-multicast forwarding-mode** command displays the Layer 2 multicast forwarding mode in VLANs.

Format

display l2-multicast forwarding-mode vlan [*vlan-id*]

Parameters

Parameter	Description	Value
vlan [*vlan-id*]	Displays the Layer 2 multicast forwarding mode in a specified VLAN. If *vlan-id* is not specified, the system displays the Layer 2 multicast forwarding mode in all VLANs.	The value is an integer ranging from 1 to 4094.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

After Layer 2 multicast is enabled on the switch, the switch maintains a Layer 2 multicast forwarding table. When receiving a multicast packet, the switch searches the Layer 2 multicast forwarding table for the outbound interface based on the multicast address of the packet. The switch determines the outbound interface based on the IP multicast address or IP multicast MAC address, depending on the configured Layer 2 multicast forwarding mode.

To check which Layer 2 multicast forwarding mode is used, run the **display l2-multicast forwarding-mode** command.

Precautions

You can change the forwarding mode using the **l2-multicast forwarding-mode** command.

Example

Display the Layer 2 multicast forwarding mode in all VLANs.

```
<HUAWEI> display l2-multicast forwarding-mode vlan
VLAN                Forwarding-mode       Router-discard
------------------------------------------------------------------
1                   IP                    disable
2                   IP                    disable
3                   MAC                   disable
```

Table 8-121 Description of the **display l2-multicast forwarding-mode vlan** command output

Item	Description
VLAN	VLAN ID.
Forwarding-mode	Forwarding mode used in a VLAN, which can be: ● MAC address-based forwarding ● IP address-based forwarding This parameter can be configured using the **l2-multicast forwarding-mode** { **ip** | **mac** } command.
Router-discard	Whether the switch is configured not to forward multicast data packets to router ports in a VLAN. ● enable: The switch does not forward multicast data packets to router ports in the VLAN. ● disable: The switch forwards multicast data packets to router ports in the VLAN. This function is configured using the **l2-multicast router-port-discard** command.

8.9.12 display l2-multicast forwarding-table vlan

Function

The **display l2-multicast forwarding-table vlan** command displays the Layer 2 multicast forwarding table in VLANs.

Format

display l2-multicast forwarding-table vlan [*vlan-id* [[**source-address** *source-address*] **group-address** { *group-address* | **router-group** }]]

Parameters

Parameter	Description	Value
vlan-id	Displays Layer 2 multicast forwarding entries in a specified VLAN. If *vlan-id* is not specified, the command displays Layer 2 multicast forwarding entries in all VLANs.	The value is an integer that ranges from 1 to 4094.
source-address *source-address*	Displays the forwarding entries of a specified Layer 2 multicast source.	The value is in dotted decimal notation.
group-address *group-address*	Displays multicast forwarding entries of a specified Layer 2 multicast group.	The value ranges from 224.0.1.0 to 239.255.255.255 in dotted decimal notation.
router-group	Displays Layer 2 multicast forwarding entries of all router ports.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

After completing IGMP snooping configuration, you can use the **display l2-multicast forwarding-table** command to view the Layer 2 multicast forwarding table. This command displays statically configured and dynamically learned multicast forwarding entries.

Each entry contains the multicast source, multicast group, list of outbound interfaces, and VLAN ID of multicast data packets. When the IGMP snooping version is set to v3 in a VLAN or when the IGMP snooping version is set to v2 or v1 but SSM mapping is configured, the **display l2-multicast forwarding-table** command displays (S, G) entries.

Precautions

This command displays Layer multicast forwarding entries in a VLAN only when the VLAN is in Up state (At least one interface in the VLAN is in Up state. If interfaces in the VLAN are dynamic group member ports, the interfaces must have received IGMP Report messages and have not been aged out.)

Example

Display multicast forwarding entries in VLAN 10.

```
<HUAWEI> display l2-multicast forwarding-table vlan 10
VLAN ID : 10, Forwarding Mode : IP
Total Group(s): 2
--------------------------------------------------------------------------------
                (Source, Group)     Interface                Out-Vlan
--------------------------------------------------------------------------------
                   Router-port     GigabitEthernet0/0/1          10
                (*, 225.1.1.6)     GigabitEthernet0/0/1          10
                                   GigabitEthernet0/0/2          10
               (*, 235.80.68.83)   GigabitEthernet0/0/1          10
                                   GigabitEthernet0/0/2          10
--------------------------------------------------------------------------------
```

Table 8-122 Description of the **display l2-multicast forwarding-table** command output

Item	Description
VLAN ID	VLAN ID of the forwarding entries.
Forwarding Mode	Multicast forwarding mode in the VLAN, which can be: • IP • MAC The multicast forwarding mode is configured using the **l2-multicast forwarding-mode** command.
(Source, Group)	(S, G) entry, specifying the multicast source and multicast group. The Router-port field indicates a router port.
Interface	Outbound interface. The value **Stream** indicates an unknown flow entry.
Out-Vlan	VLAN ID of packets.
Total Group(s)	Total number of multicast forwarding entries.

8.9.13 display l2-multicast forwarding-table statistics

Function

The **display l2-multicast forwarding-table statistics** command displays statistics about Layer 2 multicast forwarding entries.

Format

display l2-multicast forwarding-table statistics

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

After configuring IGMP snooping, you can use this command to view statistics about Layer 2 multicast forwarding entries.

Example

Display statistics about Layer 2 multicast forwarding entries. (The actual output information may differ from the following information.)

```
<HUAWEI> display l2-multicast forwarding-table statistics
------------------------------------------------------------------------------
0 Stream entries are calculated in statistics
1 IP entries are calculated in statistics
0 MAC entries are calculated in statistics
1 VLAN entries are calculated in statistics
0 VPLS entries are calculated in statistics
0 VXLAN entries are calculated in statistics
------------------------------------------------------------------------------
```

Table 8-123 Description of the **display l2-multicast forwarding-table statistics** command output

Item	Description
Stream entries are calculated in statistics	Number of unknown stream entries in a VLAN.
IP entries are calculated in statistics	Number of entries for IP address-based forwarding in a VLAN.
MAC entries are calculated in statistics	Number of entries for MAC address-based forwarding in a VLAN.
VLAN entries are calculated in statistics	Number of entries for IP address-based and MAC address-based forwarding in a VLAN.
VPLS entries are calculated in statistics	Number of entries for MAC address-based forwarding on a VPLS network.

Item	Description
VXLAN entries are calculated in statistics	Number of entries for MAC address-based forwarding on a VXLAN network.

8.9.14 igmp-snooping enable (system view)

Function

The **igmp-snooping enable** command enables IGMP snooping globally or in specified VLANs.

The **undo igmp-snooping enable** command disables IGMP snooping globally or in specified VLANs.

By default, IGMP snooping is disabled globally and in a VLAN.

Format

igmp-snooping enable [**vlan** { *vlan-id1* [**to** *vlan-id2*] } &<1-10>]

undo igmp-snooping enable [**vlan** { **all** | { *vlan-id1* [**to** *vlan-id2*] } &<1-10> }]

Parameters

Parameter	Description	Value
vlan *vlan-id1* [**to** *vlan-id2*]	Enables IGMP snooping in a VLAN or in multiple VLANs. *vlan-id1* and *vlan-id2* identify a range of VLAN IDs. If VLAN IDs are specified, IGMP snooping is enabled in the specified VLANs. If no VLAN ID is specified, IGMP snooping is enabled globally.	The values of *vlan-id1* and *vlan-id2* are integers that range from 1 to 4094.
all	Disables IGMP snooping in all VLANs.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

IGMP snooping runs on a Layer 2 device between a Layer 3 multicast device and hosts. By listening on the multicast protocol packets exchanged between the Layer 3 device and hosts, IGMP snooping maintains a multicast forwarding table to control Layer 2 multicast forwarding.

Before configuring IGMP snooping parameters, run the **igmp-snooping enable** command in the system view to enable IGMP snooping globally. Other IGMP snooping configuration commands can be used only after IGMP snooping is enabled globally.

You can enable IGMP snooping in multiple VLANs by using the **igmp-snooping enable** command in the system view.

Prerequisites

To enable IGMP snooping in multiple VLANs, ensure that IGMP snooping has been enabled globally.

Precautions

If you run the **igmp-snooping enable vlan** { *vlan-id1* [**to** *vlan-id2*] } &<1-10> command multiple times, all the configurations take effect.

When you run the **undo igmp-snooping enable** command in the system view, the system displays a message, asking you whether to disable IGMP snooping globally. When you disable IGMP snooping globally, all the IGMP snooping configurations are deleted. When you run the **igmp-snooping enable** command to enable IGMP snooping globally again, the switch uses the default IGMP snooping configuration.

Multicast functions (Layer 2 and Layer 3 multicast) and the flow control function (configured using the **flow-control** command) are mutually exclusive on the following models: S2730S-S, S5735-L-I, S5735-L1, S300, S5735-L, S5735S-L1, S5735S-L, S5735S-L-M, S500, S5735-S, S5735S-S, S5735-S-I

The **igmp snooping enable** command in a VLAN and the **igmp on-demand** configuration of the VLANIF interface are mutually exclusive.

After global IGMP snooping is enabled on a switch, the switch sends all the IGMP messages received from a VLAN to the CPU for processing. If the multicast service is not configured in a VLAN and you want the switch to directly forward the IGMP messages of this VLAN without sending them to the CPU, run the **protocol-transparent** command in the VLAN view to enable transparent transmission of protocol packets.

Example

Enable IGMP snooping globally.

```
<HUAWEI> system-view
[HUAWEI] igmp-snooping enable
```

Enable IGMP snooping in multiple VLANs.

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


8.9.15 igmp-snooping enable (VLAN view)

Function

The **igmp-snooping enable** command enables IGMP snooping in a VLAN.

The **undo igmp-snooping enable** command disables IGMP snooping in a VLAN.

By default, IGMP snooping is disabled in a VLAN.

Format

igmp-snooping enable

undo igmp-snooping enable

Parameters

None

Views

VLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

By default, IGMP snooping is not enabled in a VLAN after being enabled in the system view. To enable IGMP snooping in a VLAN, run the **igmp-snooping enable** command in the VLAN view.

Prerequisites

IGMP snooping has been enabled globally using the **igmp-snooping enable (system view)** command.

Configuration Impact

After IGMP snooping is enabled in a VLAN, this function takes effect only on interfaces in this VLAN.

After IGMP snooping is enabled globally, it is recommended that you enable IGMP snooping in all other VLANs. This prevents IGMP messages in this VLAN from being broadcast to access switches in the other VLANs.

Precautions

The **igmp snooping enable** command in a VLAN and the **igmp on-demand** configuration of the VLANIF interface are mutually exclusive.

If Layer 2 and Layer 3 multicast are both configured in a VLAN, you must delete the Layer 2 multicast configuration before you can modify or delete the Layer 3

multicast configuration. This means that you must disable IGMP snooping in the VLAN first, then modify or disable the IGMP and PIM (IPv4) configuration in the VLANIF interface view, and finally enable IGMP snooping in the VLAN. Otherwise, the Layer 3 multicast configuration cannot be modified or deleted on the corresponding VLANIF interface.

Example

Enable IGMP snooping in VLAN 2.

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

8.9.16 igmp-snooping fast-switch enable

Function

The **igmp-snooping fast-switch enable** command enables fast multicast forwarding path switching upon STP topology changes.

The **undo igmp-snooping fast-switch enable** command disables fast multicast forwarding path switching upon STP topology changes.

By default, fast multicast forwarding path switching upon STP topology changes is disabled.

Format

igmp-snooping fast-switch enable

undo igmp-snooping fast-switch enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the Layer 2 network topology changes, multicast forwarding paths may change. You can configure the switch to send Query messages upon topology changes using the **igmp-snooping send-query enable** command. In this way, multicast data flows can be switched to new forwarding paths quickly after the Layer 2 network topology changes. However, the downstream device may not

receive the Query message immediately after convergence of the Layer 2 network, because the Query message is sent after a certain interval (60s by default). As a result, multicast traffic cannot be quickly switched to the new forwarding paths.

If the Layer 2 network is running the Spanning Tree Protocol (STP), you can enable fast multicast forwarding path switching upon STP topology changes. When the STP topology changes, this function quickly changes the ports in Forwarding state into router ports to direct multicast data flows to the new forwarding paths.

Prerequisite

Global IGMP snooping has been enabled using the **igmp-snooping enable (system view)** command.

Precautions

- This function takes effect only when STP is used as the loop prevention protocol on a Layer 2 network and the STP operation mode is MSTP, RSTP, or STP.
- With this function configured, the switch sets all ports in Forwarding state as router ports when the STP topology changes. In this case, multicast data flows are forwarded to all the router ports before the router ports are aged. This will cause increase in multicast traffic on the network.

Example

Enable fast multicast forwarding path switching upon STP topology changes.

```
<HUAWEI> system-view
[HUAWEI] igmp-snooping enable
[HUAWEI] igmp-snooping fast-switch enable
```

8.9.17 igmp-snooping fast-send report enable

Function

The **igmp-snooping fast-send report enable** command configures a device to send IGMP Report messages to the upstream device through the active interface in a Smart Link group when the other Smart Link member interface experiences a change of state.

The **undo igmp-snooping fast-send report enable** command disables a device from proactively sending IGMP Report messages to the upstream device when a member interface in a Smart Link group experiences a change of state.

By default, a device does not proactively send IGMP Report messages to the upstream device through the active interface in a Smart Link group when the other Smart Link member interface experiences a change of state.

Format

igmp-snooping fast-send report enable

undo igmp-snooping fast-send report enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the status of a Smart Link member interface on a device changes, the active interface in the Smart Link group can forward IGMP Report messages to the upstream device only after receiving the next IGMP General Query message. In this way, multicast data can be switched to the new forwarding path. To enable a device to proactively send IGMP Report messages to the upstream device through the active interface in a Smart Link group when the status of the other Smart Link member interface changes, run the **igmp-snooping fast-send report enable** command. In this way, multicast data can be quickly switched to the new forwarding path.

Prerequisites

IGMP snooping has been enabled globally by running the **igmp-snooping enable** command in the system view.

Precautions

Use this command only on networks configured with Smart Link.

Example

Configure a device to send IGMP Report messages when a member interface of a Smart Link group experiences a change of state.

```
<HUAWEI> system-view
[HUAWEI] igmp-snooping enable
[HUAWEI] igmp-snooping fast-send report enable
```

8.9.18 igmp-snooping fast-send robust-count interval

Function

The **igmp-snooping fast-send robust-count interval** command configures the robustness variable and interval for sending Report messages through the active interface in a Smart Link group when the other Smart Link member interface experiences a change of state.

The **undo igmp-snooping fast-send robust-count interval** command restores the default robustness variable and interval for sending Report messages through the active interface in a Smart Link group when the other Smart Link member interface experiences a change of state.

By default, the robustness variable is 3 and the interval is 10s.

Format

igmp-snooping fast-send robust-count *robust-count* **interval** *interval*

undo igmp-snooping fast-send robust-count *robust-count* **interval** *interval*

Parameters

Parameter	Description	Value
robust-count *robust-count*	Specifies the robustness variable for sending Report messages.	The value is an integer in the range from 1 to 10.
interval *interval*	Specifies the interval for sending Report messages.	The value is an integer ranging from 1 to 60, in seconds.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To enable a device to proactively send IGMP Report messages to the upstream device through the active interface in a Smart Link group when the status of the other Smart Link member interface changes, run the **igmp-snooping fast-send report enable** command. In this way, multicast data can be quickly switched to the new forwarding path. Then, you can run the **igmp-snooping fast-send robust-count interval** command to adjust IGMP parameters to optimize multicast services.

- The robustness variable for sending Report messages refers to the number of times Report messages are sent through the active interface of a Smart Link group when the status of the other Smart Link member interface changes. The robustness variable helps prevent packet loss.
- The interval parameter configures a device to periodically send IGMP Report messages to the upstream device through the active interface of the Smart Link group when the status of the other Smart Link member interface changes. On a network with a small number of multicast receivers, a smaller interval enables multicast data to be switched to the new forwarding path more rapidly.

Maximum total time for sending Report messages = Robustness variable for sending Report messages x Interval for sending Report messages

Prerequisites

IGMP snooping has been enabled globally by running the **igmp-snooping enable** command in the system view.

Precautions

Use this command only after the **igmp-snooping fast-send report enable** command is run.

When receiving a Query message, a device stops sending IGMP Report messages to the upstream device through the active interface of a Smart Link group.

When a device sends IGMP Report messages, the transmitting interval is the maximum response time. It is recommended that you set the interval to a value greater than the suppression time, thereby preventing messages from being suppressed.

Example

Set the robustness variable and interval for sending Report messages through the active interface in a Smart Link group to 5 and 20s, respectively.

```
<HUAWEI> system-view
[HUAWEI] igmp-snooping enable
[HUAWEI] igmp-snooping fast-send robust-count 5 interval 20
```

8.9.19 igmp-snooping group-limit

Function

The **igmp-snooping group-limit** command sets the maximum number of multicast entries that an interface can learn.

The **undo igmp-snooping group-limit** command cancels the limit on the number of multicast entries that an interface can learn.

By default, the number of multicast entries that an interface can learn is not limited.

Format

igmp-snooping group-limit *group-limit* **vlan** { *vlan-id1* [**to** *vlan-id2*] } &<1-10>

undo igmp-snooping group-limit *group-limit* **vlan** { *vlan-id1* [**to** *vlan-id2*] } &<1-10>

undo igmp-snooping group-limit vlan { **all** | { *vlan-id1* [**to** *vlan-id2*] } &<1-10> }

Parameters

Parameter	Description	Value
group-limit	Specifies the maximum number of multicast groups that an interface can learn.	The value is an integer and the value range depends on the product model: • SS1720GW-E, S1720GWR-E, S5720-LI, S5720S-LI, S5731-S, S5731S-S, and S5720I-SI: 1 to 1024 • S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S500, S5735-S, S5735-S-I, and S5735S-S: 1 to 1500 • S5735S-H, S5736-S, and S6720S-S: 1 to 1536 • S5731-H, S5731S-H, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S: 1 to 4096
vlan *vlan-id1* [**to** *vlan-id2*]	Specifies the ID of a VLAN. *vlan-id1* and *vlan-id2* identify a range of VLAN IDs.	The values of *vlan-id1* and *vlan-id2* are integers that range from 1 to 4094.
all	Cancels the limit on the number of multicast groups that interfaces in all VLANs can learn.	-

Views

MultiGE interface view, Ethernet interface view, GE interface view, XGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, port group view, Eth-Trunk interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can use the **igmp-snooping group-limit** command to limit the number of multicast programs that a user can request. This configuration limits the multicast data traffic volume on the interface.

Prerequisites

IGMP snooping has been enabled globally using the **igmp-snooping enable (system view)** command.

Configuration Impact

During the configuration, if the number of multicast entries on the interface already exceeds the configured threshold, the number of multicast entries on the interface does not change and the interface cannot learn new multicast entries.

Precautions

The configuration takes effect only after you run the **igmp-snooping enable (VLAN view)** command to enable IGMP snooping in the VLAN.

Example

Configure GE0/0/1 to learn a maximum of 10 IGMP snooping entries in VLAN 10, and IGMP snooping is enabled globally and in VLAN 10.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] igmp-snooping group-limit 10 vlan 10
```

Configure GE0/0/1 to learn a maximum of 50 IGMP snooping entries in VLANs 20 to 30, and IGMP snooping is enabled globally and in these VLANs.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] igmp-snooping group-limit 50 vlan 20 to 30
```

8.9.20 igmp-snooping group-policy (interface view)

Function

The **igmp-snooping group-policy** command configures a multicast group policy on an interface.

The **undo igmp-snooping group-policy** command deletes a multicast group policy from an interface.

By default, no multicast group policy is available on an interface, and hosts connected to the interface can join any multicast group.

Format

igmp-snooping group-policy *acl-number* [**version** *version-number*] **vlan** *vlan-id1* [**to** *vlan-id2*]

undo igmp-snooping group-policy *acl-number* **vlan** *vlan-id1* [**to** *vlan-id2*]

undo igmp-snooping group-policy *acl-number* **version** *version-number* **vlan** *vlan-id1* [**to** *vlan-id2*]

undo igmp-snooping group-policy vlan { *vlan-id1* [**to** *vlan-id2*] | **all** }

Parameters

Parameter	Description	Value
acl-number	Specifies the number of the ACL that limits the multicast groups that hosts in a VLAN can join.	The number of a basic ACL is an integer that ranges from 2000 to 2999. The number of an advanced ACL ranges from 3000 to 3999.
version *version-number*	Applies the multicast group policy only to the IGMP messages of the specified version. If this parameter is not specified, the multicast group policy applies to all IGMP messages.	The value is an integer ranging from 1 to 3. • 1: IGMPv1 • 2: IGMPv2 • 3: IGMPv3
vlan *vlan-id1* [**to** *vlan-id2*]	Applies the multicast group policy to the specified VLANs on the interface.	*vlan-id1* and *vlan-id2* are integers that range 1 from 4094.
all	Deletes multicast groups policies in all VLANs from the interface.	-

Views

MultiGE interface view, Ethernet interface view, GE interface view, XGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, port group view, Eth-Trunk interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A multicast group policy controls the multicast programs that users can order on a device with IGMP snooping enabled. When a user orders a multicast program, the user host sends a Report message to the device, requesting to join the multicast group. The device checks whether the multicast group matches the ACL in the multicast group policy applied to the interface. If so, the device allows the user to

join the multicast group. If not, the device drops the message and prohibits the user from joining the multicast group.

Prerequisites

IGMP snooping has been enabled globally using the **igmp-snooping enable (system view)** command.

Precautions

- The configuration takes effect when IGMP snooping is enabled in the specified VLANs using the **igmp-snooping enable (VLAN view)** command.
- Before running the **igmp-snooping group-policy (interface view)** command, run the **acl** command to configure the ACL that you want to apply to the group policy to limit the range of multicast groups that hosts connected to the interface can join.
  - In the basic ACL view, set **source** in the **rule** command to the range of multicast groups that an interface can join.
  - In the advanced ACL view, set **source** in the **rule** command to the source address that is allowed to send multicast data to the specified multicast groups, and set **destination** to the range of multicast groups that an interface can join.

  After the **igmp-snooping group-policy (interface view)** command is executed on an interface:
  - The interface filters the received Report messages based on the ACL and maintains memberships only for the multicast groups permitted by the ACL.
  - The interface discards the Report messages that are denied by the ACL. If the entries of the multicast groups denied by the ACL exist on the switch, the switch deletes these entries when the aging time of the entries expires.
  - If the IGMP version is not specified, the specified ACL applies to IGMPv1, IGMPv2, and IGMPv3 hosts.
- A multicast group policy can also be configured in the VLAN view to control the multicast groups that users in the VLAN can join. A multicast group policy configured in the interface view controls the multicast groups that users in one or more VLANs on the interface can join. If you configure multicast group policies for the same VLAN in the interface view and VLAN view, the system first uses the policy configured in the interface view and then the policy configured in the VLAN view to determine the groups that user hosts can join.

Example

Prevent users in VLANs 20 to 30 from joining multicast group 225.1.1.123 on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] acl number 2000
[HUAWEI-acl-basic-2000] rule deny source 225.1.1.123 0
[HUAWEI-acl-basic-2000] quit
[HUAWEI] igmp-snooping enable
[HUAWEI] vlan batch 20 to 30
[HUAWEI] igmp-snooping enable vlan 20 to 30
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] port link-type trunk
```



```
[HUAWEI-GigabitEthernet0/0/1] port trunk allow-pass vlan 20 to 30
[HUAWEI-GigabitEthernet0/0/1] igmp-snooping group-policy 2000 vlan 20 to 30
```

Allow hosts belonging to VLANs 20 to 30 on GE0/0/1 to join group 225.1.1.123.

```
<HUAWEI> system-view
[HUAWEI] acl number 2000
[HUAWEI-acl-basic-2000] rule permit source 225.1.1.123 0
[HUAWEI-acl-basic-2000] quit
[HUAWEI] igmp-snooping enable
[HUAWEI] vlan batch 20 to 30
[HUAWEI] igmp-snooping enable vlan 20 to 30
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] port link-type trunk
[HUAWEI-GigabitEthernet0/0/1] port trunk allow-pass vlan 20 to 30
[HUAWEI-GigabitEthernet0/0/1] igmp-snooping group-policy 2000 vlan 20 to 30
```

8.9.21 igmp-snooping group-policy (VLAN view)

Function

The **igmp-snooping group-policy** command configures a multicast group policy in a VLAN.

The **undo igmp-snooping group-policy** command deletes the multicast group policy from a VLAN.

By default, no multicast group policy is available in a VLAN, and hosts in the VLAN can join any multicast group.

Format

igmp-snooping group-policy *acl-number* [**version** *version-number*]

undo igmp-snooping group-policy

Parameters

Parameter	Description	Value
acl-number	Specifies the number of an ACL used to restrict the range of groups users can join.	The number of a basic ACL is an integer that ranges from 2000 to 2999. The number of an advanced ACL ranges from 3000 to 3999.
version *version-number*	Applies the multicast group policy only to the IGMP messages of the specified version. If this parameter is not specified, the multicast group policy applies to all IGMP messages.	The value is an integer that ranges from 1 to 3. • 1: IGMPv1 • 2: IGMPv2 • 3: IGMPv3

Views

VLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A multicast group policy controls the multicast programs that users can order on a switch with IGMP snooping enabled. When a user orders a multicast program, the user host sends a Report message, requesting to join the multicast group. After the switch receives the message, it checks whether the multicast group matches the multicast group policy applied to the VLAN. If the messages match the ACL, the switch allows user hosts in the VLAN to join the group and accepts the Report messages. If the messages do not match the ACL, the switch prevents the user hosts in the VLAN from joining the group.

Prerequisites

IGMP snooping has been enabled globally using the **igmp-snooping enable (system view)** command.

Precautions

- The configuration takes effect when IGMP snooping is enabled in the specified VLANs using the **igmp-snooping enable (VLAN view)** command.
- Before running the **igmp-snooping group-policy (VLAN view)** command, run the **acl** command to configure the ACL that you want to apply to the group policy to limit the range of multicast groups that hosts connected to the VLAN can join.
  - In the basic ACL view, set **source** in the **rule** command to the range of multicast groups that a VLAN can join.
  - In the advanced ACL view, set **source** in the **rule** command to the source address that is allowed to send multicast data to the specified multicast groups, and set **destination** to the range of multicast groups that a VLAN can join.

  After the **igmp-snooping group-policy (VLAN view)** command is executed on an interface:
  - The VLAN filters the received Report messages based on the ACL and maintains memberships only for the multicast groups permitted by the ACL.
  - The VLAN discards the Report messages that are denied by the ACL. If the entries of the multicast groups denied by the ACL exist on the switch, the switch deletes these entries when the aging time of the entries expires.
  - If the IGMP version is not specified, the specified ACL applies to IGMPv1, IGMPv2, and IGMPv3 hosts.
- A multicast group policy can also be configured in the interface view to control the multicast groups that users in one or more VLANs on the interface

can join. A multicast group policy configured in the VLAN view controls the multicast groups that users in the VLAN can join. If you configure multicast group policies for the same VLAN in the interface view and VLAN view, the system first uses the policy configured in the interface view and then the policy configured in the VLAN view to determine the groups that user hosts can join.

Example

Prevent hosts in VLAN 2 from joining group 225.1.1.123.

```
<HUAWEI> system-view
[HUAWEI] acl number 2000
[HUAWEI-acl-basic-2000] rule deny source 225.1.1.123 0
[HUAWEI-acl-basic-2000] quit
[HUAWEI] igmp-snooping enable
[HUAWEI] vlan 2
[HUAWEI-vlan2] igmp-snooping enable
[HUAWEI-vlan2] igmp-snooping group-policy 2000
```

Allow hosts in VLAN 2 to join group 225.1.1.123.

```
<HUAWEI> system-view
[HUAWEI] acl number 2000
[HUAWEI-acl-basic-2000] rule permit source 225.1.1.123 0
[HUAWEI-acl-basic-2000] quit
[HUAWEI] igmp-snooping enable
[HUAWEI] vlan 2
[HUAWEI-vlan2] igmp-snooping enable
[HUAWEI-vlan2] igmp-snooping group-policy 2000
```

8.9.22 igmp-snooping lastmember-queryinterval

Function

The **igmp-snooping lastmember-queryinterval** command sets the last member query interval in a VLAN, that is, the interval at which Group-Specific Query messages are sent in the VLAN.

The **undo igmp-snooping lastmember-queryinterval** command restores the default last member query interval in a VLAN.

By default, Group-Specific Query messages are sent in a VLAN at intervals of 1 second.

Format

igmp-snooping lastmember-queryinterval *lastmember-queryinterval*

undo igmp-snooping lastmember-queryinterval

Parameters

Parameter	Description	Value
lastmember-queryinterval	Specifies the interval at which IGMP Group-Specific Query messages are sent.	The value is an integer that ranges from 1 to 5, in seconds.

Views

VLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

By setting the last member query interval, you can:

- Configure the switch to send IGMP Group-Specific Query messages at intervals when the querier function is enabled.
- Change the aging time of multicast group member ports.

  When the switch receives an IGMP Leave message from a host, the switch starts the aging timer for the corresponding member port. The aging time is calculated using the following formula: Aging time = Last member query interval x Last member query count. The **igmp-snooping lastmember-queryinterval** command sets the last member query interval. The last member query count is set by the **igmp-snooping robust-count** command.

  If the switch (querier) receives Report messages from other hosts within the aging time, it continues to maintain memberships of the multicast group. If the switch does not receive any Report messages within the aging time, it stops maintaining memberships of the multicast group.

Prerequisites

IGMP snooping has been enabled globally using the **igmp-snooping enable (system view)** command.

Precautions

The switch sets the maximum response time field in the Group-Specific Query message to the configured last member query interval. Therefore, the maximum response time for Group-Specific Query messages is the same as the interval at which Group-Specific Query messages are sent.

The configuration takes effect only when all the following conditions are met:

- IGMP snooping is enabled in the VLAN using the **igmp-snooping enable (VLAN view)** command.
- The IGMP message version is set to v2 or v3 messages in the VLAN. (Hosts running IGMPv1 do not send Leave messages when they leave a multicast group.)

Example

Set the last member query interval in VLAN 3 to 4 seconds.

```
<HUAWEI> system-view
[HUAWEI] igmp-snooping enable
[HUAWEI] vlan 3
[HUAWEI-vlan3] igmp-snooping enable
[HUAWEI-vlan3] igmp-snooping lastmember-queryinterval 4
```


8.9.23 igmp-snooping learning

Function

The **igmp-snooping learning** command enables learning of multicast group memberships on an interface.

The **undo igmp-snooping learning** command disables learning of multicast group memberships on an interface.

By default, learning of multicast group memberships is enabled on an interface.

Format

igmp-snooping learning vlan { { *vlan-id1* [**to** *vlan-id2*] } &<1-10> | **all** }

undo igmp-snooping learning vlan { { *vlan-id1* [**to** *vlan-id2*] } &<1-10> | **all** }

Parameters

Parameter	Description	Value
vlan { *vlan-id1* [**to** *vlan-id2*] }	Enables learning of multicast group memberships in specified VLANs. The interface must have been added to the specified VLAN. *vlan-id1* [**to** *vlan-id2*] specifies the range of VLAN IDs. • *vlan-id1*: specifies the first VLAN ID. • **to** *vlan-id2*: specifies the last VLAN ID. If **to** *vlan-id2* is not specified, learning of multicast group memberships is enabled only in the VLAN specified by *vlan-id1*.	The values of *vlan-id1* and *vlan-id2* are integers that range from 1 to 4094. The value of *vlan-id2* must be greater than the value of *vlan-id1*. The *vlan-id1* and *vlan-id2* parameters identify a range of VLANs.
all	Enables learning of multicast group memberships in all VLANs that an interface has joined.	-

Views

MultiGE interface view, Ethernet interface view, GE interface view, XGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, port group view, Eth-Trunk interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A group member port is a user-side interface that connects to multicast group members. Group memberships can be learned dynamically or configured statically. After IGMP snooping is enabled in a VLAN, all interfaces in the VLAN are enabled to learn forwarding entries from multicast packets. An interface is identified as a dynamic group member port when it receives an IGMP Report message.

If users connected to an interface need to receive data of a fixed multicast group, the interface can be statically bound to the multicast group. In this case, run the **undo igmp-snooping learning** command on the interface to disable learning of group memberships. This reduces the system resources used for protocol packet exchange.

Prerequisites

IGMP snooping has been enabled globally using the **igmp-snooping enable (system view)** command.

Precautions

The configuration takes effect only when all the following conditions are met:

- IGMP snooping is enabled in the VLAN using the **igmp-snooping enable (VLAN view)** command.
- The interface belongs to the specified VLANs.

If you run the **undo igmp-snooping learning** command multiple times, all the configurations take effect.

Example

Disable learning of group memberships in VLAN 3 and VLAN 4 on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] igmp-snooping enable
[HUAWEI] vlan 3
[HUAWEI-vlan3] igmp-snooping enable
[HUAWEI-vlan3] quit
[HUAWEI] vlan 4
[HUAWEI-vlan4] igmp-snooping enable
[HUAWEI-vlan4] quit
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] port link-type trunk
[HUAWEI-GigabitEthernet0/0/1] port trunk allow-pass vlan 3 to 4
[HUAWEI-GigabitEthernet0/0/1] undo igmp-snooping learning vlan 3 to 4
```


8.9.24 igmp-snooping limit-action

Function

The **igmp-snooping limit-action** command enables multicast entry overwriting on interfaces in a VLAN.

The **undo igmp-snooping limit-action** command disables multicast entry overwriting on interfaces in a VLAN.

By default, multicast entry overwriting is disabled on an interface. When the number of multicast entries on an interface reaches the limit, the switch does not process subsequent Report messages or replace the existing entries on the interface.

Format

igmp-snooping limit-action

undo igmp-snooping limit-action

Parameters

None

Views

VLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If the number of multicast groups on an interface or the switch reaches the limit, users connected to the interface or switch cannot join new multicast groups. To allow users to join new multicast groups in this case, enable multicast entry overwriting on interfaces in a VLAN.

After the configuration is complete, the switch records information about multicast users. When a user requests to join a new multicast group but the number of multicast groups on the interface or switch has reached the limit, the switch checks all the programs that the user has ordered. If a program is watched only by this user, the switch replaces the entry of this program with the entry of the new program.

Prerequisites

IGMP snooping has been enabled globally using the **igmp-snooping enable (system view)** command.

Precautions

To make the multicast entry overwriting configuration take effect, perform the following operations:

- Run the **igmp-snooping enable (VLAN view)** command to enable IGMP snooping in the VLAN.
- Run the **igmp-snooping group-limit** command to set the maximum number of multicast entries that an interface can learn.

The multicast entry overwriting function has the following limitations:

- When an interface is statically bound to a multicast group, the Layer 2 multicast entry overwriting function becomes invalid on the interface.
- The new multicast entry cannot replace the old one when the old multicast group has multiple multicast users or is a static multicast group.
- A new (S, G) entry can replace only an old (S, G), and a new (*, G) entry can replace only an old (*, G) entry.

Example

Enable multicast entry overwriting on interfaces in VLAN 2.

```
<HUAWEI> system-view
[HUAWEI] igmp-snooping enable
[HUAWEI] vlan 2
[HUAWEI-vlan2] igmp-snooping enable
[HUAWEI-vlan2] igmp-snooping limit-action
```

8.9.25 igmp-snooping max-response-time

Function

The **igmp-snooping max-response-time** command sets the maximum response time for IGMP General Query messages in a VLAN.

The **undo igmp-snooping max-response-time** command restores the default maximum response time for IGMP General Query messages in a VLAN.

By default, the maximum response time for IGMP General messages in a VLAN is 10 seconds.

Format

igmp-snooping max-response-time *max-response-time*

undo igmp-snooping max-response-time

Parameters

Parameter	Description	Value
max-response-time	Specifies the maximum response time for IGMP General Query messages.	The value is an integer that ranges from 1 to 25, in seconds. The default value is 10.

Views

VLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Setting IGMP snooping parameters helps improve the multicast forwarding performance. By setting the maximum response time for IGMP General Query messages, you can:

- Control the deadline for a host to send an IGMP Report message. When hosts are required to respond to IGMP General Query messages quickly, set a short maximum response time. To avoid congestion caused by a large number of IGMP messages sent by hosts, set a long maximum response time.
- Adjust the aging time of member ports. When the switch receives a Report message, it starts the aging timer for the member port. The aging time is calculated using the following formula: Aging time = General query count x General query interval + Maximum response time for General Query messages. The **igmp-snooping max-response-time** command sets the maximum response time. The General query count is set by the **igmp-snooping robust-count** command, and the general query interval is set by the **igmp-snooping query-interval** command.

The switch sets the maximum response time field in General Query messages to the value set by the **igmp-snooping max-response-time** command.

Prerequisites

IGMP snooping has been enabled globally using the **igmp-snooping enable (system view)** command.

Follow-up Procedure

Perform the following operations to improve multicast performance:

- Run the **igmp-snooping query-interval** command to set the interval at which General Query messages are sent.
- Run the **igmp-snooping lastmember-queryinterval** command to set the interval at which Group-Specific Query messages are sent.

Precautions

The configuration takes effect only after you run the **igmp-snooping enable (VLAN view)** command to enable IGMP snooping in the VLAN.

The maximum response time for General Query messages must be shorter than the interval at which General Query messages are sent. Otherwise, the switch will delete multicast memberships that should not be deleted.

Example

Set the maximum response time for IGMP Query messages in VLAN 3 to 20 seconds.

```
<HUAWEI> system-view
[HUAWEI] igmp-snooping enable
[HUAWEI] vlan 3
[HUAWEI-vlan3] igmp-snooping enable
[HUAWEI-vlan3] igmp-snooping max-response-time 20
```

8.9.26 igmp-snooping prompt-leave

Function

The **igmp-snooping prompt-leave** command enables the fast leave function in a VLAN so that member ports in the VLAN can fast leave multicast groups.

The **undo igmp-snooping prompt-leave** command disables the fast leave function in a VLAN.

By default, the fast leave function is disabled in a VLAN.

Format

igmp-snooping prompt-leave [**group-policy** *acl-number*]

undo igmp-snooping prompt-leave

Parameters

Parameter	Description	Value
group-policy	Specifies a multicast group policy that allows member ports to fast leave some multicast groups. Before using this parameter, create an ACL and configure filter rules in the ACL.	-
acl-number	Specifies the number of an ACL that defines a range of multicast groups. A basic or advanced ACL can be used.	The value is an integer that ranges from 2000 to 3999.

Views

VLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The fast leave function enables the switch to delete the multicast forwarding entry of a multicast group from an interface immediately after the interface receives an IGMP Leave message for the group. This function saves bandwidth and system resources because the switch does not need to wait until the aging timer of the interface expires.

Prerequisites

IGMP snooping has been enabled globally using the **igmp-snooping enable (system view)** command.

Precautions

When an interface has more than one receiver connected, enabling the fast leave function interrupts multicast traffic of the other receivers in the multicast group. It is recommended that you enable this function only on interfaces with one receiver.

The configuration takes effect only when all the following conditions are met:

- IGMP snooping is enabled in the VLAN using the **igmp-snooping enable (VLAN view)** command.
- IGMPv2 or IGMPv3 messages can be processed in the VLAN.
- If you do not specify **group-policy** when configuring the fast leave function, this function takes effect for all groups. To specify a group policy in the command, create an ACL and configure rules for the ACL before running the command.

Example

Allow member ports in VLAN 2 to fast leave all groups.

```
<HUAWEI> system-view
[HUAWEI] igmp-snooping enable
[HUAWEI] vlan 2
[HUAWEI-vlan2] igmp-snooping enable
[HUAWEI-vlan2] igmp-snooping prompt-leave
```

Allow member ports in VLAN 3 to fast leave group 225.1.1.123.

```
<HUAWEI> system-view
[HUAWEI] igmp-snooping enable
[HUAWEI] acl number 2000
[HUAWEI-acl-basic-2000] rule permit source 225.1.1.123 0
[HUAWEI-acl-basic-2000] quit
[HUAWEI] vlan 3
[HUAWEI-vlan3] igmp-snooping enable
[HUAWEI-vlan3] igmp-snooping prompt-leave group-policy 2000
```

Prevent member ports in VLAN 3 from fast leaving group 225.1.1.123.

```
<HUAWEI> system-view
[HUAWEI] igmp-snooping enable
[HUAWEI] acl number 2000
[HUAWEI-acl-basic-2000] rule deny source 225.1.1.123 0
[HUAWEI-acl-basic-2000] quit
```



```
[HUAWEI] vlan 3
[HUAWEI-vlan3] igmp-snooping enable
[HUAWEI-vlan3] igmp-snooping prompt-leave group-policy 2000
```

8.9.27 igmp-snooping host-based prompt-leave

Function

The **igmp-snooping host-based prompt-leave** command enables host-based fast leave in a VLAN.

The **undo igmp-snooping host-based prompt-leave** command disables host-based fast leave in a VLAN.

By default, host-based fast leave is disabled.

Format

igmp-snooping host-based prompt-leave

undo igmp-snooping host-based prompt-leave

Parameters

None

Views

VLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The host-based fast leave function enables a switch to delete a host from the host list of a group immediately after receiving an IGMP Leave message from the host. If the deleted host is the last receiver host connected to the member port, the switch deletes the forwarding entry of the group from the port, without waiting the aging timer of the port to expire. This conserves bandwidth and system resources.

Prerequisites

IGMP snooping has been enabled globally using the **igmp-snooping enable (system view)** command, then IGMP snooping has been enabled in the VLAN using the **igmp-snooping enable (VLAN view)** command.

Precautions

If a group member port is connected to multiple receiver hosts, the forwarding entry of the multicast group will be deleted without waiting for aging of the port only when the last receiver host leaves the group.

The configuration takes effect only when the switch can process IGMPv2 or IGMPv3 packets in the VLAN.

Example

Enable host-based fast leave in VLAN 2.

```
<HUAWEI> system-view
[HUAWEI] igmp-snooping enable
[HUAWEI] vlan 2
[HUAWEI-vlan2] igmp-snooping enable
[HUAWEI-vlan2] igmp-snooping host-based prompt-leave
```

8.9.28 igmp-snooping proxy

Function

The **igmp-snooping proxy** command enables IGMP snooping proxy in a VLAN.

The **undo igmp-snooping proxy** command disables IGMP snooping proxy in a VLAN.

By default, IGMP snooping proxy is disabled in a VLAN.

Format

igmp-snooping proxy

undo igmp-snooping proxy

Parameters

None

Views

VLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After IGMP snooping is enabled on a switch, the switch forwards Query messages from the upstream IGMP querier and Report/Leave messages from downstream hosts without changing the messages. When there are a large number of hosts on a network, redundant IGMP messages overload the upstream device. Enabling the IGMP snooping proxy function on the switch can solve this problem. This function allows the switch to send IGMP Query messages in place of the upstream Layer 3 device and send Report/Leave messages in place of downstream hosts, conserving link bandwidth between the Layer 3 device and switch. The switch sends IGMP Report/Leave messages to the upstream Layer 3 device only in the following situations:

- When the first member joins a multicast group or a host sends a Report message in response to an IGMP Query message, the Layer 2 device forwards a Report message to the upstream device. The upstream device can create or maintain the matching forwarding entry based on the Report message.
- When the last member of a multicast group leaves the group, the Layer 2 device forwards a Leave message to the upstream device. The upstream device then deletes the matching forwarding entry.

An upstream Layer 3 device does not send Query messages as a querier when IGMP is not enabled, for example, the Layer 3 device has only static multicast groups. In this case, the switch cannot create or maintain group memberships even though IGMP snooping is enabled. The IGMP snooping proxy function enables the switch to send Query messages to downstream hosts. For the hosts, the switch is a querier.

Prerequisites

IGMP snooping has been enabled globally using the **igmp-snooping enable (system view)** command.

Configuration Impact

If IGMP is enabled on the upstream Layer 3 device, enabling the IGMP snooping proxy function on the switch may affect the querier election result, because the General Query messages sent by the switch have a smaller source IP address than the General Query messages sent by the Layer 3 device. To solve this problem, run the **igmp-snooping proxy-uplink-port** command to prevent the switch from sending Query messages to the uplink interface connected to the upstream device. Alternatively, run the **igmp-snooping send-query source-address** command to set a large source IP address for Query messages.

Precautions

- The configuration takes effect only after you run the **igmp-snooping enable (VLAN view)** command to enable IGMP snooping in the VLAN.
- IGMP snooping proxy cannot be enabled in a VLAN if the corresponding VLANIF interface has Layer 3 multicast function (such as IGMP and PIM) enabled.
- After enabling IGMP snooping proxy in a VLAN, do not enable IGMP snooping querier or IGMP message suppression in the VLAN because these functions conflict.
- If multicast VLAN replication is configured on the switch, the IGMP snooping proxy function cannot be enabled in user VLANs.

Example

Enable IGMP snooping proxy in VLAN 100.

```
<HUAWEI> system-view
[HUAWEI] igmp-snooping enable
[HUAWEI] vlan 100
[HUAWEI-vlan100] igmp-snooping enable
[HUAWEI-vlan100] igmp-snooping proxy
```


8.9.29 igmp-snooping proxy-uplink-port

Function

The **igmp-snooping proxy-uplink-port** command configures an IGMP snooping proxy uplink interface. No IGMP Query message can be sent to this interface.

The **undo igmp-snooping proxy-uplink-port** command deletes an IGMP snooping proxy uplink interface.

By default, no IGMP snooping proxy uplink interface exists in a VLAN.

Format

igmp-snooping proxy-uplink-port vlan *vlan-id*

undo igmp-snooping proxy-uplink-port vlan *vlan-id*

Parameters

Parameter	Description	Value
vlan *vlan-id*	Specifies a VLAN ID.	The value is an integer that ranges from 1 to 4094.

Views

MultiGE interface view, Ethernet interface view, GE interface view, XGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, port group view, Eth-Trunk interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After IGMP snooping proxy or IGMP snooping querier is enabled in a VLAN, the switch periodically broadcasts IGMP Query messages to all interfaces in the VLAN, including router ports in the VLAN. This may result in IGMP querier reelection. To prevent IGMP querier reelection, run the **igmp-snooping proxy-uplink-port** command on the router port to disable the switch from sending IGMP Query messages to the router port.

Prerequisites

IGMP snooping has been enabled globally using the **igmp-snooping enable (system view)** command.

Precautions

Only one IGMP snooping proxy uplink interface can be configured in a VLAN.

The **igmp-snooping proxy-uplink-port** command is used only on an uplink interface. Therefore, the specified VLAN cannot be a user VLAN mapping the multicast VLAN.

Example

Configure GE0/0/1 in VLAN 10 as an IGMP snooping proxy uplink interface.

```
<HUAWEI> system-view
[HUAWEI] igmp-snooping enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] igmp-snooping proxy-uplink-port vlan 10
```

8.9.30 igmp-snooping querier enable

Function

The **igmp-snooping querier enable** command enables the IGMP snooping querier function in a VLAN.

The **undo igmp-snooping querier enable** command disables the IGMP snooping querier function in a VLAN.

By default, the IGMP snooping querier function is disabled in a VLAN.

Format

igmp-snooping querier enable

undo igmp-snooping querier enable

Parameters

None

Views

VLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On an IGMP-capable network, a Layer 3 multicast device functions as a querier to send IGMP Query messages and maintain group memberships on the local network segment. If the Layer 3 multicast device does not run IGMP or it uses only static multicast forwarding entries, it cannot function as a querier. In this case, you can enable IGMP snooping querier on the downstream Layer 2 device so that it acts as a querier to send IGMP Query messages.

On a Layer 2 network that has no Layer 3 devices, multicast sources are connected to Layer 2 devices. IGMP snooping querier needs to be enabled on the Layer 2 devices so that they can maintain multicast group memberships.

Prerequisites

IGMP snooping has been enabled globally using the **igmp-snooping enable (system view)** command.

Follow-up Procedure

Perform the following operations as required on your network:

- Run the **igmp-snooping query-interval** command to set the interval at which General Query messages are sent.
- Run the **igmp-snooping lastmember-queryinterval** command to set the interval at which Group-Specific Query messages are sent.
- Run the **igmp-snooping robust-count** command to set the number of times Query messages are sent.

Configuration Impact

The IGMP snooping querier does not participate in IGMP querier election. However, the IGMP snooping querier on an IGMP-capable multicast network may affect the election result, because the Query messages sent by the IGMP snooping querier may have a smaller source IP address than the Query messages sent by other devices. Therefore, the IGMP snooping querier function is not recommended on an IGMP-capable multicast network.

Precautions

- The configuration takes effect only after you run the **igmp-snooping enable (VLAN view)** command to enable IGMP snooping in the VLAN.
- The IGMP snooping querier function cannot be enabled in a VLAN if the corresponding Layer 3 VLANIF interface has Layer 3 multicast functions (such as IGMP and PIM) enabled.
- The IGMP snooping proxy and IGMP snooping querier functions cannot be enabled in the same VLAN.
- If multicast VLAN replication is configured on the switch, the IGMP snooping querier function cannot be enabled in user VLANs.

Example

Enable the querier function in VLAN 3.

```
<HUAWEI> system-view
[HUAWEI] igmp-snooping enable
[HUAWEI] vlan 3
[HUAWEI-vlan3] igmp-snooping enable
[HUAWEI-vlan3] igmp-snooping querier enable
Warning: Please confirm that no other querier is configured on the network, otherwise this command may cause querier re-election, continue? [Y/N]:y
```


8.9.31 igmp-snooping query-interval

Function

The **igmp-snooping query-interval** command sets the general query interval in a VLAN, that is, the interval at which IGMP General Query messages are sent in the VLAN.

The **undo igmp-snooping query-interval** command restores the default general query interval in a VLAN.

By default, the general query interval is 125 seconds.

Format

igmp-snooping query-interval *query-interval*

undo igmp-snooping query-interval

Parameters

Parameter	Description	Value
query-interval	Specifies the interval at which IGMP General Query messages are sent.	The value is an integer that ranges from 1 to 65535, in seconds.

Views

VLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

By setting the general query interval, you can:

- Configure the switch to send IGMP General Query messages at intervals to maintain memberships of interfaces. When a shorter interval is configured, the switch is more sensitive to multicast membership changes, but more bandwidth and system resources are consumed.
- Change the aging time of multicast member ports.

  When receiving an IGMP Report message from a host, the switch starts the aging timer for the multicast member port. The aging time is calculated using the following formula: Aging time = IGMP robustness variable x General query interval + Maximum response time for General Query messages. The **igmp-snooping query-interval** command sets the general query interval. The

general query count is set by the **igmp-snooping robust-count** command, and the maximum response time for General Query messages is set by the **igmp-snooping max-response-time** command.

The general query interval affects the aging time of group member ports. A shorter general query interval results in a shorter aging time of group member ports and therefore a faster update speed of Layer 2 multicast entries. However, when there are many downstream users connected to a device, a short general query interval can cause flapping of multicast entries, leading to a high CPU usage on the device. Therefore, the default general query interval is recommended. If you need to change the interval to suit service deployment, set the value according to the following table.

Number of IGMP Messages Sent from Downstream Users Within Maximum Response Time	Minimum General Query Interval Reference Value (Seconds)
1 to 1024	10
1024 to 2048	20
2048 to 5120	40

NOTE

The default general query interval defined in RFC documents is 125 seconds, but some vendors define their own default general query intervals. It is recommended that all devices on a multicast network use the same general query intervals (including IGMP and IGMP snooping general query intervals). On Huawei fixed switches, the default value of the IGMP general query interval is 60 seconds, and the default value of the IGMP snooping general query interval is 125 seconds.

Prerequisites

IGMP snooping has been enabled globally using the **igmp-snooping enable (system view)** command.

Precautions

- The configuration takes effect only after you run the **igmp-snooping enable (VLAN view)** command to enable IGMP snooping in the VLAN.
- The interval at which General Query messages are sent must be longer than the maximum response time for General Query messages. Otherwise, the switch will delete multicast memberships that should not be deleted.

Example

Set the general query interval in VLAN 3 to 100 seconds.

```
<HUAWEI> system-view
[HUAWEI] igmp-snooping enable
[HUAWEI] vlan 3
[HUAWEI-vlan3] igmp-snooping enable
[HUAWEI-vlan3] igmp-snooping query-interval 100
```


8.9.32 igmp-snooping report-suppress

Function

The **igmp-snooping report-suppress** command enables suppression of IGMP Report and Leave messages in a VLAN.

The **undo igmp-snooping report-suppress** command disables suppression of IGMP Report and Leave messages in a VLAN.

By default, IGMP Report and Leave message suppression is disabled in a VLAN.

Format

igmp-snooping report-suppress

undo igmp-snooping report-suppress

Parameters

None

Views

VLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When a Layer 2 device receives an IGMP Membership Report message (Report or Leave message) from a group member, the Layer 2 device forwards the message to the directly connected Layer 3 device. A group member host sends a Membership Report message in the following situations:

- When joining a multicast group, a host sends a Report message. When a multicast group has multiple members in a VLAN, the Layer 3 device receives duplicate Report messages from the member hosts.
- When receiving an IGMP General Query message, a host sends a Report message. Hosts use a timer to suppress duplicate Report messages on the same network segment. However, if the timer values on hosts are the same, the Layer 3 device can still receive duplicate Report messages.
- A host running IGMPv2 or IGMPv3 sends a Leave message when leaving a multicast group. When a multicast group has multiple members in a VLAN, the Layer 3 device receives duplicate Leave messages from the member hosts.

After Report message suppression is enabled on a Layer 2 device, the device forwards only one IGMP Membership Report message to the upstream device in the following scenarios:

- When the first member joins a multicast group or a host sends a Report message in response to an IGMP Query message, the Layer 2 device forwards a Report message to the upstream device. The upstream device can create or maintain the matching forwarding entry based on the Report message.
- When the last member of a multicast group leaves the group, the Layer 2 device forwards a Leave message to the upstream device. The upstream device then deletes the matching forwarding entry.

This reduces the number of IGMP messages on the network.

Prerequisites

IGMP snooping has been enabled globally using the **igmp-snooping enable (system view)** command.

Configuration Impact

- The configuration takes effect only after you run the **igmp-snooping enable (VLAN view)** command to enable IGMP snooping in the VLAN.
- When receiving a Leave message from a group member, the device sends Group-Specific Query messages to check whether the group has other members on the network segment.
- IGMP message suppression cannot be configured in a VLAN if the corresponding VLANIF interface has Layer 3 multicast function (such as IGMP and PIM) enabled.
- The functions of IGMP snooping proxy and IGMP message suppression cannot be configured in the same VLAN.
- If multicast VLAN replication is configured on the switch, the IGMP message suppression function cannot be enabled in user VLANs.
- The device can suppress duplicate Report messages even when IGMP message suppression is disabled. The default suppression time is 10 seconds. To change the suppression time, run the **igmp-snooping suppress-time** *suppress-time* command. If the *suppress-time* is set to 0, all the membership packets are forwarded immediately.
- This function cannot suppress IGMPv3 packets.

Example

Enable suppression of Report and Leave messages in VLAN 2.

```
<HUAWEI> system view
[HUAWEI] igmp-snooping enable
[HUAWEI] vlan 2
[HUAWEI-vlan2] igmp-snooping enable
[HUAWEI-vlan2] igmp-snooping report-suppress
```

8.9.33 igmp-snooping require-router-alert

Function

The **igmp-snooping require-router-alert** command configures the switch to drop the IGMP messages without the Router-Alert option in the IP header received from a VLAN.

The **undo igmp-snooping require-router-alert** command restores the default configuration.

By default, the switch does not check the Router-Alert option of IGMP messages and processes all the received IGMP messages, regardless of whether they carry the Router-Alert option in the IP header.

Format

igmp-snooping require-router-alert

undo igmp-snooping require-router-alert

Parameters

None

Views

VLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The Router-Alert option identifies the protocol messages that need to be processed by upper-layer routing protocols.

By default, the switch does not check whether IGMP messages contain the Router-Alert option and sends all the IGMP messages to the upper-layer routing protocol. After the **igmp-snooping require-router-alert** command is executed, the switch checks each IGMP message for the Router-Alert option and discards those IGMP messages without this option. This improves device performance, reduces cost, and enhances security of the upper-layer routing protocol

Prerequisites

IGMP snooping has been enabled globally using the **igmp-snooping enable (system view)** command.

Precautions

The configuration takes effect only after you run the **igmp-snooping enable (VLAN view)** command to enable IGMP snooping in the VLAN.

Example

Configure the switch to forward only the IGMP messages with the Router-Alert option in the IP header received from VLAN 3.

```
<HUAWEI> system-view
[HUAWEI] igmp-snooping enable
[HUAWEI] vlan 3
```



```
[HUAWEI-vlan3] igmp-snooping enable
[HUAWEI-vlan3] igmp-snooping require-router-alert
```

8.9.34 igmp-snooping robust-count

Function

The **igmp-snooping robust-count** command sets the IGMP robustness variable in a VLAN, which specifies how many times IGMP Query messages are sent.

The **undo igmp-snooping robust-count** command restores the default IGMP robustness variable in a VLAN.

By default, the robustness variable in a VLAN is 2.

Format

igmp-snooping robust-count *robust-count*

undo igmp-snooping robust-count

Parameters

Parameter	Description	Value
robust-count	Specifies the IGMP robustness variable in a VLAN.	The value is an integer that ranges from 2 to 5.

Views

VLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Setting IGMP snooping parameters helps improve the multicast forwarding performance. By setting the IGMP robustness variable, you can:

- Specify the number of times the querier sends a Group-Specific Query message, which prevents packet loss on the network.

  When receiving an IGMP Leave message for a multicast group, the switch sends a Group-Specific Query message a certain number of times (specified by the IGMP robustness variable) to check whether this group has any other members. If the quality of transmission links is low, increase the IGMP robustness variable.
- Change the aging time of multicast group member ports.

When receiving an IGMP Report message from a host, the switch starts the aging timer for the member port. The aging time is calculated using the following formula: Aging time = IGMP robustness variable x General query interval + Maximum response time for General Query messages. The **igmp-snooping robust-count** command sets the general query count.

Prerequisites

IGMP snooping has been enabled globally using the **igmp-snooping enable (system view)** command.

Follow-up Procedure

Perform the following operations to optimize multicast service performance:

- Run the **igmp-snooping query-interval** command to set the interval at which General Query messages are sent.
- Run the **igmp-snooping max-response-time** command to set the maximum response time for General Query messages.
- Run the **igmp-snooping lastmember-queryinterval** command to set the interval at which Group-Specific Query messages are sent.

Precautions

The configuration takes effect only after you run the **igmp-snooping enable (VLAN view)** command to enable IGMP snooping in the VLAN.

Example

Set the IGMP robustness variable to 5 in VLAN 3.

```
<HUAWEI> system-view
[HUAWEI] igmp-snooping enable
[HUAWEI] vlan 3
[HUAWEI-vlan3] igmp-snooping enable
[HUAWEI-vlan3] igmp-snooping robust-count 5
```

8.9.35 igmp-snooping router-aging-time

Function

The **igmp-snooping router-aging-time** command sets the aging time of dynamic router ports in a VLAN.

The **undo igmp-snooping router-aging-time** command restores the default aging time of dynamic router ports in a VLAN.

By default, the aging time of dynamic router ports in a VLAN is 180 seconds or equal to the holdtime value contained in PIM Hello messages.

Format

igmp-snooping router-aging-time *router-aging-time*

undo igmp-snooping router-aging-time

Parameters

Parameter	Description	Value
router-aging-time	Specifies the aging time of dynamic router ports in a VLAN.	The value is an integer that ranges from 1 to 1000, in seconds.

Views

VLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When a short-term congestion occurs on the network, it takes a longer time to transmit Query messages from the IGMP querier to the switch. If a router port on the switch ages in this period, the switch does not send Report or Leave messages to router ports. As a result, multicast data forwarding may be interrupted. Therefore, set a long aging time for the router port if the network is unstable.

When a dynamic router port on the switch receives an IGMP Query message or a PIM Hello message, the switch resets the aging time of the router port.

- If the router port receives an IGMP Query message, the switch sets the remaining aging time of the interface to the configured value.
- If the router port receives a PIM Hello message, the switch sets the aging time of the interface to the holdtime value.

Prerequisites

IGMP snooping has been enabled globally using the **igmp-snooping enable (system view)** command.

Precautions

If IGMP snooping is disabled in the specified VLAN, the configuration succeeds but does not take effect until IGMP snooping is enabled in the VLAN. To enable IGMP snooping in a VLAN, run the **igmp-snooping enable (VLAN view)** command.

If the aging time of a router port is too short, the router port ages frequently, degrading system performance.

Example

Set the aging time of router ports in VLAN 3 to 300 seconds.

```
<HUAWEI> system-view
[HUAWEI] igmp-snooping enable
[HUAWEI] vlan 3
```



```
[HUAWEI-vlan3] igmp-snooping enable
[HUAWEI-vlan3] igmp-snooping router-aging-time 300
```

8.9.36 igmp-snooping router-learning (interface view)

Function

The **igmp-snooping router-learning** command enables router port learning on an interface.

The **undo igmp-snooping router-learning** command disables router port learning on an interface.

By default, router port learning is enabled on an interface.

Format

igmp-snooping router-learning vlan { { *vlan-id1* [**to** *vlan-id2*] } &<1-10> | **all** }

undo igmp-snooping router-learning vlan { { *vlan-id1* [**to** *vlan-id2*] } &<1-10> | **all** }

Parameters

Parameter	Description	Value
vlan *vlan-id1* [**to** *vlan-id2*]	Enables an interface to function as a router port in the specified VLANs.	*vlan-id1* and *vlan-id2* are integers that range from 1 to 4094.
all	Enables an interface to function as a router port in all the VLANs.	-

Views

MultiGE interface view, Ethernet interface view, GE interface view, XGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, port group view, Eth-Trunk interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A router port is located on a Layer 2 device and connects to an upstream Layer 3 device (a multicast router or Layer 3 switch). A switch running IGMP snooping considers an interface as a dynamic router port when the interface receives an IGMP General Query message with any source IP address except 0.0.0.0 or a PIM Hello message. If the switch does not need to receive Query messages or PIM

Hello messages from a VLAN, disable router port learning in the VLAN. A router port provides the following functions:

- Receives multicast data from the upstream device.
- Forwards IGMP Report/Leave messages. IGMP Report/Leave messages received in a VLAN are forwarded only to router ports in the VLAN.

By default, router port learning is enabled on an interface. To prevent an interface from becoming a router port, disable router port learning on the interface.

Prerequisites

IGMP snooping has been enabled globally using the **igmp-snooping enable (system view)** command.

Follow-up Procedure

After router port learning is disabled on an interface, the interface no longer listens on IGMP Query or PIM Hello messages. Run the **igmp-snooping static-router-port** command to configure a static router port.

Precautions

- This command takes effect only when the interface has been added to the specified VLANs and IGMP snooping has been enabled in these VLANs using the **igmp-snooping enable (VLAN view)** command.
- You can also disable router port learning by running the **undo igmp-snooping router-learning (VLAN view)** command. The **undo igmp-snooping router-learning (VLAN view)** command is the same as the **undo igmp-snooping router-learning (interface view)** command only except for the scopes they take effect. The command used in the VLAN view disables router port learning on all interfaces in a VLAN, whereas the command used in the interface view disables router port learning on a specific interface in a VLAN.
- If the specified VLAN is bound to a BD, this command takes effect only in the VLAN, but not in the BD bound to the VLAN.

Example

Disable router port learning on GE0/0/1 in VLAN 10.

```
<HUAWEI> system-view
[HUAWEI] igmp-snooping enable
[HUAWEI] vlan 10
[HUAWEI-vlan10] igmp-snooping enable
[HUAWEI-vlan10] quit
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo igmp-snooping router-learning vlan 10
```

8.9.37 igmp-snooping router-learning (VLAN view)

Function

The **igmp-snooping router-learning** command enables router port learning in a VLAN.

The **undo igmp-snooping router-learning** command disables router port learning in a VLAN.

By default, router port learning is enabled in a VLAN.

Format

igmp-snooping router-learning

undo igmp-snooping router-learning

Parameters

None

Views

VLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A router port is located on a Layer 2 device and connects to an upstream Layer 3 device (a multicast router or Layer 3 switch). A switch running IGMP snooping considers an interface as a dynamic router port when the interface receives an IGMP General Query message with any source IP address except 0.0.0.0 or a PIM Hello message. If the switch does not need to receive Query messages or PIM Hello messages from a VLAN, disable router port learning in the VLAN. A router port provides the following functions:

- Receives multicast data from the upstream device.
- Forwards IGMP Report/Leave messages. IGMP Report/Leave messages received in a VLAN are forwarded only to router ports in the VLAN.

By default, router port learning is enabled on an interface. To prevent interfaces in a VLAN from becoming a router port, disable router port learning in the VLAN.

Prerequisites

IGMP snooping has been enabled globally using the **igmp-snooping enable (system view)** command.

Follow-up Procedure

The switch does not listen on IGMP Query or PIM Hello messages in a VLAN after router port learning is disabled in the VLAN. To ensure normal multicast forwarding in the VLAN, run the **igmp-snooping static-router-port** command to configure a static router port.

Precautions

If IGMP snooping is disabled in the specified VLAN, the configuration succeeds but does not take effect until IGMP snooping is enabled in the VLAN. To enable IGMP snooping in a VLAN, run the **igmp-snooping enable (VLAN view)** command.

You can also disable router port learning by running the **undo igmp-snooping router-learning (interface view)** command. The **undo igmp-snooping router-learning (interface view)** command is the same as the **undo igmp-snooping router-learning (VLAN view)** command only except for the scope they take effect. The command used in the VLAN view disables router port learning on all interfaces in a VLAN, whereas the command used in the interface view disables router port learning on a specific interface in a VLAN.

When inter-VLAN multicast replication is enabled on the switch, enable router port learning in user VLANs.

Example

Disable router port learning in VLAN 3.

```
<HUAWEI> system-view
[HUAWEI] igmp-snooping enable
[HUAWEI] vlan 3
[HUAWEI-vlan3] igmp-snooping enable
[HUAWEI-vlan3] undo igmp-snooping router-learning
```

8.9.38 igmp-snooping send-query enable

Function

The **igmp-snooping send-query enable** command enables the switch to send IGMP General Query messages to non-router ports when receiving topology change events.

The **undo igmp-snooping send-query enable** command disables the switch from sending IGMP General Query messages to non-router ports.

By default, the switch does not send IGMP General Query messages to non-router ports when receiving topology change events.

Format

igmp-snooping send-query enable

undo igmp-snooping send-query enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the network topology changes, the switch receives a topology change event. By default, the switch does not send IGMP General Query messages in this case. A network topology change triggers recalculation of the ring network protocol used (such as STP, MSTP, RRPP, SEP, and Smart Link), but multicast data packets cannot be switched to the new path immediately. To enable multicast data flows to be switched to the new forwarding path immediately after a network topology change, configure the switch to send IGMP General Query messages upon topology changes.

Prerequisites

IGMP snooping has been enabled globally using the **igmp-snooping enable (system view)** command.

Follow-up Procedure

This command is used on a ring network. When the ring network topology changes, the switch sends IGMP General Query messages with source IP address 192.168.0.1. When this address has been occupied by another device on the network, run the **igmp-snooping send-query source-address** command to change the source IP address.

Precautions

Use this command only when a ring network protocol is enabled on the switch.

Example

Configure the switch to send IGMP General Query messages upon topology changes.

```
<HUAWEI> system-view
[HUAWEI] igmp-snooping enable
[HUAWEI] igmp-snooping send-query enable
```

8.9.39 igmp-snooping send-query source-address

Function

The **igmp-snooping send-query source-address** command sets the source IP address of IGMP Query messages.

The **undo igmp-snooping send-query source-address** command restores the default source IP address of IGMP Query messages.

By default, the source IP address of IGMP Query messages is 192.168.0.1.

Format

igmp-snooping send-query source-address *ip-address*

undo igmp-snooping send-query source-address

Parameters

Parameter	Description	Value
ip-address	Specifies the source IP address of IGMP Query messages.	The value is in dotted decimal notation.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

IGMP Query messages include General Query messages, Group-Specific Query messages, and Group-and-Source-Specific Query messages. A Layer 2 device sends two types of IGMP General Query messages:

- IGMP General Query messages sent by the querier when the querier function is enabled using the **igmp-snooping proxy** or **igmp-snooping querier enable** command.
- IGMP General Query messages that the Layer 2 device sends after receiving Layer 2 topology change events (configured using the **igmp-snooping send-query enable** command).

By default, IGMP Query messages sent from a Layer 2 device use the source IP address 192.168.0.1. When this IP address is used by another device on the network, run the **igmp-snooping send-query source-address** command to change the source IP address of IGMP Query messages.

When multiple Layer 2 devices exist on a shared network, you can set source IP addresses of IGMP Query messages to identify the devices. For example, when multiple devices with different performance need to participate in querier election, you must configure a different source IP address of IGMP Query messages for each device.

When the IGMP proxy function is enabled on a device using the **igmp-snooping proxy** command or the function of suppressing Report and Leave messages is enabled in a VLAN using the **igmp-snooping report-suppress** command, the device sends IGMP Report and IGMP Leave messages on behalf of downstream users, with the default source IP address of the IGMP Report and IGMP Leave messages being 192.168.0.1. You can run this command to change the source IP address of IGMP Report and IGMP Leave messages.

Prerequisites

IGMP snooping has been enabled globally using the **igmp-snooping enable (system view)** command.

Example

Set the source IP address of IGMP Query messages sent by the switch to 192.168.0.2.

```
<HUAWEI> system-view
[HUAWEI] igmp-snooping enable
[HUAWEI] igmp-snooping send-query source-address 192.168.0.2
```

8.9.40 igmp-snooping send-router-alert

Function

The **igmp-snooping send-router-alert** command configures the switch to send IGMP messages with the Router-Alert option in the IP header to a VLAN.

The **undo igmp-snooping send-router-alert** command configures the switch to send IGMP messages without the Router-Alert option in the IP header to a VLAN.

By default, the switch sends IGMP messages with the Router-Alert option in the IP header.

Format

igmp-snooping send-router-alert

undo igmp-snooping send-router-alert

Parameters

None

Views

VLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The Router-Alert option identifies the protocol messages that need to be processed by upper-layer routing protocols.

By default, the switch sends IGMP messages with the Router-Alert option. If some devices in the same VLAN as the switch can process only the IGMP messages without the Router-Alert option, use the **undo igmp-snooping send-router-alert** command to configure the switch to send IGMP messages without the Router-Alert option.

The switch adds the Router-Alert option only to locally originated IGMP messages and does not add this option to IGMP messages received from other devices.

Prerequisites

IGMP snooping has been enabled globally using the **igmp-snooping enable (system view)** command.

Precautions

If IGMP snooping is disabled in the specified VLAN, the configuration succeeds but does not take effect until IGMP snooping is enabled in the VLAN. To enable IGMP snooping in a VLAN, run the **igmp-snooping enable (VLAN view)** command.

Example

Configure the switch to send IGMP messages that do not contain the Router-Alert option in the IP header to VLAN 3.

```
<HUAWEI> system-view
[HUAWEI] igmp-snooping enable
[HUAWEI] vlan 3
[HUAWEI-vlan3] igmp-snooping enable
[HUAWEI-vlan3] undo igmp-snooping send-router-alert
```

8.9.41 igmp-snooping ssm-mapping

Function

The **igmp-snooping ssm-mapping** command configures the mapping between a multicast group and a multicast source in a VLAN.

The **undo igmp-snooping ssm-mapping** command deletes the mapping between a multicast group and a multicast source in a VLAN.

By default, no mappings between multicast groups and multicast sources exist in a VLAN.

Format

igmp-snooping ssm-mapping *group-address* { *group-mask* | *mask-length* } *source-address*

undo igmp-snooping ssm-mapping *group-address* { *group-mask* | *mask-length* } *source-address*

Parameters

Parameter	Description	Value
group-address	Specifies the IP address of a multicast group.	The value is in dotted decimal notation, and the value range is specified by the **igmp-snooping ssm-policy** command.
group-mask	Specifies the mask of the multicast group address.	The value is in dotted decimal notation.

Parameter	Description	Value
mask-length	Specifies the mask length of the multicast group address.	The value is an integer that ranges from 4 to 32.
source-address	Specifies the IP address of the multicast source mapped to a multicast group.	The value is in dotted decimal notation.

Views

VLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The SSM mapping mechanism converts IGMPv1 and IGMPv2 Report messages into messages with (S, G) information. This mechanism enables hosts that do not support IGMPv3 to work with SSM. To use this mechanism, enable SSM mapping and configure mappings between a multicast group G and multicast sources such as S1, S2 on the Layer 2 device connected to user hosts. When the Layer 2 device receives IGMPv1 and IGMPv2 Report messages for a multicast group, it checks the group address of the messages. If the group address is in the SSM group range, the Layer 2 device converts the messages into one or more IGMPv3 IS_IN (S1, S2...) messages with the group address G.

Prerequisites

- IGMP snooping has been enabled globally using the **igmp-snooping enable (system view)** command.

Precautions

Before configuring the mapping between a multicast group and a multicast source:

- IGMP snooping has been enabled in the specified VLAN using the **igmp-snooping enable (VLAN view)** command.
- The IGMP message version is set to IGMPv3 using the **igmp-snooping version** command in the VLAN.
- SSM mapping has been enabled using the **igmp-snooping ssm-mapping enable** command.
- An SSM group policy has been configured using the **igmp-snooping ssm-policy** command in the VLAN to add the multicast group address to the SSM group range. This prerequisite is required when the multicast group address is an any-source multicast (ASM) address.

Example

Map multicast groups 238.1.1.1 through 238.1.1.255 to multicast source 10.1.1.1 in VLAN 10.

```
<HUAWEI> system-view
[HUAWEI] igmp-snooping enable
[HUAWEI] vlan 10
[HUAWEI-vlan10] igmp-snooping enable
[HUAWEI-vlan10] igmp-snooping version 3
[HUAWEI-vlan10] igmp-snooping ssm-mapping enable
[HUAWEI-vlan10] igmp-snooping ssm-mapping 238.1.1.0 24 10.1.1.1
```

8.9.42 igmp-snooping ssm-mapping enable

Function

The **igmp-snooping ssm-mapping enable** command enables Source-Specific Multicast (SSM) mapping in a VLAN.

The **undo igmp-snooping ssm-mapping enable** command disables SSM mapping in a VLAN.

By default, SSM mapping is disabled in a VLAN.

Format

igmp-snooping ssm-mapping enable

undo igmp-snooping ssm-mapping enable

Parameters

None

Views

VLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On an SSM network, hosts running IGMPv1 or IGMPv2 cannot select multicast sources when they join a multicast group. To provide SSM services for these hosts, enable SSM mapping on the Layer 2 devices connected to the hosts.

Prerequisites

IGMP snooping has been enabled globally using the **igmp-snooping enable (system view)** command.

Follow-up Procedure

Run the **igmp-snooping ssm-mapping** command to configure group-source mappings.

Precautions

- If IGMP snooping is disabled in the specified VLAN, the configuration succeeds but does not take effect until IGMP snooping is enabled in the VLAN. To enable IGMP snooping in a VLAN, run the **igmp-snooping enable (VLAN view)** command.
- SSM mapping is applicable only to the VLANs where IGMP snooping can process IGMPv3 messages. To set the IGMP message version to v3, use the **igmp-snooping version** command in the VLAN.
- If the multicast group address is an Any-Source Multicast (ASM) address, configure an SSM group policy to add the multicast group address to the SSM group range using the **igmp-snooping ssm-policy** command in the VLAN view.
- If the inter-VLAN multicast replication function is configured, you only need to configure SSM mapping in the multicast VLAN.

Example

Enable SSM mapping in VLAN 10.

```
<HUAWEI> system-view
[HUAWEI] igmp-snooping enable
[HUAWEI] vlan 10
[HUAWEI-vlan10] igmp-snooping enable
[HUAWEI-vlan10] igmp-snooping version 3
[HUAWEI-vlan10] igmp-snooping ssm-mapping enable
```

8.9.43 igmp-snooping ssm-policy

Function

The **igmp-snooping ssm-policy** command configures an SSM group policy in a VLAN to specify the range of SSM groups.

The **undo igmp-snooping ssm-policy** command deletes the SSM group policy from a VLAN.

By default, no SSM group policy is available in a VLAN.

Format

igmp-snooping ssm-policy *basic-acl-number*

undo igmp-snooping ssm-policy

Parameters

Parameter	Description	Value
basic-acl-number	Specifies the number of a basic ACL that defines the range of SSM groups.	The value is an integer that ranges from 2000 to 2999.

Views

VLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

SSM allows multicast group addresses in the range of 232.0.0.0 to 232.255.255.255. If hosts need to join multicast groups out of this range or they are allowed to join only some of multicast groups in the range, configure an SSM group range for the hosts.

Prerequisites

IGMP snooping has been enabled globally using the **igmp-snooping enable (system view)** command.

Precautions

The **igmp-snooping ssm-policy** command takes effect only when the following configurations are complete:

- IGMP snooping has been enabled in the specified VLAN using the **igmp-snooping enable (VLAN view)** command.
- SSM mapping has been enabled in the specified VLAN using the **igmp-snooping ssm-mapping enable** command.
- If IGMPv1 or IGMPv2 packets are sent by user hosts, the IGMP message version is set to IGMPv3 using the **igmp-snooping version** command in the VLAN.
- The ACL has been created and configured rules for the ACL. By default, the ACL applied to an SSM group policy denies all multicast groups. Therefore, to exclude specific group addresses from the SSM group address range, use a **rule permit source any** rule with **deny** rules in the ACL. For details about ACL configuration commands, see **14.1 ACL Configuration Commands**.

Example

Specify multicast group 225.1.1.123 as an SSM group in VLAN 3.

```
<HUAWEI> system-view
[HUAWEI] acl number 2000
[HUAWEI-acl-basic-2000] rule permit source 225.1.1.123 0
[HUAWEI-acl-basic-2000] quit
[HUAWEI] igmp-snooping enable
[HUAWEI] vlan 3
[HUAWEI-vlan3] igmp-snooping enable
[HUAWEI-vlan3] igmp-snooping ssm-mapping enable
[HUAWEI-vlan3] igmp-snooping ssm-policy 2000
```


8.9.44 igmp-snooping static-group suppress-dynamic-join

Function

The **igmp-snooping static-group suppress-dynamic-join** command disables a device from forwarding IGMP Report and Leave messages that are received from a VLAN and contain a static group address to upstream Layer 3 devices configured with the static group address.

The **undo igmp-snooping static-group suppress-dynamic-join** command enables a device to forward IGMP Report and Leave messages that are received from a VLAN and contain a static group address to upstream Layer 3 devices configured with the static group address.

By default, a device forwards IGMP Report and Leave messages that are received from a VLAN and contain a static group address to upstream Layer 3 devices configured with the static group address.

Format

igmp-snooping static-group suppress-dynamic-join

undo igmp-snooping static-group suppress-dynamic-join

Parameters

None

Views

VLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If the upstream Layer 3 multicast device is a non-Huawei device and a static group is configured on its interface connected to the device, users cannot dynamically join or leave the multicast group. You must disable the device from sending Report and Leave messages that contain static group addresses to the Layer 3 multicast device.

This function takes effect only for IGMPv1 and IGMPv2 message and is invalid for IGMPv3 messages.

Prerequisites

IGMP snooping has been enabled globally using the **igmp-snooping enable (system view)** command.

Precautions

If IGMP snooping is disabled in the specified VLAN, the configuration succeeds but does not take effect until IGMP snooping is enabled in the VLAN. To enable IGMP snooping in a VLAN, run the **igmp-snooping enable (VLAN view)** command.

Example

Disable a device from forwarding IGMP Report and Leave messages that are received from VLAN 10 and contain a static group address to upstream Layer 3 devices configured with the static group address.

```
<HUAWEI> system-view
[HUAWEI] igmp-snooping enable
[HUAWEI] vlan 10
[HUAWEI-vlan10] igmp-snooping enable
[HUAWEI-vlan10] igmp-snooping static-group suppress-dynamic-join
```

8.9.45 igmp-snooping static-router-port

Function

The **igmp-snooping static-router-port** command configures an interface as a static router port in specified VLANs.

The **undo igmp-snooping static-router-port** command cancels the router port configuration in specified VLANs.

By default, an interface is not a static router port.

Format

igmp-snooping static-router-port vlan { *vlan-id1* [**to** *vlan-id2*] } &<1-10>

undo igmp-snooping static-router-port vlan { { *vlan-id1* [**to** *vlan-id2*] } &<1-10> | **all** }

Parameters

Parameter	Description	Value
vlan { *vlan-id1* [**to** *vlan-id2*] } &<1-10>	Specifies VLAN IDs. This parameter specifies in which VLANs the current interface functions as a router port. • *vlan-id1* specifies the first VLAN ID. • **to** *vlan-id2* specifies the last VLAN ID. If **to** *vlan-id2* is not specified, the interface functions as a router port only in the VLAN specified by *vlan-id1*.	The value is an integer that ranges from 1 to 4094. The value of vlan-id2 must be greater than the value of vlan-id1. The vlan-id1 and vlan-id2 parameters identify a range of VLANs.

Parameter	Description	Value
all	Cancels the static router port configuration in all VLANs on the interface.	-

Views

MultiGE interface view, Ethernet interface view, GE interface view, XGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, port group view, Eth-Trunk interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When an interface needs to keep forwarding IGMP Report/Leave messages for a long time, configure the interface as a static router port.

Prerequisites

IGMP snooping has been enabled globally using the **igmp-snooping enable (system view)** command.

Precautions

This command takes effect only when the interface is added to the specified VLANs.

If you run the **igmp-snooping static-router-port** command multiple times, all the configurations take effect.

Example

Configure GE0/0/1 as a static router port in VLAN 2.

```
<HUAWEI> system-view
[HUAWEI] igmp-snooping enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] igmp-snooping static-router-port vlan 2
```

8.9.46 igmp-snooping suppress-time

Function

The **igmp-snooping suppress-time** command sets the IGMP message suppression time in a VLAN.

The **undo igmp-snooping suppress-time** command restores the default IGMP message suppression time in a VLAN.

By default, the IGMP message suppression time is 10 seconds.

Format

igmp-snooping suppress-time *suppress-time*

undo igmp-snooping suppress-time

Parameters

Parameter	Description	Value
suppress-time	Specifies the IGMP message suppression time in a VLAN.	The value is an integer that ranges from 0 to 300, in seconds. The value 0 indicates that IGMP messages are not suppressed.

Views

VLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To reduce the IGMP messages sent from a Layer 2 device to the upstream Layer 3 device and protect the Layer 3 device from attacks, enable the Layer 2 device to suppress IGMP Report and IGMP Leave messages sent by hosts in a VLAN. After this function is enabled, the Layer 2 device processes IGMP Report and IGMP Leave messages as follows:

- After receiving an IGMP Report/Leave message and forwarding the message, the Layer 2 device does not forward the same type of messages to the router port within the suppression time.
- If the Layer 2 device receives an IGMP General Query message or Group-Specific message, it does not suppress the first IGMP Report message that responds to the General Query message. In addition, the Layer 2 device resets the suppression timer when it receives the first IGMP Report message.

Prerequisites

IGMP snooping has been enabled globally using the **igmp-snooping enable (system view)** command.

Follow-up Procedure

Run the **igmp-snooping max-response-time** command to set the maximum response time for General Query messages. It is recommended that the

suppression time be the same as the maximum response time for IGMP Query messages in a VLAN.

Precautions

The configuration takes effect only after you run the **igmp-snooping enable (VLAN view)** command to enable IGMP snooping in the VLAN.

The configured suppression time is invalid for IGMPv3 messages.

Example

Set the IGMP message suppression time in VLAN 2 to 15 seconds.

```
<HUAWEI> system-view
[HUAWEI] igmp-snooping enable
[HUAWEI] vlan 2
[HUAWEI-vlan2] igmp-snooping enable
[HUAWEI-vlan2] igmp-snooping suppress-time 15
```

8.9.47 igmp-snooping version

Function

The **igmp-snooping version** command configures the version of IGMP messages that IGMP snooping can process in a VLAN.

The **undo igmp-snooping version** command restores the default IGMP message version.

By default, the IGMP snooping version is 2, indicating that IGMP snooping can process IGMPv1 and IGMPv2 messages.

Format

igmp-snooping version { **1** | **2** | **3** [**mode asm-ssm**] }

undo igmp-snooping version

Parameters

Parameter	Description	Value
1	Indicates that IGMP snooping only processes IGMPv1 messages.	-
2	Indicates that IGMP snooping processes both IGMPv1 and IGMPv2 messages.	-
3	Indicates that IGMP snooping processes IGMPv1, IGMPv2, and IGMPv3 messages.	-

Parameter	Description	Value
mode asm-ssm	Indicates that when IGMPv3 is configured, the ASM-SSM model is used.	If this parameter is not specified, the SSM model is used when IGMPv3 is configured.

Views

VLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The IGMP protocol maintains group memberships between Layer 3 multicast devices and hosts. IGMP has three versions: v1, v2, and v3. This command specifies the version of IGMP messages that IGMP snooping can process. Generally, configure the same version on the Layer 2 device as that on the upstream Layer 3 multicast device. If IGMP is not enabled on the Layer 3 multicast device, configure the IGMP message version on the Layer 2 device to be later than or equal to the version running on downstream hosts.

When hosts in a VLAN run different IGMP versions, run the **igmp-snooping version** command to enable the Layer 2 device to process IGMP messages sent from all the hosts.

Table 8-124 compares how Report messages are processed in the ASM and ASM-SSM models when IGMPv3 is configured.

Table 8-124 Difference in Report message processing in SSM and ASM-SSM models

Multicast Address in a Report Message	Filtering Action	Processing Mode in the SSM Model	Processing Mode in the ASM-SSM Model
SSM group address, for example, 232.1.1.1	INCLUDE	The message is processed normally and the (S, G) entry is generated.	The message is processed normally and the (S, G) entry is generated.
SSM group address, for example, 232.1.1.1	EXCLUDE	The message is considered invalid and discarded.	The message is considered invalid and discarded.

Multicast Address in a Report Message	Filtering Action	Processing Mode in the SSM Model	Processing Mode in the ASM-SSM Model
ASM group address, for example, 225.1.1.1	INCLUDE	The message is considered invalid and discarded.	The message is processed normally and the (S, G) entry is generated.
ASM group address, for example, 225.1.1.1	EXCLUDE (None)	The message is processed normally and the (*, G) entry is generated.	The message is processed normally and the (*, G) entry is generated.
ASM group address, for example, 225.1.1.1	EXCLUDE (Source)	The message is processed, and the (*, G) entry is generated. However, the expected result cannot be achieved.	The message is processed normally, and the INCLUDE (*, G) and EXCLUDE (S, G) entries are generated, which are consistent with the expected result.

Prerequisites

IGMP snooping has been enabled globally using the **igmp-snooping enable (system view)** command.

Precautions

- If IGMP snooping is disabled in the specified VLAN, the configuration succeeds but does not take effect until IGMP snooping is enabled in the VLAN. To enable IGMP snooping in a VLAN, run the **igmp-snooping enable (VLAN view)** command.
- When the IGMP snooping version is set to IGMPv3:
  - The switch can use only the default Layer 2 multicast forwarding mode.
  - The S1720GW-E, S1720GWR-E, S5720-LI, S5720S-LI, S5720I-SI, S5735S-H, S5736-S, and S6720S-S forward multicast data by looking up the forwarding table according to the VLAN ID and group address.
- This command cannot be used in user VLANs of a multicast VLAN.
- If the IGMP message version is changed from IGMPv3 to IGMPv2, the system deletes all the dynamic IGMP snooping entries when the aging time expires and processes static IGMP snooping entries as follows:
  - Does not delete static entries that have only multicast groups and no multicast sources.
  - Deletes the static entries that have both multicast groups and multicast sources. When the IGMP message version is restored to IGMPv3, the system restores these entries.

- Before modifying the service model used when IGMP snooping v3 is configured, run the **undo igmp-snooping enable** command in the VLAN view to disable IGMP snooping in the VLAN.
- After the **igmp-snooping version 3 mode asm-ssm** command is configured in a VLAN, no (S, G) entry can be generated if the **l2-multicast static-group** command is run to add an interface to a specified multicast group with a non-SSM multicast address to receive multicast packets from a multicast source. For example, when the **igmp-snooping version 3 mode asm-ssm** command is configured in VLAN 10 and the **l2-multicast static-group source-address 2.1.1.1 group-address 225.0.0.1 vlan 10** command is configured on an interface, the (2.1.1.1, 225.0.0.1) entry cannot be generated.

Example

Set the version of the IGMP messages that can be processed by IGMP snooping to IGMPv1 in VLAN 2.

```
<HUAWEI> system-view
[HUAWEI] igmp-snooping enable
[HUAWEI] vlan 2
[HUAWEI-vlan2] igmp-snooping enable
[HUAWEI-vlan2] igmp-snooping version 1
```

8.9.48 l2-multicast forwarding-mode

Function

The **l2-multicast forwarding-mode** command configures the forwarding mode of multicast data in a VLAN.

The **undo l2-multicast forwarding-mode** command restores the default forwarding mode of multicast data.

By default, multicast data is forwarded in a VLAN based on IP addresses.

Format

l2-multicast forwarding-mode { **ip** | **mac** }

undo l2-multicast forwarding-mode mac

Parameters

Parameter	Description	Value
ip	Forwards multicast data based on IP addresses.	-
mac	Forwards multicast data based on MAC addresses.	-

Views

VLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After Layer 2 multicast is enabled on a Layer 2 device, the Layer 2 device maintains a Layer 2 multicast forwarding table. When receiving a multicast packet, the Layer 2 device searches the Layer 2 multicast forwarding table for the outbound interface based on the multicast address of the packet. The Layer 2 device determines the outbound interface based on the IP multicast address or IP multicast MAC address, depending on the configured Layer 2 multicast forwarding mode.

Multiple multicast IP addresses may be mapped to one MAC address. If multicast data is forwarded based on MAC addresses, multicast data may be sent to the users who do not require the multicast data. To prevent this problem, use the IP address-based forwarding mode on devices with Layer 3 functions.

Configuration Impact

To set the IGMP snooping version to IGMPv3 or the MLD snooping version to MLDv2, do not change the default forwarding mode using this command.

After the multicast data forwarding mode is set to MAC address-based forwarding in a VLAN using this command, the VLAN cannot be configured as a multicast VLAN.

Precautions

- This command can only be used in VLANs with Layer 2 multicast snooping disabled. After running this command in a VLAN, enable Layer 2 multicast snooping in the VLAN for the configuration to take effect.
  - On an IPv4 network, run the **igmp-snooping enable (VLAN view)** command to enable IGMP snooping in the VLAN.
  - On an IPv6 network, run the **mld-snooping enable** command to enable MLD snooping in the VLAN.

Example

After IGMP snooping is enabled globally, configure the switch to forward multicast data in VLAN 100 based on MAC addresses.

```
<HUAWEI> system-view
[HUAWEI] igmp-snooping enable
[HUAWEI] vlan 100
[HUAWEI-vlan100] l2-multicast forwarding-mode mac
[HUAWEI-vlan100] igmp-snooping enable
```

After MLD snooping is enabled globally, configure the switch to forward multicast data in VLAN 100 based on MAC addresses.

```
<HUAWEI> system-view
[HUAWEI] mld-snooping enable
[HUAWEI] vlan 100
[HUAWEI-vlan100] l2-multicast forwarding-mode mac
[HUAWEI-vlan100] mld-snooping enable
```


8.9.49 l2-multicast router-port-discard

Function

The **l2-multicast router-port-discard** command disables the switch from sending multicast data to routed ports in a VLAN.

The **undo l2-multicast router-port-discard** command restores the default configuration.

By default, multicast data can be forwarded to routed ports in a VLAN.

Format

l2-multicast router-port-discard

undo l2-multicast router-port-discard

Parameters

None

Views

VLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In some scenarios, multicast data does not need to be forwarded to routed ports in a VLAN. For example, when all interfaces on a switch are configured as static router ports in a VLAN, you can use this command to conserve bandwidth by preventing multicast data from being sent to these interfaces.

Precautions

This command can only be used in VLANs with Layer 2 multicast snooping disabled. After running this command in a VLAN, enable Layer 2 multicast snooping in the VLAN for the configuration to take effect.

- On an IPv4 network, run the **igmp-snooping enable (VLAN view)** command to enable IGMP snooping in the VLAN.
- On an IPv6 network, run the **mld-snooping enable** command to enable MLD snooping in the VLAN.

Example

Disable the switch from forwarding multicast data to routed ports in VLAN 10 on an IPv4 network.


```
<HUAWEI> system-view
[HUAWEI] igmp-snooping enable
[HUAWEI] vlan 10
[HUAWEI-vlan10] l2-multicast router-port-discard
[HUAWEI-vlan10] igmp-snooping enable
```

Disable the switch from forwarding multicast data to routed ports in VLAN 10 on an IPv6 network.

```
<HUAWEI> system-view
[HUAWEI] mld-snooping enable
[HUAWEI] vlan 10
[HUAWEI-vlan10] l2-multicast router-port-discard
[HUAWEI-vlan10] mld-snooping enable
```

8.9.50 l2-multicast static-group

Function

The **l2-multicast static-group** command configures static group memberships on an interface.

The **undo l2-multicast static-group** command deletes static group memberships from an interface.

By default, no static group membership is configured on an interface.

Format

Configure a single static multicast group:

l2-multicast static-group [**source-address** *source-ip-address*] **group-address** *group-ip-address* **vlan** { *vlan-id1* [**to** *vlan-id2*] } &<1-10>

undo l2-multicast static-group [**source-address** *source-ip-address*] **group-address** *group-ip-address* **vlan** { **all** | { *vlan-id1* [**to** *vlan-id2*] } &<1-10> }

Configure a series of static multicast groups:

l2-multicast static-group [**source-address** *source-ip-address*] **group-address** *group-ip-address1* **to** *group-ip-address2* **vlan** *vlan-id*

undo l2-multicast static-group [**source-address** *source-ip-address*] **group-address** *group-ip-address1* **to** *group-ip-address2* **vlan** *vlan-id*

undo l2-multicast static-group [**source-address** *source-ip-address*] **group-address all vlan** { **all** | { *vlan-id1* [**to** *vlan-id2*] } &<1-10> }

Parameters

Parameter	Description	Value
source-address *source-ip-address*	Specifies the IP address of a multicast source.	The value of *source-ip-address* can be any Class A, Class B, or Class C address, in dotted decimal notation.

Parameter	Description	Value
group-address *group-ip-address*	Specifies the IP address of a multicast group.	The value of *group-ip-address* ranges from 224.0.1.0 to 239.255.255.255 in dotted decimal notation.
vlan { *vlan-id1* [**to** *vlan-id2*] }	Specifies the VLANs that the interface belongs to. *vlan-id1* [**to** *vlan-id2*] specifies a range of VLAN IDs. • *vlan-id1* specifies the first VLAN ID. • **to** *vlan-id2* specifies the last VLAN ID. If **to** *vlan-id2* is not specified, the interface is bound only to the multicast group in the VLAN specified by *vlan-id1*.	The values of *vlan-id1* and *vlan-id2* are integers that range from 1 to 4094. *vlan-id2* must be larger than *vlan-id1*.
all	Deletes all group memberships from the interface. • In **group-address all**, **all** indicates that the interface is removed from all multicast groups. • In **vlan** { **all** | {*vlan-id1* [**to** *vlan-id2*] } &<1-10> }, **all** indicates that the interface is removed from multicast groups in all VLANs.	-
group-ip-address1 **to** *group-ip-address2*	Configures multiple static group memberships on the interface. *group-ip-address1* and *group-ip-address2* identify a range of multicast group addresses.	The value ranges from 224.0.1.0 to 239.255.255.255, in dotted decimal notation. The values of *group-ip-address1* and *group-ip-address2* must be in the same network segment (with a 24-bit mask).

Views

MultiGE interface view, Ethernet interface view, GE interface view, XGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, port group view, Eth-Trunk interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In addition to dynamic multicast forwarding entries generated by Layer 2 multicast protocols, you can configure static Layer 2 multicast forwarding entries by binding interfaces to multicast groups. After an interface is statically bound to a multicast group, users connected to this interface can receive multicast data of the multicast group over a long time. The interface then becomes a static member interface.

Configuring static member interfaces has the following advantages:

- Protects the system against attacks from protocol packets.
- Reduces the network delay by directly forwarding multicast packets based on static forwarding entries.
- Prevents unregistered users from receiving multicast flows, improving information security and protecting service providers' interests.

Prerequisites

IGMP snooping has been enabled globally using the **igmp-snooping enable (system view)** command.

Precautions

- The configuration takes effect only when both the following conditions are met:
  - IGMP snooping is enabled in the specified VLANs using the **igmp-snooping enable (VLAN view)**.
  - The specified VLANs have been created and the interface has been added to these VLANs.
  - The specified group address is not a reserved group address.
- If a device is configured to forward Layer 2 multicast traffic on a network configured with MUX VLAN using the **multicast-snooping mux-vlan enable** command, the VLAN specified in the **l2-multicast static-group** command must not be a MUX VLAN (include principal VLAN and subordinate VLAN).
- After the **igmp-snooping version 3 mode asm-ssm** command is configured in a VLAN, no (S, G) entry can be generated if the **l2-multicast static-group** command is run to add an interface to a specified multicast group with a non-SSM multicast address to receive multicast packets from a multicast source. For example, when the **igmp-snooping version 3 mode asm-ssm** command is configured in VLAN 10 and the **l2-multicast static-group**

source-address 2.1.1.1 group-address 225.0.0.1 vlan 10 command is configured on an interface, the (2.1.1.1, 225.0.0.1) entry cannot be generated.

Example

Configure a static multicast group 224.1.1.1 on GE0/0/1 in VLAN 2.

```
<HUAWEI> system-view
[HUAWEI] igmp-snooping enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] port link-type trunk
[HUAWEI-GigabitEthernet0/0/1] port trunk allow-pass vlan 2
[HUAWEI-GigabitEthernet0/0/1] l2-multicast static-group group-address 224.1.1.1 vlan 2
```

Configure static multicast groups 224.1.1.1 to 224.1.1.3 on GE0/0/1 in VLAN 2.

```
<HUAWEI> system-view
[HUAWEI] igmp-snooping enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] port link-type trunk
[HUAWEI-GigabitEthernet0/0/1] port trunk allow-pass vlan 2
[HUAWEI-GigabitEthernet0/0/1] l2-multicast static-group group-address 224.1.1.1 to 224.1.1.3 vlan 2
```

Delete static multicast group 224.1.1.1 from GE0/0/1 in all VLANs.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo l2-multicast static-group group-address 224.1.1.1 vlan all
```

8.9.51 multicast drop-unknown

Function

The **multicast drop-unknown** command configures the switch to drop unknown multicast flows in a VLAN.

The **undo multicast drop-unknown** command restores the default measure taken for unknown multicast flows.

The default method that a switch uses to process unknown multicast flows depends on whether Layer 2 multicast is enabled and which Layer 2 multicast forwarding mode is used.

Format

multicast drop-unknown

undo multicast drop-unknown

Parameters

None

Views

VLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Unknown multicast flows are those that do not match any entry in the multicast forwarding table or match multicast forwarding entries with an empty outbound interface list. These flows are not requested by users. The default method that a switch uses to process unknown IPv4 multicast flows depends on whether Layer 2 multicast is enabled and which Layer 2 multicast forwarding mode is used:

- If Layer 2 multicast is not enabled on the switch, the switch broadcasts unknown multicast flows in the corresponding VLAN.
- If Layer 2 multicast is enabled on the S1720GW-E and S1720GWR-E, they broadcast unknown multicast flows in the corresponding VLAN.
- If Layer 2 multicast is enabled on other switch models, they broadcast unknown multicast flows in the corresponding VLAN in MAC address-based forwarding mode and drop unknown multicast flows in IP address-based forwarding mode.

If a switch broadcasts unknown multicast flows in a VLAN, you can configure the switch to drop unknown multicast flows, reducing instant bandwidth usage.

Configuration Impact

After the **multicast drop-unknown** command is executed, all unknown IPv4 and IPv6 multicast packets are dropped, including the protocol packets that are transparently transmitted within the VLAN and use the reserved multicast address.

After the **multicast drop-unknown** command is run on the following models, protocol packets that are transparently transmitted within the VLAN and use the reserved multicast address will not be discarded: S5731-H, S5731S-H, S5732-H, S5731-S, S5731S-S, S6730-H S6730S-H, S6730-S, and S6730S-S

After the **multicast drop-unknown** command is run on the following models, protocol packets that are transparently transmitted within the VLAN and use the reserved multicast address 224.0.0.9 will not be discarded: S1720GW-E, S1720GWR-E, S5720S-LI, S5720I-SI, S5735S-H, S5736-S, and S6720S-S.

For the S2730S-S, S5735-L-I, S5735-L1, S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735-S-I, and S5735S-S, if MAC address-based forwarding is configured as the Layer 2 multicast forwarding mode and the **multicast drop-unknown** command is executed, unknown multicast packets destined for the following reserved network segments and IP address cannot be dropped: 239.0.0.0/8, 224.0.0.0/24, 224.0.1.0/24, FF0X:0:0:0:0:0:0:0/96, FF0X::DB8:0:0/96, and the IPv6 address with the last 32 bits being 0000:00XX. To drop such unknown multicast packets, configure a traffic policy.

Example

Drop unknown multicast packets in VLAN 10.

```
<HUAWEI> system-view
[HUAWEI] vlan 10
[HUAWEI-vlan10] multicast drop-unknown
```


8.9.52 multicast-snooping mux-vlan enable

Function

The **multicast-snooping mux-vlan enable** command enables a device to transmit Layer 2 multicast traffic on a network configured with MUX VLAN.

The **undo multicast-snooping mux-vlan enable** command disables a device from transmitting Layer 2 multicast traffic on a network configured with MUX VLAN.

By default, a device is disabled from transmitting Layer 2 multicast traffic on a network configured with MUX VLAN.

Format

multicast-snooping mux-vlan enable

undo multicast-snooping mux-vlan enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

By default, on a network configured with MUX VLAN, Layer 2 multicast traffic cannot be transmitted between the principal VLAN and subordinate VLANs. You can run the **multicast-snooping mux-vlan enable** command to enable Layer 2 multicast traffic to be transmitted on the network configured with MUX VLAN.

Precautions

If a MUX VLAN is bound to a static multicast group using the **l2-multicast static-group** or **mld-snooping static-group** command, the **multicast-snooping mux-vlan enable** command cannot be executed. You must delete the association between the MUX VLAN and static multicast group before running the **multicast-snooping mux-vlan enable** command.

After the **multicast-snooping mux-vlan enable** command is configured, you cannot run the **l2-multicast static-group** or **mld-snooping static-group** command to bind a MUX VLAN to a static multicast group.

Example

Enable a device to forward Layer 2 multicast traffic on a network configured with MUX VLAN.

```
<HUAWEI> system-view
[HUAWEI] multicast-snooping mux-vlan enable
```

8.9.53 multicast-source-deny

Function

The **multicast-source-deny** command discards multicast data packets sent from specified VLANs on an interface.

The **undo multicast-source-deny** command restores multicast forwarding in specified VLANs on an interface.

By default, multicast data packets from all VLANs are forwarded on an interface.

Format

multicast-source-deny [**vlan** { *vlan-id1* [**to** *vlan-id2*] } &<1-10>]

undo multicast-source-deny [**vlan** { *vlan-id1* [**to** *vlan-id2*] } &<1-10>]

Parameters

Parameter	Description	Value
vlan *vlan-id1* [**to** *vlan-id2*]	Specifies a VLAN ID. • *vlan-id1* specifies the first VLAN ID. • **to** *vlan-id2* specifies the last VLAN ID. *vlan-id2* must be larger than *vlan-id1*. *vlan-id1* and *vlan-id2* specify a range of VLANs. If you do not specify **to** *vlan-id2*, only one VLAN is specified.	The value is an integer that ranges from 1 to 4094.

Views

MultiGE interface view, Ethernet interface view, GE interface view, XGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, port group view, Eth-Trunk interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After you run the **multicast-source-deny** command on an interface, multicast packets received from specified VLANs are discarded on the interface. You may need to use this command in the following scenarios:

- A user-side interface receives multicast packets, but the switch does not need to receive multicast data packets from user-side interfaces. Discarding multicast data packets received on a user-side interface protects the system against forged multicast flows sent from malicious users.
- Multiple multicast sources in different VLANs are connected to the switch through a Layer 2 network, but the switch only needs to receive multicast data from some of the multicast sources.
- In some situations, for example, multicast services for users connected to an interface have expired and need to be stopped, the network administrator can use this command on this interface. Then multicast data packets from specified VLANs cannot be sent to the users.

Precautions

If you run the **multicast-source-deny** command multiple times, all the configurations take effect.

When using the **multicast-source-deny** command on an interface, ensure that the interface has been added to the specified VLANs. Otherwise, the configuration does not take effect.

This command can discard only multicast data packets that meet both of the following conditions:

- The destination MAC address is an IP multicast MAC address (IPv4 MAC address starting with 0x01-00-5e or IPv6 multicast MAC address starting with 0x3333).
- The packet encapsulation protocol is UDP.

Example

Discard multicast data packets sent from VLANs 100 to 105 on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet0/0/1
[HUAWEI-GigabitEthernet0/0/1] multicast-source-deny vlan 100 to 105
```

8.9.54 reset igmp-snooping group

Function

The **reset igmp-snooping group** command deletes dynamic group memberships learned by IGMP snooping.

Format

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

Parameters

Parameter	Description	Value
all	Deletes all dynamic group memberships learned by IGMP snooping.	-
vlan { **all** | *vlan-id* }	Deletes the dynamic group memberships of a specified VLAN. If **all** is specified, the system deletes IGMP dynamic group memberships of all VLANs.	The value of *vlan-id* is an integer that ranges from 1 to 4094.
source-address *source-address*	Deletes the dynamic group memberships of a specified source address.	The multicast source address is a Class A, Class B, or Class C IP address on a nature network segment. The value is in dotted decimal notation.
group-address *group-address*	Deletes the dynamic group memberships of a specified group address.	The value of *group-address* ranges from 224.0.1.0 to 239.255.255.255 in dotted decimal notation.

Views

User view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When multicast groups on a network change, the switch generates new Layer 2 multicast forwarding entries until the aging time of member ports expire. To enable the switch to generate new multicast forwarding entries immediately, use the **reset igmp-snooping group** command to delete existing group memberships.

Precautions

NOTICE

Deleting group memberships in a VLAN temporarily interrupts multicast forwarding in the VLAN. The switch generates new forwarding entries only when receiving IGMP Report messages from hosts in the VLAN. The hosts can then receive multicast data.

This command cannot delete static group memberships.

This command is valid only for VLANs with IGMP snooping enabled and is invalid for a VLAN if IGMP is enabled on the corresponding VLANIF interface.

Example

Delete all dynamic group memberships learned by IGMP snooping.

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

Delete dynamic group memberships in VLAN 3.

```
<HUAWEI> reset igmp-snooping group vlan 3
```

8.9.55 reset igmp-snooping qinq-port-info

Function

The **reset igmp-snooping qinq-port-info** command clears multicast group membership on a QinQ or Dot1q termination sub-interface.

Format

reset igmp-snooping qinq-port-info interface *interface-type interface-number*

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Clears multicast group membership on a specified interface.	-

Views

User view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When multicast users access a multicast group through a sub-interface, multicast group members change, and the switch generates new Layer 3 multicast forwarding entries until the aging time of multicast member interfaces expires. To enable the switch to generate new multicast forwarding entries immediately, use the **reset igmp-snooping qinq-port-info** command to clear old Layer 3 multicast forwarding entries.

Configuration Impact

During the execution of the **reset igmp-snooping qinq-port-info** command on a sub-interface, multicast traffic to hosts connected to this sub-interface will be interrupted.

Precautions

This command cannot delete static group membership.

Example

Clear group membership of all multicast groups on QinQ termination sub-interface GE0/0/18.1.

```
<HUAWEI> reset igmp-snooping qinq-port-info interface GigabitEthernet 0/0/18.1
```

8.9.56 reset igmp-snooping statistics

Function

The **reset igmp-snooping statistics** command clears IGMP snooping statistics.

Format

reset igmp-snooping statistics { **all** | **vlan** { **all** | *vlan-id* } }

Parameters

Parameter	Description	Value
all	Clears all the IGMP snooping statistics.	-
vlan { **all** | *vlan-id* }	Clears IGMP snooping statistics of a specified VLAN. If **all** is specified, the system clears IGMP snooping statistics of all VLANs.	The value of *vlan-id* is an integer that ranges from 1 to 4094.

Views

User view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To analyze the IGMP snooping statistics collected in a certain period, run this command to clear the previous statistics. After a while, run the **display igmp-snooping statistics** command to view the IGMP snooping statistics.

Precautions

NOTICE

The cleared IGMP snooping statistics cannot be restored.

Example

Clear IGMP snooping statistics of VLAN 2.

```
<HUAWEI> reset igmp-snooping statistics vlan 2
```

8.10 VSI-based IGMP Snooping Configuration Commands

8.10.1 Command Support

Only the S5731-H, S5731S-H, S5731-S, S6730-S, S5732-H, S6720-EI, S6720S-EI, S6730S-H, and S6730-H support VSI-based IGMP Snooping.

VSI-based IGMP snooping depends on the MPLS feature.

8.10.2 display igmp-snooping

Function

The **display igmp-snooping** command displays the IGMP snooping running parameters in a VSI.

Format

display igmp-snooping [**vsi** [*vsi-name*]]

Parameters

Parameter	Description	Value
vsi [*vsi-name*]	Displays the IGMP snooping running parameters in a specified VSI.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

After completing IGMP snooping configuration in a VSI, you can use this command to check IGMP snooping parameter settings. When a fault occurs in the multicast service, use this command to identify the cause of the fault.

Precautions

The IGMP snooping configuration of a VSI is displayed only when the VSI is in Up state.

Example

Display IGMP snooping running parameters in VSI company1.

```
<HUAWEI> display igmp-snooping vsi company1
 IGMP Snooping Information for VSI company1
    IGMP Snooping is Enabled
    IGMP Version is Set to default 2
    IGMP Query Interval is Set to default 125s
    IGMP Max Response Interval is Set to default 10s
    IGMP Robustness is Set to default 2
    IGMP Last Member Query Interval is Set to default 1s
    IGMP Router Port Aging Interval is Set to 180s or holdtime in hello
    IGMP Filter Group-Policy is not set
    IGMP Prompt Leave Disable
    IGMP Router Alert is Not Required
    IGMP Send Router Alert Enable
    IGMP Router Port Learning Enable
    IGMP SSM-Mapping Disable
```


Table 8-125 Description of the **display igmp-snooping** command output

Item	Description
IGMP Snooping Information for VSI company1	IGMP snooping running parameters are displayed in VSI company1.
IGMP Snooping is Enabled	IGMP snooping is enabled in the VSI. By default, IGMP snooping is disabled in a VSI. IGMP snooping can be enabled in a VSI using the **igmp-snooping enable (VSI view)** command.
IGMP Version is Set to default 2	Both IGMPv1 and IGMPv2 messages can be processed in the VSI (default configuration). This parameter is configured using the **igmp-snooping version** command.
IGMP Query Interval is Set to default 125s	The interval at which IGMP General Query messages are sent in the VSI is 125 seconds (default configuration). This parameter is configured using the **igmp-snooping query-interval** command.
IGMP Max Response Interval is Set to default 10s	The maximum response time for IGMP General Query messages in the VSI is 10 seconds (default configuration). This parameter is configured using the **igmp-snooping max-response-time** command.
IGMP Robustness is Set to default 2	The IGMP robustness variable is 2 (default configuration). This parameter is configured using the **igmp-snooping robust-count** command.
IGMP Last Member Query Interval is Set to default 1s	The interval at which IGMP Group-Specific Query messages are sent in the VSI 1 second (default configuration). This parameter is configured using the **igmp-snooping lastmember-queryinterval** command.
IGMP Router Port Aging Interval is Set to 180s or holdtime in hello	The aging time of router ports in the VSI is 180 seconds or the holdtime in PIM Hello messages (default configuration). This parameter is configured using the **igmp-snooping router-aging-time** command.
IGMP Filter Group-Policy is not set	The default multicast group policy is used in the VSI. A multicast group policy is configured using the **igmp-snooping group-policy** command.

Item	Description
IGMP Prompt Leave Disable	Prompt leave is disabled in the VSI (default configuration). The prompt leave function can be enabled using the **igmp-snooping prompt-leave** command.
IGMP Router Alert is Not Required	The device does not require that the IGMP messages received in the VSI contain the Router-Alert option in the IP header (default configuration). The switch can be configured to discard IGMP messages without the Router-Alert option using the **igmp-snooping require-router-alert** command.
IGMP Send Router Alert Enable	The device sends the IGMP messages that contain the Router-Alert option in the IP headers to the hosts in the VSI (default configuration). The switch can be configured to send IGMP messages with the Router-Alert option using the **igmp-snooping send-router-alert** command.
IGMP Router Port Learning Enable	Learning of IGMP router ports is enabled in the VSI. Router port learning can be enabled using the **igmp-snooping router-learning** command.
IGMP SSM-Mapping Disable	IGMP SSM mapping is disabled in the VSI. IGMP snooping SSM mapping can be enabled using the **igmp-snooping ssm-mapping enable** command.

8.10.3 display igmp-snooping configuration

Function

The **display igmp-snooping configuration** command displays the IGMP snooping configuration in a VSI.

Format

display igmp-snooping [**vsi** [*vsi-name*]] **configuration**

Parameters

Parameter	Description	Value
vsi [*vsi-name*]	Displays the non-default IGMP snooping configuration in a specified VSI.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

After completing IGMP snooping configuration in a VSI, use this command to verify the configuration. This command displays only the IGMP snooping configuration.

Prerequisites

This command does not display information about static multicast groups and static router ports. To view information about static multicast groups and static router ports, run the **display igmp-snooping port-info** and **display igmp-snooping router-port** command.

Example

Display the IGMP snooping configuration in VSI company1.

```
<HUAWEI> display igmp-snooping vsi company1 configuration
 IGMP Snooping Configuration for VSI company1
    igmp-snooping enable
    igmp-snooping version 3
```

8.10.4 display igmp-snooping port-info

Function

The **display igmp-snooping port-info** command displays information about group member ports.

Format

display igmp-snooping port-info [**vsi** *vsi-name* [**group-address** *group-address*]] [**verbose**]

Parameters

Parameter	Description	Value
vsi *vsi-name*	Displays group memberships in a specified VSI.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
group-address *group-address*	Displays member ports of a specified multicast group in a VSI. *group-address* specifies the IP address of a multicast group.	The value ranges from 224.0.1.0 to 239.255.255.255, in dotted decimal notation.
verbose	Displays detailed information about member ports.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

After IGMP snooping is configured in a VSI on a switch, the IGMP snooping module maintains a Layer 2 multicast forwarding table by snooping the IGMP messages exchanged between the upstream router and downstream hosts. The **display igmp-snooping port-info** command shows member interfaces in the Layer 2 multicast forwarding table. According to the command output, you can know which downlink interfaces have multicast users connected, and control multicast services conveniently.

Precautions

Only multicast member ports in Up state are displayed in the command output.

Example

Display information about group member ports in the VSI **company1**.

```
<HUAWEI> display igmp-snooping port-info vsi company1
------------------------------------------------------------------------------
                  (Source, Group)  Port                      Flag
 Flag: S:Static     D:Dynamic     M: Ssm-mapping
 -----------------------------------------------------------------------------
VSI company1, 3 Entry(s)
                  (*, 225.0.0.1)  GE0/0/11(VID:1001)          -D-
                                  1 port(s) include
                  (*, 225.0.0.2)  PW(10.1.1.1/100)            -D-
                                  1 port(s) include
                  (*, 225.0.0.3)  GE0/0/13                    -D-
                                  1 port(s) include
 -----------------------------------------------------------------------------
```

Table 8-126 Description of the **display igmp-snooping port-info** command output

Item	Description
(Source, Group)	(S, G) entry, specifying a multicast source and multicast group.
Port	Outbound port name. **include** and **exclude** indicate the multicast source filtering mode. Different ports in the command output are described as follows: • GE0/0/11 (VID:1001) indicates that the AC-side interface is VLANIF 1001, and the group member port is GE0/0/11 in VLAN 1001. • PW (10.1.1.1/100) indicates that the member port is a PW-side interface. 10.1.1.1 is the IP address of the remote peer, and 100 is the VC ID of the remote peer. • GE0/0/13 indicates that the AC-side interface is GE0/0/13 working in Layer 3 mode, and the group member port is GE0/0/13.
Flag	Type of an outbound port. • S: static member port • D: dynamic member port • M: member port established through SSM mapping
VSI company1, 3 Entry(s)	Number of multicast entries in VSI company 1.

8.10.5 display igmp-snooping router-port

Function

The **display igmp-snooping router-port** command displays information about the router ports in a specified VSI, including static and dynamic router ports.

Format

display igmp-snooping router-port vsi [*vsi-name*]

Parameters

Parameter	Description	Value
vsi [*vsi-name*]	Displays information about router ports in a specified VSI. If *vsi-name* is not specified, the command displays router ports in all VSIs.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

A router port connects to an upstream multicast router. The router port can be statically configured or dynamically generated after the interface receives an IGMP Query message.

After completing basic IGMP snooping configuration in a VSI, you can run the **display igmp-snooping router-port** command to view the type, name, lifetime, and remaining aging time of a router port in the VSI.

Precautions

Information about a router port is displayed only when the interface is in Up state.

Example

Display information about router ports in VSI company1.

```
<HUAWEI> display igmp-snooping router-port vsi company1
 Port Name                 UpTime       Expires      Flags
 ----------------------------------------------------------------------
 VSI company1, 3 router-port(s)
 GE0/0/21(VID:100)           18:02:13     00:02:35     DYNAMIC
 PW(1.1.1.1/2)               03:28:16     00:01:20     DYNAMIC
 GE0/0/15                    18:02:13     00:02:35     DYNAMIC
```


Table 8-127 Description of the display igmp-snooping router-port command output

Item	Description
Port Name	Router port name. Different ports in the command output are described as follows: • GE0/0/21(VID:100) indicates that the AC-side interface is VLANIF 100, and the router port is GE0/0/21 in VLAN 100. • PW(1.1.1.1/2) indicates that the member port is a PW-side interface. 1.1.1.1 is the IP address of the remote peer, and 2 is the VC ID of the remote peer. • GE0/0/15 indicates that the AC-side interface is GE0/0/15 working in Layer 3 mode, and the router port is GE0/0/15.
UpTime	Time elapsed since the interface became a router port.
Expires	Remaining aging time of the router port. • The remaining aging time is displayed for a dynamic router port. • For a static router port, "--" is displayed, indicating that the interface does not age.
Flags	Type of the router port. • STATIC: static router port • DYNAMIC: dynamic router port
VSI company1, 3 router-port(s)	Number of router ports in VSI company 1.

8.10.6 display igmp-snooping statistics

Function

The **display igmp-snooping statistics** command displays IGMP snooping statistics.

Format

display igmp-snooping statistics vsi [*vsi-name*]

Parameters

Parameter	Description	Value
vsi-name	Displays IGMP snooping statistics on a specified VSI.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

After completing basic IGMP snooping configuration in a VSI, you can use the **display igmp-snooping statistics** command to view IGMP snooping statistics, including the number of IGMP messages sent and received, and the number of PIM hello messages received in each VSI. When a multicast fault occurs, the IGMP snooping statistics help you identify the cause of the fault.

Configuration Impact

When *vsi-name* is specified, this command displays IGMP snooping statistics in the specified VSI, but does not display IGMP snooping events that occur in the VSI.

Example

Display IGMP snooping statistics in VSI company1.

```
<HUAWEI> display igmp-snooping statistics vsi company1
 IGMP Snooping Packets Counter
   Statistics for VSI company1
     Recv V1 Report          0
     Recv V2 Report          304
     Recv V3 Report          0
     Recv V1 Query           0
     Recv V2 Query           523
     Recv V3 Query           0
     Recv Leave              0
     Recv Pim Hello          0
     Send Query(S=0)         0
     Send Query(S!=0)        0
```


Table 8-128 Description of the **display igmp-snooping statistics** command output

Item	Description
IGMP Snooping Packets Counter	Statistics on IGMP and PIM packets.
Statistics for VSI company1	Packet statistics in VSI company1.
Recv V1 Report	Number of received IGMPv1 Membership Report messages.
Recv V2 Report	Number of received IGMPv2 Membership Report messages.
Recv V3 Report	Number of received IGMPv3 Membership Report messages.
Recv V1 Query	Number of received IGMPv1 Query messages.
Recv V2 Query	Number of received IGMPv2 Query messages.
Recv V3 Query	Number of received IGMPv3 Query messages.
Recv Leave	Number of received IGMP Leave messages.
Recv Pim Hello	Number of received PIM Hello messages.
Send Query(S=0)	Number of sent IGMP Query messages with the source address 0.0.0.0.
Send Query(S!=0)	Number of sent IGMP Query messages with source addresses other than 0.0.0.0.

8.10.7 display l2-multicast forwarding-table vsi

Function

The **display l2-multicast forwarding-table vsi** command displays the VSI-based Layer 2 multicast forwarding table.

Format

display l2-multicast forwarding-table vsi [*vsi-name* [**group-address** { *group-address* | **router-group** }]]

Parameters

Parameter	Description	Value
vsi-name	Displays Layer 2 multicast forwarding entries in a specified VSI. If *vsi-name* is not specified, the command displays Layer 2 multicast forwarding entries in all VSIs.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
group-address { *group-address* | **router-group** }	Displays Layer 2 multicast forwarding entries of a specified multicast group or all router ports. • If you specify *group-address*, the command displays forwarding entries of the specified multicast group. • If you specify **router-group**, the command displays forwarding entries of all router ports.	The value of *group-address* is in dotted decimal notation and ranges from 224.0.1.0 to 239.255.255.255.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

After completing configuration of IGMP snooping over VPLS, you can use the **display l2-multicast forwarding-table** command to view the Layer 2 multicast forwarding table.

Precautions

This command displays multicast forwarding entries in a VSI only when the VSI is in Up state.

Example

Display the multicast forwarding entries of the VSI **company1**.


```
<HUAWEI> display l2-multicast forwarding-table vsi company1
VSI Name : company1, Forwarding Mode : MAC
Total Group(s) : 2
--------------------------------------------------------------------------
Group(Mac)                          Interface     Out-Vlan/InLabel
--------------------------------------------------------------------------
                    Router-port    5.5.5.9/28              1036
0100-5e00-0001                       5.5.5.9/28              1036
                                GigabitEthernet0/0/21    1000
0100-5e00-0002                       5.5.5.9/28              1036
                                GigabitEthernet0/0/21    1000
                                GigabitEthernet0/0/22    0
--------------------------------------------------------------------------
```

Table 8-129 Description of the **display l2-multicast forwarding-table** command output

Item	Description
VSI Name	Name of the VSI of which the multicast forwarding entries are displayed.
Forwarding Mode	Multicast forwarding mode used in the VSI. Only the MAC address-based forwarding mode is supported.
Group(Mac)	Group MAC address.
Interface	Group member ports and router ports. In this example, 5.5.5.9/28 indicates a PW-side interface, of which the remote peer IP address is 5.5.5.9 and remote peer VSI ID is 28. GigabitEthernet0/0/21 indicates an AC-side interface.
Out-Vlan/InLabel	VLAN ID or inner MPLS label of packets. The value 0 indicates that the router port or member port is an AC-side interface, which is a physical interface working in Layer 3 mode.
Router-port	Router port in the VSI.

8.10.8 igmp-snooping enable (system view)

Function

The **igmp-snooping enable** command enables IGMP snooping globally.

The **undo igmp-snooping enable** command disables IGMP snooping globally.

By default, IGMP snooping is disabled globally.

Format

igmp-snooping enable

undo igmp-snooping enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After IGMP snooping is enabled in a VSI, IGMP snooping runs on PE devices in the VSI and maintains a multicast forwarding table by snooping IGMP messages forwarded between the PE devices. The PE devices can manage and control Layer 2 multicast forwarding based on the multicast forwarding table.

Before configuring IGMP snooping in a VSI, enable IGMP snooping globally. Other IGMP snooping configuration commands can be used only after you run the **igmp-snooping enable** command in the system view.

Precautions

NOTICE

When you run the **undo igmp-snooping enable** command in the system view, the system displays a message, asking you whether to disable IGMP snooping globally. When you disable IGMP snooping globally, all the IGMP snooping configurations are deleted. When you run the **igmp-snooping enable** command to enable IGMP snooping globally again, the device uses the default IGMP snooping configuration.

Example

Enable IGMP snooping globally.

```
<HUAWEI> system-view
[HUAWEI] igmp-snooping enable
```

8.10.9 igmp-snooping enable (VSI view)

Function

The **igmp-snooping enable** command enables IGMP snooping in a VSI.

The **undo igmp-snooping enable** command disables IGMP snooping in a VSI.

By default, IGMP snooping is disabled in a VSI.

Format

igmp-snooping enable

undo igmp-snooping enable

Parameters

None

Views

VSI view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

By default, IGMP snooping not enabled in a VSI after being enabled in the system view. To enable IGMP snooping in a VSI, run the **igmp-snooping enable** command in the VSI view.

Prerequisites

IGMP snooping has been enabled for VPLS using the **igmp-snooping over-vpls enable** command in the system view.

Example

Enable IGMP snooping in VSI company1.

```
<HUAWEI> system-view
[HUAWEI] igmp-snooping enable
[HUAWEI] igmp-snooping over-vpls enable
[HUAWEI] vsi company1
[HUAWEI-vsi-company1] igmp-snooping enable
```

8.10.10 igmp-snooping group-limit

Function

The **igmp-snooping group-limit** command sets the maximum number of Layer 2 multicast entries that an AC-side interface can learn.

The **undo igmp-snooping group-limit** command cancels the limit on the number of Layer 2 multicast entries that an AC-side interface can learn.

By default, the number of Layer 2 multicast entries that an AC-side interface can learn is not limited.

Format

igmp-snooping group-limit *group-limit* **vsi** *vsi-name*

undo igmp-snooping group-limit [*group-limit*] **vsi** *vsi-name*

Parameters

Parameter	Description	Value
group-limit	Specifies the maximum number of Layer 2 multicast entries that an AC-side interface can learn.	The value is an integer ranging from 1 to 4096.
vsi *vsi-name*	Limits the number of Layer 2 multicast entries that can be learned in a VSI.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Views

GE interface view, 100GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, Eth-Trunk interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

By limiting the number of Layer 2 multicast entries learned on an interface, you can control the number of programs users connected to the interface can order. This configuration limits the multicast data traffic volume on the interface.

On a VPLS network, the maximum number of Layer 2 multicast entries can only be configured on an AC-side interface. The configuration method varies according to the type of the AC-side interface:

- If the AC-side interface bound to a VSI is a VLANIF interface, configure the maximum number of Layer 2 multicast entries on the Layer 2 interface in the corresponding VLAN. For details, see the **igmp-snooping group-limit** command in "VLAN-based IGMP Snooping Configuration Commands."
- If the AC-side interface bound to a VSI is a physical interface that has been switched to Layer 3 mode using the **undo portswitch** command, run the **igmp-snooping group-limit** *group-limit* **vsi** *vsi-name* command on this interface.

Prerequisites

IGMP snooping has been enabled globally using the **igmp-snooping enable (system view)** command.

Configuration Impact

If the number of Layer 2 multicast entries on the interface already exceeds the configured limit, the number of Layer 2 multicast entries on the interface does not change and the interface cannot learn new Layer 2 multicast entries.

Precautions

The configuration takes effect only after you run the **igmp-snooping enable (VSI view)** command to enable IGMP snooping in the VSI.

Example

Set the maximum number of Layer 2 multicast entries on the AC-side interface GE0/0/1 bound to the VSI **company1** to 10. (IGMP snooping has been enabled globally and in the VSI.)

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] igmp-snooping group-limit 10 vsi company1
```

8.10.11 igmp-snooping group-policy (interface view)

Function

The **igmp-snooping group-policy** command applies a multicast group policy on an AC-side interface.

The **undo igmp-snooping group-policy** command deletes a multicast group policy from an AC-side interface.

By default, no multicast group policy is available on an AC-side interface bound to a VSI, and hosts in sites connected to the interface can join any multicast group.

Format

igmp-snooping group-policy *acl-number* [**version** *version-number*] **vsi** *vsi-name*

undo igmp-snooping group-policy [*acl-number* [**version** *version-number*]] **vsi** *vsi-name*

Parameters

Parameter	Description	Value
acl-number	Specifies the number of the ACL that limits the multicast groups that hosts in a VSI can join.	The number of a basic ACL is an integer that ranges from 2000 to 2999. The number of an advanced ACL ranges from 3000 to 3999.

Parameter	Description	Value
version *version-number*	Applies the multicast group policy only to the IGMP messages of the specified version.	The value is an integer that ranges from 1 to 3. ● 1: IGMPv1 ● 2: IGMPv2 ● 3: IGMPv3
vsi *vsi-name*	Specifies the VSI to which the multicast group policy is applied.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Views

GE interface view, 100GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, Eth-Trunk interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A multicast group policy controls the multicast programs that users can order on a device with IGMP snooping enabled. In multicast applications, user hosts send IGMP Report messages to join a group when they order programs of this group. When the upstream Layer 2 device receives the Report messages, the switch matches the Report messages with the ACL referenced in the group policy configured on the interface. If the messages match the ACL, the switch allows user hosts in the VSI to join the group and accepts the Report messages. If the messages do not match the ACL, the switch prevents the user hosts in the VSI from joining the group.

Prerequisites

IGMP snooping has been enabled globally using the **igmp-snooping enable (system view)** command.

Precautions

- The configuration takes effect only when IGMP snooping is enabled in the VSI using the **igmp-snooping enable (VSI view)** command.
- Before running the **igmp-snooping group-policy (interface view)** command, run the **acl** command to configure the ACL that you want to apply to the

group policy to limit the range of multicast groups that hosts connected to the VLAN can join.

- In the basic ACL view, set **source** in the **rule** command to the range of multicast groups that the VLAN can join.
- In the advanced ACL view, set **source** in the **rule** command to the source address that is allowed to send multicast data to the specified multicast groups, and set **destination** to the range of multicast groups that the VLAN can join.

After the **igmp-snooping group-policy (interface view)** command is executed on an interface:

- The VLAN filters the received Report messages based on the ACL and maintains memberships only for the multicast groups permitted by the ACL.
- The VLAN discards the Report messages that are denied by the ACL. If the entries of the multicast groups denied by the ACL exist on the switch, the switch deletes these entries when the aging time of the entries expires.
- If the IGMP version is not specified, the specified ACL applies to IGMPv1, IGMPv2, and IGMPv3 hosts.

- The **igmp-snooping group-policy (interface view)** applies a multicast group policy to the sites connected to an AC-side interface. You can also apply a multicast group policy to a VSI using the **igmp-snooping group-policy (VSI view)** command. If multicast group policies are configured for the same VSI in the VSI view and interface view, the system first uses the policy configured in the interface to filter the groups that hosts in the VSI can join, and then use the group configured in the VSI view.
- On a VPLS network, ACs can be set up on different types of interfaces. The method to apply a multicast group policy to an AC-side interface various according to the type of the AC-side interface:
  - If the AC-side interface bound to a VSI is a physical interface that has been switched to Layer 3 mode using the **undo portswitch** command, run the **igmp-snooping group-policy** command on this interface.
  - If the AC-side interface bound to a VSI instance is a VLANIF interface, configure a multicast group policy on the Layer 2 interface in the corresponding VLAN. For details, see the **igmp-snooping group-policy (interface view)** commands in "VLAN-based IGMP Snooping Configuration Commands."

Example

Apply a multicast group policy to AC-side interface GE0/0/1 bound to the VSI **company1**, which allows hosts in the sites connected to GE0/0/1 to join group 225.1.1.123.

```
<HUAWEI> system-view
[HUAWEI] acl number 2000
[HUAWEI-acl-basic-2000] rule permit source 225.1.1.123 0
[HUAWEI-acl-basic-2000] quit
[HUAWEI] igmp-snooping enable
[HUAWEI] igmp-snooping over-vpls enable
[HUAWEI] vsi company1
[HUAWEI-vsi-company1] igmp-snooping enable
```



```
[HUAWEI-vsi-company1] quit
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] igmp-snooping group-policy 2000 vsi company1
```

8.10.12 igmp-snooping group-policy (VSI view)

Function

The **igmp-snooping group-policy** command configures a multicast group policy in a VSI.

The **undo igmp-snooping group-policy** command deletes a multicast group policy from a VSI.

By default, no multicast group policy is available in a VSI, and hosts in the VSI can join any multicast group.

Format

igmp-snooping group-policy *acl-number* [**version** *version-number*]

undo igmp-snooping group-policy

Parameters

Parameter	Description	Value
acl-number	Specifies the number of the ACL that limits the multicast groups that hosts in a VSI can join.	The number of a basic ACL is an integer that ranges from 2000 to 2999. The number of an advanced ACL ranges from 3000 to 3999.
version *version-number*	Applies the multicast group policy only to the IGMP messages of the specified version.	The value is an integer that ranges from 1 to 3. • 1: IGMPv1 • 2: IGMPv2 • 3: IGMPv3

Views

VSI view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A multicast group policy controls the multicast programs that users can order on a device with IGMP snooping enabled. In multicast applications, user hosts send IGMP Report messages to join a group when they order programs of this group. When the upstream Layer 2 device receives the Report messages, the switch matches the Report messages with the ACL referenced in the group policy configured in the VSI. If the messages match the ACL, the switch allows user hosts in the VSI to join the group and accepts the Report messages. If the messages do not match the ACL, the switch prevents the user hosts in the VSI from joining the group.

Prerequisites

IGMP snooping has been enabled for VPLS using the **igmp-snooping over-vpls enable** command in the system view.

Precautions

- The configuration takes effect only when IGMP snooping is enabled in the VSI using the **igmp-snooping enable (VSI view)** command.
- Before running the **igmp-snooping group-policy (VSI view)** command, run the **acl** command to configure the ACL that you want to apply to the group policy to limit the range of multicast groups that hosts connected to the VSI can join.
  - In the basic ACL view, set **source** in the **rule** command to the range of multicast groups that a VSI can join.
  - In the advanced ACL view, set **source** in the **rule** command to the source address that is allowed to send multicast data to the specified multicast groups, and set **destination** to the range of multicast groups that a VSI can join.

  After the **igmp-snooping group-policy (VSI view)** command is executed on a VSI:
  - The VSI filters the received Report messages based on the ACL and maintains memberships only for the multicast groups permitted by the ACL.
  - The VSI discards the Report messages that are denied by the ACL. If the entries of the multicast groups denied by the ACL exist on the switch, the switch deletes these entries when the aging time of the entries expires.
  - If the IGMP version is not specified, the specified ACL applies to IGMPv1, IGMPv2, and IGMPv3 hosts.
- The **igmp-snooping group-policy (VSI view)** command applies a multicast group policy to a VSI. You can also apply a multicast group to the sites connected to an AC-side interface by using either of the following methods:
  - If the AC-side interface bound to a VSI instance is a VLANIF interface, configure a multicast group policy on the Layer 2 interface in the corresponding VLAN. For details, see the **igmp-snooping group-policy (interface view)** commands in "VLAN-based IGMP Snooping Configuration Commands."
  - If the AC-side interface bound to a VSI is a physical interface that has been switched to Layer 3 mode using the **undo portswitch** command, run the **igmp-snooping group-policy** *acl-number* [**version** *version-number*] **vsi** *vsi-name* command on this interface.

If multicast group policies are configured for the same VSI in the VSI view and interface view, the system first uses the policy configured in the interface to filter the groups that hosts in the VSI can join, and then use the group configured in the VSI view.

Example

Allow hosts in the VSI **company1** to join group 225.1.1.123.

```
<HUAWEI> system-view
[HUAWEI] acl number 2000
[HUAWEI-acl-basic-2000] rule permit source 225.1.1.123 0
[HUAWEI-acl-basic-2000] quit
[HUAWEI] igmp-snooping enable
[HUAWEI] igmp-snooping over-vpls enable
[HUAWEI] vsi company1
[HUAWEI-vsi-company1] igmp-snooping enable
[HUAWEI-vsi-company1] igmp-snooping group-policy 2000
```

8.10.13 igmp-snooping lastmember-queryinterval

Function

The **igmp-snooping lastmember-queryinterval** command sets the last member query interval in a VSI, that is, the interval at which Group-Specific Query messages are sent in the VSI.

The **undo igmp-snooping lastmember-queryinterval** command restores the default last member query interval in a VSI.

By default, Group-Specific Query messages are sent in a VSI at intervals of 1 second.

Format

igmp-snooping lastmember-queryinterval *lastmember-queryinterval*

undo igmp-snooping lastmember-queryinterval

Parameters

Parameter	Description	Value
lastmember-queryinterval	Specifies the interval at which IGMP Group-Specific Query messages are sent.	The value is an integer that ranges from 1 to 5, in seconds.

Views

VSI view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When a member interface receives an IGMP Leave message from a downstream host, the switch starts the aging timer for the interface. The aging time is calculated using the following formula: Aging time = Last member query interval x Last member query count. The **igmp-snooping lastmember-queryinterval** command sets the last member query interval. The last member query count is set by the **igmp-snooping robust-count** command.

If the member interface receives Report messages from downstream hosts within the aging time, the switch retains the member interface in the outbound interface list of the corresponding Layer 2 multicast forwarding entry. If the member interface does not receive any Report messages within the aging time, the switch considers that no group member is connected to the interface, and therefore deletes the interface from the Layer 2 multicast forwarding entry.

Prerequisites

IGMP snooping has been enabled for VPLS using the **igmp-snooping over-vpls enable** command in the system view.

Precautions

The configuration takes effect only when IGMP snooping is enabled in the VSI using the **igmp-snooping enable (VSI view)** command.

Hosts running IGMPv1 do not send Leave messages when they leave a multicast group. Therefore, the **igmp-snooping lastmember-queryinterval** command is valid only when the IGMP message version is set to v2 or v3 in the VSI.

Example

Set the last member query interval in VSI company1 to 4 seconds.

```
<HUAWEI> system-view
[HUAWEI] igmp-snooping enable
[HUAWEI] igmp-snooping over-vpls enable
[HUAWEI] vsi company1
[HUAWEI-vsi-company1] igmp-snooping enable
[HUAWEI-vsi-company1] igmp-snooping lastmember-queryinterval 4
```

8.10.14 igmp-snooping max-response-time

Function

The **igmp-snooping max-response-time** command sets the maximum response time for IGMP General Query messages in a VSI.

The **undo igmp-snooping max-response-time** command restores the default maximum response time for IGMP General Query messages in a VSI.

By default, the maximum response time for IGMP General messages in a VSI is 10 seconds.

Format

igmp-snooping max-response-time *max-response-time*

undo igmp-snooping max-response-time

Parameters

Parameter	Description	Value
max-response-time	Specifies the maximum response time for IGMP General Query messages.	The value is an integer that ranges from 1 to 25, in seconds. The default value is 10.

Views

VSI view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The maximum response time for General Query messages is used to calculate the aging time of group member interfaces. When a member port receives a Report message from a downstream host, the switch starts the aging timer for the interface. The aging time is calculated using the following formula: Aging time = Query count x General query interval + Maximum response time for General Query messages. This command sets the maximum response time in the formula. The general query interval is set by the **igmp-snooping robust-count** command, and the general query interval is set by the **igmp-snooping query-interval** command.

If the member port receives Report messages from downstream hosts within the aging time, the switch retains the member port in the outbound interface list of the corresponding Layer 2 multicast forwarding entry. If the member port does not receive any Report messages within the aging time, the switch considers that no group member is connected to the interface, and therefore deletes the interface from the Layer 2 multicast forwarding entry.

Prerequisites

IGMP snooping has been enabled for VPLS using the **igmp-snooping over-vpls enable** command in the system view.

Precautions

The configuration takes effect only when IGMP snooping is enabled in the VSI using the **igmp-snooping enable (VSI view)** command.

Example

Set the maximum response time for IGMP General Query messages in VSI company1 to 20 seconds.


```
<HUAWEI> system-view
[HUAWEI] igmp-snooping enable
[HUAWEI] igmp-snooping over-vpls enable
[HUAWEI] vsi company1
[HUAWEI-vsi-company1] igmp-snooping enable
[HUAWEI-vsi-company1] igmp-snooping max-response-time 20
```

8.10.15 igmp-snooping over-vpls enable

Function

The **igmp-snooping over-vpls enable** command enables IGMP snooping for VPLS.

The **undo igmp-snooping over-vpls enable** command disables IGMP snooping for VPLS.

By default, IGMP snooping for VPLS is disabled.

Format

igmp-snooping over-vpls enable

undo igmp-snooping over-vpls enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Before configuring IGMP snooping in a VSI, enable IGMP snooping globally and for VPLS in the system view.

Prerequisites

IGMP snooping has been enabled globally using the **igmp-snooping enable (system view)** command in the system view.

Precautions

When you run the **undo igmp-snooping over-vpls enable** command in the system view, the system displays a message, asking you whether to disable IGMP snooping for VPLS. If any IGMP snooping for VPLS configuration has been made in the system, the device prompts you to delete all the IGMP snooping for VPLS configuration.

Example

Enable IGMP snooping for VPLS.

```
<HUAWEI> system-view
[HUAWEI] igmp-snooping enable
[HUAWEI] igmp-snooping over-vpls enable
```

8.10.16 igmp-snooping prompt-leave

Function

The **igmp-snooping prompt-leave** command enables the fast leave function in a VSI so that member ports in the VSI can fast leave multicast groups.

The **undo igmp-snooping prompt-leave** command disables the fast leave function in a VSI.

By default, the fast leave function is disabled in a VSI.

Format

igmp-snooping prompt-leave [**group-policy** *acl-number*]

undo igmp-snooping prompt-leave

Parameters

Parameter	Description	Value
group-policy *acl-number*	Allows member ports to fast leave the multicast group specified by an ACL.	The value of *acl-number* is an integer that ranges from 2000 to 3999.

Views

VSI view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The fast leave function allows the switch to delete an interface from a group immediately after the interface receives an IGMP Leave message for the multicast group.

Prerequisites

IGMP snooping has been enabled for VPLS using the **igmp-snooping over-vpls enable** command in the system view.

Precautions

- The configuration takes effect only when IGMP snooping is enabled in the VSI using the **igmp-snooping enable (VSI view)** command.
- The configuration is valid only when IGMPv2 or IGMPv3 messages can be processed in the VSI.
- If you do not specify **group-policy** when configuring the fast leave function, this function applies to all groups. To specify a group policy in the command, create an ACL and configure rules for the ACL before running the command. The default ACL rule denies all multicast groups. If you do not want to apply the fast leave to a group, use the **rule permit source any** command.

Example

Allow member ports in the VSI **company1** to fast leave group 225.1.1.123.

```
<HUAWEI> system-view
[HUAWEI] acl number 2000
[HUAWEI-acl-basic-2000] rule permit source 225.1.1.123 0
[HUAWEI-acl-basic-2000] quit
[HUAWEI] igmp-snooping enable
[HUAWEI] igmp-snooping over-vpls enable
[HUAWEI] vsi company1
[HUAWEI-vsi-company1] igmp-snooping enable
[HUAWEI-vsi-company1] igmp-snooping prompt-leave group-policy 2000
```

Prevent member ports in the VSI **company1** from fast leaving group 225.1.1.123.

```
<HUAWEI> system-view
[HUAWEI] acl number 2000
[HUAWEI-acl-basic-2000] rule deny source 225.1.1.123 0
[HUAWEI-acl-basic-2000] quit
[HUAWEI] igmp-snooping enable
[HUAWEI] igmp-snooping over-vpls enable
[HUAWEI] vsi company1
[HUAWEI-vsi-company1] igmp-snooping enable
[HUAWEI-vsi-company1] igmp-snooping prompt-leave group-policy 2000
```

8.10.17 igmp-snooping query-interval

Function

The **igmp-snooping query-interval** command sets the general query interval in a VSI, that is, the interval at which IGMP General Query messages are sent in the VSI.

The **undo igmp-snooping query-interval** command restores the default general query interval in a VSI.

By default, Group-Specific Query messages are sent in a VSI at an interval of 125 seconds.

Format

igmp-snooping query-interval *query-interval*

undo igmp-snooping query-interval

Parameters

Parameter	Description	Value
query-interval	Specifies the interval at which IGMP General Query messages are sent.	The value is an integer that ranges from 1 to 65535, in seconds. The default value is 125.

Views

VSI view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The general query interval is used to calculate the aging time of group member ports. When a member port receives an IGMP Report message from a host, the switch starts the aging timer for the interface. The aging time is calculated using the following formula: Aging time = IGMP robustness variable x General query interval + Maximum response time for General Query messages. The **igmp-snooping query-interval** command sets the general query interval. The general query count is set by the **igmp-snooping robust-count** command, and the maximum response time for General Query messages is set by the **igmp-snooping max-response-time** command.

If the member port receives Report messages from downstream hosts within the aging time, the switch retains the member port in the outbound interface list of the corresponding Layer 2 multicast forwarding entry. If the member port does not receive any Report messages within the aging time, the switch considers that no group member is connected to the interface, and therefore deletes the interface from the Layer 2 multicast forwarding entry.

Prerequisites

IGMP snooping has been enabled for VPLS using the **igmp-snooping over-vpls enable** command in the system view.

Precautions

The configuration takes effect only when IGMP snooping is enabled in the VSI using the **igmp-snooping enable (VSI view)** command.

Example

Set the general query interval in VSI company1 to 100 seconds.

```
<HUAWEI> system-view
[HUAWEI] igmp-snooping enable
[HUAWEI] igmp-snooping over-vpls enable
```



```
[HUAWEI] vsi company1
[HUAWEI-vsi-company1] igmp-snooping enable
[HUAWEI-vsi-company1] igmp-snooping query-interval 100
```

8.10.18 igmp-snooping require-router-alert

Function

The **igmp-snooping require-router-alert** command configures the switch to drop the IGMP messages without the Router-Alert option in the IP header received from a VSI.

The **undo igmp-snooping require-router-alert** command restores the default setting.

By default, the switch does not check the Router-Alert option of IGMP messages and processes all the received IGMP messages, regardless of whether they carry the Router-Alert option in the IP header.

Format

igmp-snooping require-router-alert

undo igmp-snooping require-router-alert

Parameters

None

Views

VSI view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The Router-Alert option identifies the protocol packets that need to be processed by upper-layer routing protocols.

By default, the switch does not check whether IGMP messages contain the Router-Alert option and sends all the IGMP messages to the upper-layer routing protocol. After the **igmp-snooping require-router-alert** command is executed, the switch checks each IGMP message for the Router-Alert option and discards those IGMP messages with this option. This improves device performance, reduces cost, and enhances security of the upper-layer routing protocol.

Prerequisites

IGMP snooping has been enabled for VPLS using the **igmp-snooping over-vpls enable** command in the system view.

Precautions

The configuration takes effect only when IGMP snooping is enabled in the VSI using the **igmp-snooping enable (VSI view)** command.

Example

Configure the switch to discard the IGMP messages without the Router-Alert option in the IP header received from VSI company1.

```
<HUAWEI> system-view
[HUAWEI] igmp-snooping enable
[HUAWEI] igmp-snooping over-vpls enable
[HUAWEI] vsi company1
[HUAWEI-vsi-company1] igmp-snooping enable
[HUAWEI-vsi-company1] igmp-snooping require-router-alert
```

8.10.19 igmp-snooping robust-count

Function

The **igmp-snooping robust-count** command sets the IGMP robustness variable in a VSI, which specifies the query count.

The **undo igmp-snooping robust-count** command restores the default IGMP robustness variable in a VSI.

By default, the robustness variable in a VSI is 2.

Format

igmp-snooping robust-count *robust-count*

undo igmp-snooping robust-count

Parameters

Parameter	Description	Value
robust-count	Specifies the IGMP robustness variable in a VSI.	The value is an integer that ranges from 2 to 5. The default value is 2.

Views

VSI view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The IGMP robustness variable is used to adjust the aging time of group member interfaces.

- When a member port receives an IGMP Report message from a downstream host, the switch sets the aging time of the interface to: General query count x General query interval + Maximum response time for General Query messages. The **igmp-snooping robust-count** command sets the general query count. The general query interval is set by the **igmp-snooping query-interval** command, and the maximum response time for General Query messages is set by the **igmp-snooping max-response-time** command.
- When the member port receives a Leave message from a downstream host, the switch starts the aging timer of the interface to: Last member query interval x Last member query count. The **igmp-snooping robust-count** command sets the general query count. The last member query interval is set by the **igmp-snooping lastmember-queryinterval** command.

Prerequisites

IGMP snooping has been enabled for VPLS using the **igmp-snooping over-vpls enable** command in the system view.

Precautions

The configuration takes effect only when IGMP snooping is enabled in the VSI using the **igmp-snooping enable (VSI view)** command.

Example

Set the IGMP robustness variable to 5 in VSI company1.

```
<HUAWEI> system-view
[HUAWEI] igmp-snooping enable
[HUAWEI] igmp-snooping over-vpls enable
[HUAWEI] vsi company1
[HUAWEI-vsi-company1] igmp-snooping enable
[HUAWEI-vsi-company1] igmp-snooping robust-count 5
```

8.10.20 igmp-snooping router-aging-time

Function

The **igmp-snooping router-aging-time** command sets the aging time of dynamic router ports in a VSI.

The **undo igmp-snooping router-aging-time** command restores the default aging time of dynamic router ports in a VSI.

By default, the aging time of dynamic router ports in a VSI is 180 seconds.

Format

igmp-snooping router-aging-time *router-aging-time*

undo igmp-snooping router-aging-time

Parameters

Parameter	Description	Value
router-aging-time	Specifies the aging time of dynamic router ports in a VSI.	The value is an integer that ranges from 1 to 1000, in seconds. The default value is 180 seconds.

Views

VSI view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When a short-term congestion occurs on the network, it takes a longer time to transmit Query messages from the IGMP querier to the switch. If a router port on the switch ages in this period, the switch does not send Report or Leave messages to the router port. As a result, multicast data forwarding may be interrupted. Therefore, set a long aging time for router ports if the network is unstable.

Prerequisites

IGMP snooping has been enabled for VPLS using the **igmp-snooping over-vpls enable** command in the system view.

Configuration Impact

If a router port receives an IGMP Query message, the switch sets the remaining aging time of the router port to the configured value.

Precautions

The configuration takes effect only when IGMP snooping is enabled in the VSI using the **igmp-snooping enable (VSI view)** command.

A too short aging time causes frequent aging of router ports and degrades system performance.

Example

Set the aging time of router ports in VSI company1 to 500 seconds.

```
<HUAWEI> system-view
[HUAWEI] igmp-snooping enable
[HUAWEI] igmp-snooping over-vpls enable
[HUAWEI] vsi company1
[HUAWEI-vsi-company1] igmp-snooping enable
[HUAWEI-vsi-company1] igmp-snooping router-aging-time 500
```


8.10.21 igmp-snooping router-learning

Function

The **igmp-snooping router-learning** command enables router port learning in a VSI.

The **undo igmp-snooping router-learning** command disables router port learning in a VSI.

By default, router port learning is enabled in a VSI.

Format

igmp-snooping router-learning

undo igmp-snooping router-learning

Parameters

None

Views

VSI view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A switch running IGMP snooping considers an interface as a dynamic router port when the interface receives an IGMP General Query message with any source IP address except 0.0.0.0. Router ports are configured to guide forwarding of IGMP Report/Leave messages. To prevent interfaces in a VSI from becoming a router port, disable router port learning in the VSI.

Prerequisites

IGMP snooping has been enabled for VPLS using the **igmp-snooping over-vpls enable** command in the system view.

Follow-up Procedure

The switch does not listen on IGMP Query messages in a VSI after router port learning is disabled in the VSI. Therefore, run the **igmp-snooping static-router-port** command to configure a static router port.

Precautions

The configuration takes effect only when IGMP snooping is enabled in the VSI using the **igmp-snooping enable (VSI view)** command.

Example

Disable router port learning in VSI company1.

```
<HUAWEI> system-view
[HUAWEI] igmp-snooping enable
[HUAWEI] igmp-snooping over-vpls enable
[HUAWEI] vsi company1
[HUAWEI-vsi-company1] igmp-snooping enable
[HUAWEI-vsi-company1] undo igmp-snooping router-learning
```

8.10.22 igmp-snooping send-router-alert

Function

The **igmp-snooping send-router-alert** command configures the switch to send IGMP messages with the Router-Alert option in the IP header to a VSI.

The **undo igmp-snooping send-router-alert** command configures the switch to send IGMP messages without the Router-Alert option in the IP header to a VSI.

By default, the switch sends the IGMP messages with the Router-Alert option in the IP header.

Format

igmp-snooping send-router-alert

undo igmp-snooping send-router-alert

Parameters

None

Views

VSI view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The Router-Alert option identifies the protocol packets that need to be processed by upper-layer routing protocols.

By default, the switch does not check whether IGMP messages contain the Router-Alert option and sends all the IGMP messages to the upper-layer routing protocol. Sending IGMP messages without the Router-Alert option improves device performance, reduces cost, and enhances security of the upper-layer routing protocol.

Prerequisites

IGMP snooping has been enabled for VPLS using the **igmp-snooping over-vpls enable** command in the system view.

Precautions

The configuration takes effect only when IGMP snooping is enabled in the VSI using the **igmp-snooping enable (VSI view)** command.

Example

Configure the switch to send IGMP messages without the Router-Alert option in the IP header to VSI company1.

```
<HUAWEI> system-view
[HUAWEI] igmp-snooping enable
[HUAWEI] igmp-snooping over-vpls enable
[HUAWEI] vsi company1
[HUAWEI-vsi-company1] igmp-snooping enable
[HUAWEI-vsi-company1] undo igmp-snooping send-router-alert
```

8.10.23 igmp-snooping ssm-mapping

Function

The **igmp-snooping ssm-mapping** command configures the mapping between a multicast group and a multicast source in a VSI.

The **undo igmp-snooping ssm-mapping** command deletes the mapping between a multicast group and a multicast source in a VSI.

By default, no mappings between multicast groups and multicast sources exist in a VSI.

Format

igmp-snooping ssm-mapping *ip-group-address* { *ip-group-mask* | *mask-length* } *ip-source-address*

undo igmp-snooping ssm-mapping *ip-group-address* { *ip-group-mask* | *mask-length* } *ip-source-address*

Parameters

Parameter	Description	Value
ip-group-address	Specifies the IP address of a multicast group.	The value is in dotted decimal notation, and the value range is specified by the **igmp-snooping ssm-policy** command.
ip-group-mask	Specifies the mask of the multicast group address.	The value is in dotted decimal notation.

Parameter	Description	Value
mask-length	Specifies the mask length of the multicast group address.	The value is an integer that ranges from 4 to 32.
ip-source-address	Specifies the IP address of a multicast source.	The value is in dotted decimal notation.

Views

VSI view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The SSM mapping mechanism converts IGMPv1 and IGMPv2 Report messages into messages with (S, G) information. This mechanism enables hosts that do not support IGMPv3 to work with SSM. To use this mechanism, enable SSM mapping and configure mappings between a multicast group G and multicast sources such as S1, S2 on the switch connected to user hosts. When the switch receives IGMPv1 and IGMPv2 Report messages for a multicast group, it checks the group address of the messages. If the group address is in the SSM group range, the switch converts the messages into one or more IGMPv3 IS_IN (S1, S2...) messages with the group address G.

Prerequisites

- IGMP snooping has been enabled for VPLS using the **igmp-snooping over-vpls enable** command.
- The IGMP message version is set to IGMPv3 using the **igmp-snooping version** command in the VSI.
- An SSM group policy has been configured using the **igmp-snooping ssm-policy** command in the VSI to add the multicast group address to the SSM group range. This prerequisite is required when the multicast group address is an any-source multicast (ASM) address.
- SSM mapping is enabled using the **igmp-snooping ssm-mapping enable** command.

Precautions

The configuration takes effect only when IGMP snooping is enabled in the VSI using the **igmp-snooping enable (VSI view)** command.

Example

Map multicast group 238.0.0.1 to multicast source 10.1.1.1 in VSI company1.


```
<HUAWEI> system-view
[HUAWEI] igmp-snooping enable
[HUAWEI] igmp-snooping over-vpls enable
[HUAWEI] vsi company1
[HUAWEI-vsi-company1] igmp-snooping enable
[HUAWEI-vsi-company1] igmp-snooping version 3
[HUAWEI-vsi-company1] igmp-snooping ssm-mapping enable
[HUAWEI-vsi-company1] igmp-snooping ssm-mapping 238.0.0.1 32 10.1.1.1
```

8.10.24 igmp-snooping ssm-mapping enable

Function

The **igmp-snooping ssm-mapping enable** command enables source-specific multicast (SSM) mapping in a VSI.

The **undo igmp-snooping ssm-mapping enable** command disables SSM mapping in a VSI.

By default, SSM mapping is disabled in a VSI.

Format

igmp-snooping ssm-mapping enable

undo igmp-snooping ssm-mapping enable

Parameters

None

Views

VSI view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On an SSM network, hosts running IGMPv1 or IGMPv2 cannot select multicast sources when they join a multicast group. To provide SSM services for these hosts, enable SSM mapping on the switch.

Prerequisites

- IGMP snooping has been enabled for VPLS using the **igmp-snooping over-vpls enable** command.
- The IGMP message version is set to v3 using the **igmp-snooping version** command in the VSI.

Follow-up Procedure

If the multicast group address is an any-source multicast (ASM) address, configure an SSM group policy to add the multicast group address to the SSM group range using the **igmp-snooping ssm-policy** command in the VSI view.

Run the **igmp-snooping ssm-mapping** command to configure mapping between multicast groups and multicast sources.

Precautions

The configuration takes effect only when IGMP snooping is enabled in the VSI using the **igmp-snooping enable (VSI view)** command.

Example

Enable SSM mapping in VSI company1.

```
<HUAWEI> system-view
[HUAWEI] igmp-snooping enable
[HUAWEI] igmp-snooping over-vpls enable
[HUAWEI] vsi company1
[HUAWEI-vsi-company1] igmp-snooping enable
[HUAWEI-vsi-company1] igmp-snooping version 3
[HUAWEI-vsi-company1] igmp-snooping ssm-mapping enable
```

8.10.25 igmp-snooping ssm-policy

Function

The **igmp-snooping ssm-policy** command configures an SSM group policy in a VSI. All the multicast groups permitted by the SSM group policy are SSM groups.

The **undo igmp-snooping ssm-policy** command deletes the SSM group policy from a VSI.

By default, no SSM group policy is available in a VSI.

Format

igmp-snooping ssm-policy *basic-acl-number*

undo igmp-snooping ssm-policy

Parameters

Parameter	Description	Value
basic-acl-number	Specifies the number of the basic ACL that defines the range of SSM groups.	The value is an integer that ranges from 2000 to 2999.

Views

VSI view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

SSM allows multicast group addresses in the range of 232.0.0.0 to 232.255.255.255. If hosts need to join multicast groups out of this range or they are allowed to join only some of multicast groups in the range, configure an SSM group range for the hosts.

Prerequisites

IGMP snooping has been enabled for VPLS using the **igmp-snooping over-vpls enable** command in the system view.

Precautions

The **igmp-snooping ssm-policy** command takes effect only when the following configurations are complete:

- IGMP snooping has been enabled in the specified VSI using the **igmp-snooping enable (VSI view)** command.
- SSM mapping has been enabled in the specified VSI using the **igmp-snooping ssm-mapping enable** command.
- If IGMPv1 or IGMPv2 packets are sent by user hosts, the IGMP message version is set to IGMPv3 using the **igmp-snooping version** command in the VSI.
- The ACL has been created and configured rules for the ACL. By default, the ACL applied to an SSM group policy denies all multicast groups. Therefore, to exclude specific group addresses from the SSM group address range, use a **rule permit source any** rule with **deny** rules in the ACL. For details about ACL configuration commands, see **14.1 ACL Configuration Commands**.

Example

Specify multicast group 225.1.1.123 as an SSM group in VSI company1.

```
<HUAWEI> system-view
[HUAWEI] acl number 2000
[HUAWEI-acl-basic-2000] rule permit source 225.1.1.123 0
[HUAWEI-acl-basic-2000] quit
[HUAWEI] igmp-snooping enable
[HUAWEI] igmp-snooping over-vpls enable
[HUAWEI] vsi company1
[HUAWEI-vsi-company1] igmp-snooping enable
[HUAWEI-vsi-company1] igmp-snooping ssm-mapping enable
[HUAWEI-vsi-company1] igmp-snooping ssm-policy 2000
```

8.10.26 igmp-snooping static-router-port (interface view)

Function

The **igmp-snooping static-router-port** command configures an AC-side interface in a VSI as a static router port.

The **undo igmp-snooping static-router-port** command deletes the static router port configuration.

By default, no AC-side interface in a VSI is configured as a static router port.

Format

igmp-snooping static-router-port vsi *vsi-name*

undo igmp-snooping static-router-port vsi *vsi-name*

Parameters

Parameter	Description	Value
vsi *vsi-name*	Specifies the VSI to which a static router port belongs.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Views

GE interface view, 100GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, Eth-Trunk interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To allow the interface connected to an upstream router to keep receiving or forwarding IGMP Report/Leave packets for a long time, configure the interface as a static router port.

Prerequisites

IGMP snooping has been enabled globally using the **igmp-snooping enable (system view)** command.

Precautions

- The configuration takes effect only when IGMP snooping is enabled in the VSI using the **igmp-snooping enable (VSI view)** command.
- Interfaces on a VPLS network include PW-side interfaces and AC-side interfaces. This command configures an AC-side interface as a static router port. To configure a PW-side interface as a static router port, run the **igmp-snooping static-router-port (VSI view)** command.

- On a VPLS network, ACs can be set up on different types of interfaces. The method to configure an AC-side interface as a static router port varies according to the type of the AC-side interface:
  - If the AC-side interface bound to a VSI is a physical interface that has been switched to Layer 3 mode using the **undo portswitch** command, run the **igmp-snooping static-router-port** command on this interface.
  - If the AC-side interface bound to a VSI is a VLANIF interface, configure the Layer 2 interface in the corresponding VLAN as a static router port. For details, see the **igmp-snooping static-router-port vlan** { *vlan-id1* [**to** *vlan-id2*] } &<1-10> command in "VLAN-based IGMP Snooping Configuration Commands."

Example

Configure GE0/0/1 as a static router port in the VSI **company1**. (GE0/0/1 has been bound to the VSI **company1**. IGMP snooping has been enabled globally and in the VSI **company1**.)

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] igmp-snooping static-router-port vsi company1
```

8.10.27 igmp-snooping static-router-port (VSI view)

Function

The **igmp-snooping static-router-port** command configures a PW-side interface in a VSI as a static router port.

The **undo igmp-snooping static-router-port** command deletes the static router port configuration.

By default, no PW-side interface in a VSI is configured as a static router port.

Format

igmp-snooping static-router-port remote-peer *ip-address* [**negotiation-vc-id** *vc-id*]

undo igmp-snooping static-router-port remote-peer *ip-address* [**negotiation-vc-id** *vc-id*]

Parameters

Parameter	Description	Value
remote-peer *ip-address*	Specifies the IP address of the remote peer.	The value is in dotted decimal notation.

Parameter	Description	Value
negotiation-vc-id *vc-id*	Specifies a virtual circuit ID. Generally, this parameter is specified when two ends of a PW have different VSI names. The *vc-id* parameter must specify an unused VC ID. That is, the specified VC ID cannot be the same as the VSI ID configured for any other VSI or the VC ID specified by **negotiation-vc-id** *vc-id* in another VSI.	The value is an integer that ranges from 1 to 4294967295.

Views

VSI view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To allow the interface connected to an upstream router to keep receiving or forwarding IGMP Report/Leave packets for a long time, configure the interface as a static router port.

Prerequisites

IGMP snooping has been enabled for VPLS using the **igmp-snooping over-vpls enable** command in the system view.

Precautions

The configuration takes effect only when IGMP snooping is enabled in the VSI using the **igmp-snooping enable (VSI view)** command.

Interfaces on a VPLS network include PW-side interfaces and AC-side interfaces. This command configures a PW-side interface as a static router port. The method to configure an AC-side interface as a static router port varies according to the type of the AC-side interface:

- If the AC-side interface bound to a VSI is a VLANIF interface, configure the Layer 2 interface in the corresponding VLAN as a static router port. For details, see the **igmp-snooping static-router-port vlan** { *vlan-id1* [**to** *vlan-id2*] } &<1-10> command in "VLAN-based IGMP Snooping Configuration Commands."

- If the AC-side interface bound to a VSI is a physical interface that has been switched to Layer 3 mode using the **undo portswitch** command, run the **igmp-snooping static-router-port vsi** *vsi-name* command on this interface.

Example

Configure the PW-side interface (with remote peer 1.1.1.1) as a static router port.

```
<HUAWEI> system-view
[HUAWEI] igmp-snooping enable
[HUAWEI] igmp-snooping over-vpls enable
[HUAWEI] vsi company1
[HUAWEI-vsi-company1] igmp-snooping enable
[HUAWEI-vsi-company1] igmp-snooping static-router-port remote-peer 1.1.1.1
```

8.10.28 igmp-snooping version

Function

The **igmp-snooping version** command configures the version of IGMP messages that can be processed by IGMP snooping in a VSI.

The **undo igmp-snooping version** command restores the default IGMP snooping version.

By default, the IGMP snooping version is 2, indicating that IGMP snooping can process IGMPv1 and IGMPv2 messages.

Format

igmp-snooping version *version*

undo igmp-snooping version

Parameters

Parameter	Description	Value
version	Specifies the version of IGMP messages that can be processed in a VSI.	The value is an integer that ranges from 1 to 3. • 1: indicates that IGMP snooping processes only IGMPv1 messages. • 2: indicates that IGMP snooping processes IGMPv1 and IGMPv2 messages. • 3: indicates that IGMP snooping processes IGMPv1, IGMPv2, and IGMPv3 messages.

Views

VSI view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When hosts in a VSI run different IGMP versions, run the **igmp-snooping version** command to enable the switch to process IGMP message from all the hosts.

Prerequisites

IGMP snooping has been enabled for VPLS using the **igmp-snooping over-vpls enable** command in the system view.

Precautions

The configuration takes effect only when IGMP snooping is enabled in the VSI using the **igmp-snooping enable (VSI view)** command.

Example

Set the IGMP snooping version to IGMPv1 in VSI company1.

```
<HUAWEI> system-view
[HUAWEI] igmp-snooping enable
[HUAWEI] igmp-snooping over-vpls enable
[HUAWEI] vsi company1
[HUAWEI-vsi-company1] igmp-snooping enable
[HUAWEI-vsi-company1] igmp-snooping version 1
```

8.10.29 l2-multicast backup-query forward

Function

The **l2-multicast backup-query forward** command configures the switch to forward IGMP Query messages to the backup PW.

The **undo l2-multicast backup-query forward** command disables the switch from forwarding IGMP Query messages to the backup PW.

By default, the switch does not forward IGMP Query messages to the backup PW.

Format

l2-multicast backup-query forward [**source-mac-replace**]

undo l2-multicast backup-query forward

Parameters

Parameter	Description	Value
source-mac-replace	Replaces the source MAC addresses in Query messages to the device MAC address before forwarding the Query messages.	-

Views

VSI view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Generally, two PWs are deployed on a VPLS network to ensure reliable service traffic transmission. The two PWs provide redundancy protection for service transmission. If IGMP snooping over VPLS is configured on the switch, the switch does not forward IGMP protocol packets to the backup PW by default. In this case, devices on the backup PW cannot create Layer 2 multicast forwarding entries because they cannot receive IGMP protocol packets. When the primary PW is Down and the backup PW becomes the new primary PW, multicast data traffic will be interrupted for a short time because devices on the new primary PW have not learned Layer 2 multicast forwarding entries. To solve this problem, configure the switch to forward IGMP protocol packets to the backup PW so that multicast data traffic can be quickly switched to the new primary PW.

This command configures the switch to forward IGMP Query messages to the backup PW.

Prerequisites

IGMP snooping has been enabled globally using the **igmp-snooping enable (system view)** command.

Precautions

The configuration takes effect only when IGMP snooping is enabled in the VSI using the **igmp-snooping enable (VSI view)** command.

Example

Configure the switch to forward IGMP Query messages to the backup PW.

```
<HUAWEI> system-view
[HUAWEI] igmp-snooping enable
[HUAWEI] igmp-snooping over-vpls enable
[HUAWEI] vsi company1
[HUAWEI-vsi-company1] igmp-snooping enable
[HUAWEI-vsi-company1] l2-multicast backup-query forward
```


8.10.30 l2-multicast backup-report forward

Function

The **l2-multicast backup-report forward** command configures the switch to forward IGMP Report/Leave messages to the backup PW.

The **undo l2-multicast backup-report forward** command disables the switch from forwarding IGMP Report/Leave messages to the backup PW.

By default, the switch does not forward IGMP Report/Leave messages to the backup PW.

Format

l2-multicast backup-report forward [**source-mac-replace**]

undo l2-multicast backup-report forward

Parameters

Parameter	Description	Value
source-mac-replace	Replaces the source MAC addresses in Report/Leave messages to the device MAC address before forwarding the Report/Leave messages.	-

Views

VSI view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Generally, two PWs are deployed on a VPLS network to ensure reliable service traffic transmission. The two PWs provide redundancy protection for service transmission. If IGMP snooping over VPLS is configured on the switch, the switch does not forward IGMP protocol packets to the backup PW by default. In this case, devices on the backup PW cannot create Layer 2 multicast forwarding entries because they cannot receive IGMP protocol packets. When the primary PW is Down and the backup PW becomes the new primary PW, multicast data traffic will be interrupted for a short time because devices on the new primary PW have not learned Layer 2 multicast forwarding entries. To solve this problem, configure the switch to forward IGMP protocol packets to the backup PW so that multicast data traffic can be quickly switched to the new primary PW.

This command configures the switch to forward IGMP Report/Leave messages to the backup PW.

Prerequisites

IGMP snooping has been enabled globally using the **igmp-snooping enable (system view)** command.

Precautions

The configuration takes effect only when IGMP snooping is enabled in the VSI using the **igmp-snooping enable (VSI view)** command.

Example

Configure the switch to forward IGMP Report/Leave messages to the backup PW.

```
<HUAWEI> system-view
[HUAWEI] igmp-snooping enable
[HUAWEI] igmp-snooping over-vpls enable
[HUAWEI] vsi company1
[HUAWEI-vsi-company1] igmp-snooping enable
[HUAWEI-vsi-company1] l2-multicast backup-report forward
```

8.10.31 l2-multicast static-group (interface view)

Function

The **l2-multicast static-group** command statically binds a multicast group to an AC-side interface in a VSI.

The **undo l2-multicast static-group** command deletes a static multicast from an AC-side interface.

By default, no multicast group is statically bound to an AC-side interface in a VSI.

Format

l2-multicast static-group [**source-address** *source-address*] **group-address** *group-address1* [**to** *group-address2*] **vsi** *vsi-name*

undo l2-multicast static-group [**source-address** *source-address*] **group-address** { *group-address1* [**to** *group-address2*] | **all** } **vsi** *vsi-name*

Parameters

Parameter	Description	Value
source-address *source-address*	Specifies the IP address of a multicast source.	The value is in dotted decimal notation.
group-address *group-address1* [**to** *group-address2*]	Specifies the IP address of a static multicast group.	The value ranges from 224.0.1.0 to 239.255.255.255 in dotted decimal notation.

Parameter	Description	Value
vsi *vsi-name*	Specifies the name of a VSI.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
all	Deletes all static multicast groups.	-

Views

GE interface view, 100GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, Eth-Trunk interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In addition to dynamic multicast forwarding entries generated by Layer 2 protocol protocols, you can configure static Layer 2 multicast forwarding entries by binding groups to interfaces. After a group is statically bound to an interface, users connected to this interface can keep receiving multicast data of the group over a long time.

Static Layer 2 multicast has the following advantages:

- Protects the system against attacks from protocol packets.
- Reduces the network delay by directly forwarding multicast packets based on static forwarding entries.
- Prevents unregistered users from receiving multicast flows, improving information security and protecting service providers' interests.

Prerequisites

IGMP snooping has been enabled globally using the **igmp-snooping enable (system view)** command.

Precautions

- The configuration takes effect only when IGMP snooping is enabled in the VSI using the **igmp-snooping enable (VSI view)** command.
- A static multicast member port does not respond to Query messages sent from an IGMP querier. When a group or (S, G) is statically bound to or

unbound from an interface, the interface does not send an IGMP Membership Report message or Leave message.

- Interfaces on a VPLS network include PW-side interfaces and AC-side interfaces. This command statically binds a group to an AC-side interface. To statically bind a group to a PW-side interface, run the **l2-multicast static-group (VSI view)** command.
- On a VPLS network, ACs can be set up on different types of interfaces. The method to statically bind a group to an AC-side interface varies according to the type of the AC-side interface:
  - If the AC-side interface bound to a VSI is a physical interface that has been switched to Layer 3 mode using the **undo portswitch** command, run the **l2-multicast static-group** command on this interface.
  - If the AC-side interface bound to a VSI is a VLANIF interface, bind a group to the Layer 2 interface in the corresponding VLAN. For details, see the **l2-multicast static-group** command in "VLAN-based IGMP Snooping Configuration Commands."

Example

Statically bind group 225.0.0.1 to GE0/0/1. (GE0/0/1 has been bound to the VSI **company1**. IGMP snooping has been enabled globally and in the VSI **company1**.)

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] l2-multicast static-group group-address 225.0.0.1 vsi company1
```

8.10.32 l2-multicast static-group (VSI view)

Function

The **l2-multicast static-group** command statically binds a multicast group to a PW-side interface in a VSI.

The **undo l2-multicast static-group** command deletes a static multicast from a PW-side interface.

By default, no multicast group is statically bound to a PW-side interface in a VSI.

Format

l2-multicast static-group [**source-address** *source-address*] **group-address** *group-address* **remote-peer** *ip-address* [**negotiation-vc-id** *vc-id*]

undo l2-multicast static-group [**source-address** *source-address*] **group-address** { *group-address* | **all** } **remote-peer** *ip-address* [**negotiation-vc-id** *vc-id*]

Parameters

Parameter	Description	Value
source-address *source-address*	Specifies the IP address of a multicast source.	The value is in dotted decimal notation.

Parameter	Description	Value
group-address *group-address*	Specifies the IP address of a static multicast group.	The value of *group-address* ranges from 224.0.1.0 to 239.255.255.255 in dotted decimal notation.
remote-peer *ip-address*	Indicates the IP address of the remote peer.	The value is in dotted decimal notation.
negotiation-vc-id *vc-id*	Specifies a virtual circuit ID. Generally, this parameter is specified when two ends of a PW have different VSI names.	The *vc-id* parameter must specify an unused VC ID. That is, the specified VC ID cannot be the same as the VSI ID configured for any other VSI or the VC ID specified by **negotiation-vc-id** *vc-id* in another VSI. The value is an integer that ranges from 1 to 4294967295.
all	Deletes all static multicast groups.	-

Views

VSI view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In addition to dynamic multicast forwarding entries generated by Layer 2 protocol protocols, you can configure static Layer 2 multicast forwarding entries by binding entries to interfaces. After a multicast group is statically bound to an interface, users connected to this interface can keep receiving multicast data of the multicast group for a long time.

Static Layer 2 multicast has the following advantages:

- Protects the system against attacks from protocol packets.
- Reduces the network delay by directly forwarding multicast packets based on static forwarding entries.
- Prevents unregistered users from receiving multicast flows, improving information security and protecting service providers' interests.

Prerequisites

IGMP snooping has been enabled for VPLS using the **igmp-snooping over-vpls enable** command in the system view.

Precautions

- The configuration takes effect only when IGMP snooping is enabled in the VSI using the **igmp-snooping enable (VSI view)** command.
- A static multicast member port does not respond to Query messages sent from an IGMP querier. When an interface is statically bound to or unbound from a multicast group or (S, G), the interface does not send an IGMP Membership Report message or Leave message.
- Interfaces on a VPLS network include PW-side interfaces and AC-side interfaces. This command statically binds a group to a PW-side interface. The method to statically bind a group to an AC-side interface varies according to the type of the AC-side interface:
  - If the AC-side interface bound to a VSI is a VLANIF interface, bind a group to the Layer 2 interface in the corresponding VLAN. For details, see the **l2-multicast static-group** command in "VLAN-based IGMP Snooping Configuration Commands."
  - If the AC-side interface bound to a VSI is a physical interface that has been switched to Layer 3 mode using the **undo portswitch** command, run the **l2-multicast static-group** [**source-address** *source-address*] **group-address** *group-address1* [**to** *group-address2*] **vsi** *vsi-name* command on this interface.

Example

Statically bind group 224.1.1.1 to the PW (with the remote IP address as 1.1.1.1) in the VSI **company1**.

```
<HUAWEI> system-view
[HUAWEI] igmp-snooping enable
[HUAWEI] igmp-snooping over-vpls enable
[HUAWEI] vsi company1
[HUAWEI-vsi-company1] igmp-snooping enable
[HUAWEI-vsi-company1] l2-multicast static-group group-address 224.1.1.1 remote-peer 1.1.1.1
```

8.10.33 reset igmp-snooping group

Function

The **reset igmp-snooping group** command clears dynamic multicast forwarding entries.

Format

reset igmp-snooping group { **vsi** { **name** *vsi-name* [[**source-address** *source-address*] **group-address** *group-address*] | **all** } | **all** }

Parameters

Parameter	Description	Value
name *vsi-name*	Clears the dynamic multicast forwarding entries of a specified VSI.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
all	Clears the dynamic multicast forwarding entries of all VSIs.	-
source-address *source-address*	Deletes the dynamic group memberships of a specified source address.	The value is in dotted decimal notation.
group-address *group-address*	Deletes the dynamic group memberships of a specified group address.	The value of *group-address* ranges from 224.0.1.0 to 239.255.255.255 in dotted decimal notation.

Views

User view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When multicast groups on interfaces change, the system generates new Layer 2 multicast forwarding entries until the aging time of multicast member interfaces expire. To enable the system to generate new multicast forwarding entries immediately, use the **reset igmp-snooping group** command to clear old multicast forwarding entries.

Precautions

NOTICE

If the command clears the dynamic forwarding entries of a VSI, the hosts in the VSI cannot receive multicast packets.

This command cannot clear static multicast forwarding entries.

Example

Delete all dynamic forwarding entries of VSI **company1**.

```
<HUAWEI> reset igmp-snooping group vsi name company1
```

8.10.34 reset igmp-snooping statistics

Function

The **reset igmp-snooping statistics** command clears IGMP snooping statistics.

Format

reset igmp-snooping statistics { **vsi** { **name** *vsi-name* | **all** } | **all** }

Parameters

Parameter	Description	Value
name *vsi-name*	Clears IGMP snooping statistics in a specified VSI.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
all	Clears all the IGMP snooping statistics.	-

Views

User view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To analyze the IGMP snooping statistics collected in a certain period, run this command to clear the previous statistics. After a while, run the **display igmp-snooping statistics** command to view the IGMP snooping statistics.

Precautions

NOTICE

The cleared IGMP snooping statistics cannot be restored.

Example

Clear IGMP snooping statistics of VSI company1.

```
<HUAWEI> reset igmp-snooping statistics vsi name company1
```

8.11 BD-based IGMP Snooping Configuration Commands

8.11.1 Command Support

Only the S6730-H, S6730S-H, S6730-S, S6730S-S, S5732-H, S5731-S, S5731S-S, S5731S-H, S5731-H, S6735-S, S6720-EI, S6720S-EI support BD-based IGMP snooping.

8.11.2 display igmp-snooping

Function

The **display igmp-snooping** command displays the IGMP snooping running parameters.

Format

display igmp-snooping [**bridge-domain** [*bd-id*]]

Parameters

Parameter	Description	Value
bridge-domain [*bd-id*]	Displays the IGMP snooping running parameters in a specified BD.	The value is an integer that ranges from 1 to 16777215.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After IGMP snooping is configured for a VXLAN network, you can use this command to view the IGMP snooping running parameters.

To view the IGMP snooping configuration, run the **display igmp-snooping configuration** command.

Example

Display the IGMP snooping running parameters.

```
<HUAWEI> display igmp-snooping bridge-domain 123
  IGMP Snooping Information for BDID 123
    IGMP Snooping is Enabled
    IGMP Version is Set to default 2
    IGMP Query Interval is 1s
    IGMP Max Response Interval is Set to default 10s
    IGMP Robustness is Set to default 2
    IGMP Last Member Query Interval is Set to default 1s
    IGMP Router Port Aging Interval is Set to 180s
    IGMP Filter Group-Policy is not set
    IGMP Prompt Leave Disable
    IGMP Router Alert is Not Required
    IGMP Send Router Alert Enable
    IGMP Report Suppress Disable
    IGMP Suppress Time is set to default 10 seconds
    IGMP Querier Enable
    IGMP Router Port Learning Enable
    IGMP SSM-Mapping Enable
    IGMP SSM-policy acl number is 2008
```

Table 8-130 Description of the **display igmp-snooping** command output

Item	Description
IGMP Snooping Information for BDID 123	The following information displayed is the IGMP snooping running parameters in BD 123.
IGMP Snooping is Enabled	IGMP snooping is enabled in the BD. By default, IGMP snooping is disabled in a BD. IGMP snooping can be enabled in a BD using the **igmp-snooping enable (BD view)** command.
IGMP Version is Set to default 2	Version of IGMP messages that can be processed in the BD. In this example, the default version 2 is displayed, indicating that both IGMPv1 and IGMPv2 messages can be processed. This parameter is configured using the **igmp-snooping version** command.
IGMP Query Interval is 1s	Interval at which IGMP General Query messages are sent. This parameter is configured using the **igmp-snooping query-interval** command.
IGMP Max Response Interval is Set to default 10s	Maximum response time for IGMP General Query messages. This parameter is configured using the **igmp-snooping max-response-time** command.

Item	Description
IGMP Robustness is Set to default 2	IGMP robustness variable. This parameter is configured using the **igmp-snooping robust-count** command.
IGMP Last Member Query Interval is Set to default 1s	Interval at which IGMP Group-Specific Query messages are sent. This parameter is configured using the **igmp-snooping lastmember-queryinterval** command.
IGMP Router Port Aging Interval is Set to 180s	Aging time of a router port. This parameter is configured using the **igmp-snooping router-aging-time** command.
IGMP Filter Group-Policy is not set	Multicast group policy. In this example, that is, no policy is configured. A multicast group policy is configured using the **igmp-snooping group-policy** command.
IGMP Prompt Leave Disable	The fast leave function is disabled for interfaces in the BD. The fast leave function can be enabled using the **igmp-snooping prompt-leave** command.
IGMP Router Alert is Not Required	The switch does not require that the IGMP messages received from the BD contain the Router-Alert option in the IP header. The switch can be configured to discard IGMP messages without the Router-Alert option using the **igmp-snooping require-router-alert** command.
IGMP Send Router Alert Enable	The switch sends the IGMP messages with the Router-Alert option to the BD. The switch can be configured to send IGMP messages with the Router-Alert option using the **igmp-snooping send-router-alert** command.
IGMP Report Suppress Disable	IGMP message suppression is disabled. IGMP message suppression can be enabled using the **igmp-snooping report-suppress** command.
IGMP Suppress Time is set to default 10 seconds	IGMP message suppression time. This parameter is configured using the **igmp-snooping suppress-time** command.
IGMP Querier Enable	IGMP snooping querier is enabled. IGMP snooping querier can be enabled using the **igmp-snooping querier enable** command.
IGMP Router Port Learning Enable	Router port learning is enabled. Router port learning can be enabled using the **igmp-snooping router-learning** command.

Item	Description
IGMP SSM-Mapping Disable	IGMP snooping SSM mapping is disabled. IGMP snooping SSM mapping can be enabled using the **igmp-snooping ssm-mapping enable** command.
IGMP SSM-policy acl number is 2008	SSM group policy for IGMP snooping. The SSM group policy for IGMP snooping can be configured using the **igmp-snooping ssm-policy** command.

8.11.3 display igmp-snooping configuration

Function

The **display igmp-snooping configuration** command displays the IGMP snooping configuration.

Format

display igmp-snooping [**bridge-domain** [*bd-id*]] **configuration**

Parameters

Parameter	Description	Value
bridge-domain [*bd-id*]	Displays IGMP snooping configurations in a specified BD.	The value is an integer that ranges from 1 to 16777215.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run this command to check whether the IGMP snooping configurations for a VXLAN network are correct.

To check all IGMP snooping running parameters, run the **display igmp-snooping** command.

Example

Display the IGMP snooping configuration in BD 123.


```
<HUAWEI> display igmp-snooping bridge-domain 123 configuration
 IGMP Snooping Configuration for BDID 123
    igmp-snooping enable
    igmp-snooping query-interval 1s
    igmp-snooping querier enable
    igmp-snooping ssm-mapping enable
    igmp-snooping ssm-policy 2008
    igmp-snooping ssm-mapping 225.0.0.1 255.255.255.255 10.0.0.1
```

8.11.4 display igmp-snooping port-info

Function

The **display igmp-snooping port-info** command displays information about multicast group member ports.

Format

display igmp-snooping port-info [**bridge-domain** *bd-id* [**group-address** *group-address*]] [**verbose**]

Parameters

Parameter	Description	Value
bridge-domain *bd-id*	Displays multicast group member ports in a specified BD.	The value is an integer that ranges from 1 to 16777215.
group-address *group-address*	Displays information about member ports of a specified multicast group. If this parameter is not specified, the system displays member ports of all multicast groups.	The value ranges from 224.0.1.0 to 239.255.255.255, in dotted decimal notation.
verbose	Displays detailed information about multicast group member ports. If this parameter is not specified, the system displays the summary of multicast group member ports.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

When the switch with IGMP snooping enabled receives IGMP messages exchanged between hosts and a Layer 3 device, the switch maintains a Layer 2 multicast forwarding table based on information in the messages. The **display igmp-snooping port-info** command shows member ports in the Layer 2 multicast forwarding table. According to the command output, you can know which downlink ports of the switch have multicast users connected, and control multicast services conveniently.

Precautions

Information about multicast group member ports can be displayed only after IGMP snooping is enabled in the BD using the **igmp-snooping enable** command.

Example

Display information about multicast group member ports in BD 123.

```
<HUAWEI> display igmp-snooping port-info bridge-domain 123
----------------------------------------------------------------------------
                        (Source, Group)  Port                      Flag
             Flag: S:Static    D:Dynamic    M: Ssm-mapping
----------------------------------------------------------------------------
 BDID 123, 1 Entry(s)
                         (*, 225.0.0.2)  XGE0/0/4(VID:101)          S--
                                         1 port(s) include
----------------------------------------------------------------------------
```

Table 8-131 Description of the **display igmp-snooping port-info** command output

Item	Description
(Source, Group)	(S, G) entry, specifying the multicast source and multicast group. Multicast data is sent from multicast source S to group G. If S is displayed as *, multicast data may be sent from any multicast source. If S is displayed as an IP address, multicast data is sent from this IP address.
Port	Member port. TNL indicates VXLAN tunnel information. **include** and **exclude** indicate the multicast source filtering mode.
Flag	Type of a member port, which can be: ● S: static member port, which is configured using the **l2-multicast static-group** command ● D: dynamic member port learned through IGMP snooping ● M: member port established through SSM mapping
BDID 123, 1 Entry(s)	BD ID and the number of entries in the BD.

Display detailed information about all multicast group member ports.

```
<HUAWEI> display igmp-snooping port-info verbose
The port information of Group 225.0.0.2 on BDID 123:
   Time of this group has been up : 05:05:07

 The port information of (0.0.0.0, 225.0.0.2):
   Time of this source has been up : 05:05:07
   Port Table on this source(0.0.0.0):
   List of ports in include mode:
     No.1
       Port name : XGE0/0/4(VID:101)
       Time of this port has been up as a host-port : NA
       Remain time of port expire as dynamic host-port : NA
       Host-port flags : Static
   There are 1 port(s) in include mode.
   List of ports in exclude mode:
     No.1
       Port name : XGE0/0/5(VID:101)
       Time of this port has been up as a host-port : NA
       Remain time of port expire as dynamic host-port : NA
       Host-port flags : Static
   There are 1 port(s) in exclude mode.
```

Table 8-132 Description of the display igmp-snooping port-info verbose command output

Item	Description
The port information of Group 225.0.0.2 on BDID 123	Information about member ports of multicast group 225.0.0.2 in BD 123.
Time of this group has been up	Time that elapsed since the multicast group was set up.
The port information of (0.0.0.0, 225.0.0.2)	Information about member ports of a specified (S, G).
Time of this source has been up	Time that elapsed since the multicast source was set up.
Port Table on this source	List of member ports of the specified multicast source.
List of ports in include mode	Information about member ports that join a multicast group in INCLUDE mode.
List of ports in exclude mode	Information about member ports that join a multicast group in EXCLUDE mode.
No.1	First member port.
Port name	Type and number of the first member port.
Time of this port has been up as a host-port	Time that elapsed since the first member port was bound to a source or (S, G).

Item	Description
Remain time of port expire as dynamic host-port	Aging time of the first member port. This field displays "NA" for a static member port. The aging time of a dynamic member port is calculated using the following formula: Aging time = Robustness variable x General query interval + Maximum response time for General Query messages. The robustness variable is configured using the **igmp-snooping robust-count** command. The general query interval is configured using the **igmp-snooping query-interval** command. The maximum response time for General Query messages is configured using the **igmp-snooping max-response-time** command.
Host-port flags	Type of a member port, which can be: ● Static: static member ● Dynamic: dynamic member port learned through IGMP snooping ● Mapping: member port established through SSM mapping
There are *x* port(s) in include mode	Number of member ports that join a multicast group in INCLUDE mode.
There are *x* port(s) in exclude mode	Number of member ports that join a multicast group in EXCLUDE mode.

8.11.5 display igmp-snooping router-port

Function

The **display igmp-snooping router-port** command displays information about the router ports in a specified BD, including static and dynamic router ports.

Format

display igmp-snooping router-port bridge-domain [*bd-id*]

Parameters

Parameter	Description	Value
bridge-domain [*bd-id*]	Displays information about the router ports in a specified BD. If *bd-id* is not specified, the command displays router ports in all BDs.	The value is an integer that ranges from 1 to 16777215.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

A router port connects the switch to an upstream Layer 3 multicast device. The router port can be statically configured or dynamically generated after the interface receives an IGMP Query message or a PIM Hello message.

You can run the **display igmp-snooping router-port** command to view the type, name, lifetime, and aging time of a router port.

Precautions

This command can display information about router ports in a BD only when IGMP snooping has been enabled in the BD using the **igmp-snooping enable (BD view)** command, and at least one interface in the BD is in Up state.

Example

Display information about router ports in BD 123.

```
<HUAWEI> display igmp-snooping router-port bridge-domain 123
Port Name                UpTime       Expires      Flags
 ----------------------------------------------------------------------------
 BDID 123, 2 router-port(s)
 XGE0/0/36(VID:101)       07:24:05     --           STATIC
 XGE0/0/4(VID:102)        05:15:50     --           STATIC
```

Table 8-133 Description of the display igmp-snooping router-port command output

Item	Description
Port Name	Type and number of a router port. TNL indicates VXLAN tunnel information.
UpTime	Time that elapsed since the interface became a router port.
Expires	Aging time of the router port. • The aging time is displayed for a dynamic router port. This parameter is configured using the **igmp-snooping router-aging-time** command. • For a static router port, "--" is displayed, indicating that the static router does not age.

Item	Description
Flags	Type of the router port, which can be: • STATIC: static router port configured using the **igmp-snooping static-router-port** command. • DYNAMIC: dynamic router port

8.11.6 display igmp-snooping statistics

Function

The **display igmp-snooping statistics** command displays IGMP snooping statistics.

Format

display igmp-snooping statistics bridge-domain [*bd-id*]

Parameters

Parameter	Description	Value
bridge-domain [*bd-id*]	Displays IGMP snooping statistics in a specified BD. If *bd-id* is not specified, the system displays IGMP snooping statistics in all BDs.	The value is an integer that ranges from 1 to 16777215.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

After IGMP snooping is configured, you can run the **display igmp-snooping statistics** command to view IGMP snooping statistics, including the number of IGMP messages sent and received in each BD.

Precautions

This command displays IGMP snooping statistics only when IGMP snooping has been enabled globally using the **igmp-snooping enable (BD view)** command.

Example

Display IGMP snooping statistics in BD 123.

```
<HUAWEI> display igmp-snooping statistics bridge-domain 123
 IGMP Snooping Packets Counter
   Statistics for BDID 123
     Recv V1 Report          0
     Recv V2 Report          6621
     Recv V3 Report          0
     Recv V1 Query           0
     Recv V2 Query           335516
     Recv V3 Query           0
     Recv General Query      0
     Recv Leave              26
     Recv Pim Hello          0
     Send Query(S=0)         33
     Send Query(S!=0)        0
     Suppress Report         0
     Suppress Leave          0
     Proxy Send General Query              0
     Proxy Send Group-Specific Query       0
     Proxy Send Group-Source-Specific Query 0
```

Table 8-134 Description of the display igmp-snooping statistics command output

Item	Description
IGMP Snooping Packets Counter	Statistics on IGMP Snooping packets.
Statistics for BDID 123	Packet statistics in BD 123.
Recv V1 Report	Number of IGMPv1 Report messages received.
Recv V2 Report	Number of IGMPv2 Report messages received.
Recv V3 Report	Number of IGMPv3 Report messages received.
Recv V1 Query	Number of IGMPv1 Query messages received.
Recv V2 Query	Number of IGMPv2 Query messages received.
Recv V3 Query	Number of IGMPv3 Query messages received.
Recv General Query	Interval for sending IGMP General Query messages.
Recv Leave	Number of IGMP Leave messages received.
Recv Pim Hello	Number of PIM Hello messages received.
Send Query(S=0)	Number of IGMP Query messages sent with the source address 0.0.0.0.
Send Query(S!=0)	Number of IGMP Query messages sent with source addresses other than 0.0.0.0.

Item	Description
Suppress Report	Number of duplicate IGMP Report messages dropped.
Suppress Leave	Number of duplicate IGMP Leave messages dropped.
Proxy Send General Query	Number of General Query messages sent by the IGMP snooping proxy.
Proxy Send Group-Specific Query	Number of Group-Specific Query messages sent by the IGMP snooping proxy.
Proxy Send Group-Source-Specific Query	Number of Group-Source-Specific Query messages sent by the IGMP snooping proxy.

8.11.7 display l2-multicast forwarding-table bridge-domain

Function

The **display l2-multicast forwarding-table bridge-domain** command displays the Layer 2 multicast forwarding table in BDs.

Format

display l2-multicast forwarding-table bridge-domain [*bd-id* [[**source-address** *source-address*] **group-address** { *group-address* | **router-group** }]]

Parameters

Parameter	Description	Value
bd-id	Displays Layer 2 multicast forwarding entries in a specified BD. If *bd-id* is not specified, the command displays Layer 2 multicast forwarding entries in all BDs.	The value is an integer that ranges from 1 to 16777215.
source-address *source-address*	Displays the forwarding entries of a specified Layer 2 multicast source.	The value is in dotted decimal notation.
group-address *group-address*	Displays multicast forwarding entries of a specified Layer 2 multicast group.	The value ranges from 224.0.1.0 to 239.255.255.255, in dotted decimal notation.

Parameter	Description	Value
router-group	Displays Layer 2 multicast forwarding entries of all router ports.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After completing IGMP snooping configuration, you can use the **display l2-multicast forwarding-table** command to view the Layer 2 multicast forwarding table. This command displays statically configured and dynamically learned multicast forwarding entries.

Example

Display the Layer 2 multicast forwarding table in BD 123.

```
<HUAWEI> display l2-multicast forwarding-table bridge-domain 123
Bridge domain  : 123, Forwarding Mode : MAC
Total Group(s) : 1
--------------------------------------------------------------------------------
Group(Mac)                          Interface       Out-Vlan/InLabel
--------------------------------------------------------------------------------
                       Router-port   XGigabitEthernet0/0/36      101
                       Router-port   XGigabitEthernet0/0/4       102
0100-5e00-0002                         XGigabitEthernet0/0/4       101
                                  XGigabitEthernet0/0/36      101
                                  XGigabitEthernet0/0/4       102
--------------------------------------------------------------------------------
```

Table 8-135 Description of the **display l2-multicast forwarding-table bridge-domain** command output

Item	Description
Bridge domain	BD ID of the forwarding entries.
Forwarding Mode	Multicast forwarding mode used in the BD. Only the MAC address-based forwarding mode is supported.
Total Group(s)	Total number of multicast forwarding entries.
Group(Mac)	Group MAC address.
Interface	Outbound interface. The Router-port field indicates a router port.

Item	Description
Out-Vlan/InLabel	VLAN ID. When the **Interface** value is a VTEP IP address, this parameter is left blank.

8.11.8 igmp-snooping enable (system view)

Function

The **igmp-snooping enable** command enables IGMP snooping globally.

The **undo igmp-snooping enable** command disables IGMP snooping globally.

By default, IGMP snooping is disabled globally.

Format

igmp-snooping enable

undo igmp-snooping enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

BD-based IGMP snooping runs on multiple VTEPs on a VXLAN network. A device sets up a Layer 2 multicast forwarding table by snooping IGMP messages exchanged between multicast users in a BD and the upstream device, and forwards multicast packets on the VXLAN network according to the Layer 2 multicast forwarding table.

Before configuring IGMP snooping for a VXLAN network, enable IGMP snooping globally. Other IGMP snooping configuration commands can be used only after you run the **igmp-snooping enable** command in the system view.

Precautions

When you run the **undo igmp-snooping enable** command in the system view, the system displays a message, asking you whether to disable IGMP snooping globally. When you disable IGMP snooping globally, all the IGMP snooping configurations

are deleted. When you run the **igmp-snooping enable** command to enable IGMP snooping globally again, the device uses the default IGMP snooping configuration.

Example

Enable IGMP snooping globally.

```
<HUAWEI> system-view
[HUAWEI] igmp-snooping enable
```

8.11.9 igmp-snooping enable (BD view)

Function

The **igmp-snooping enable** command enables IGMP snooping in a BD.

The **undo igmp-snooping enable** command disables IGMP snooping in a BD.

By default, IGMP snooping is disabled in a BD.

Format

igmp-snooping enable

undo igmp-snooping enable

Parameters

None

Views

BD view

Default Level

2: Configuration level

Usage Guidelines

Application Scenario

To implement IGMP snooping on a VXLAN network, a device needs to set up Layer 2 multicast forwarding entries by snooping IGMP messages exchanged between multicast users in a BD and the upstream router. To achieve this, IGMP snooping needs to be enabled in the BD view.

Prerequisites

IGMP snooping has been enabled for the VXLAN network using the **igmp-snooping over-vxlan enable** command in the system view.

Example

Enable IGMP snooping in BD 123.

```
<HUAWEI> system-view
[HUAWEI] igmp-snooping enable
```



```
[HUAWEI] igmp-snooping over-vxlan enable
[HUAWEI] bridge-domain 123
[HUAWEI-bd123] igmp-snooping enable
```

8.11.10 igmp-snooping fast-switch enable

Function

The **igmp-snooping fast-switch enable** command enables fast multicast forwarding path switching upon STP topology changes.

The **undo igmp-snooping fast-switch enable** command disables fast multicast forwarding path switching upon STP topology changes.

By default, fast multicast forwarding path switching upon STP topology changes is disabled.

Format

igmp-snooping fast-switch enable

undo igmp-snooping fast-switch enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the Layer 2 network topology changes, multicast forwarding paths may change. When this occurs, the upstream querier sends a Query message to switch the multicast forwarding path. However, there is a delay (60s by default) between the time when network topology change occurs and the time when the Query message is sent. As a result, the downstream device cannot receive the Query message immediately, so the multicast forwarding path cannot be quickly switched.

If the Layer 2 network is running the Spanning Tree Protocol (STP), you can enable fast multicast forwarding path switching upon STP topology changes. When the STP topology changes, this function quickly changes the ports in Forwarding state into router ports to direct multicast data flows to the new forwarding paths.

Prerequisite

Global IGMP snooping has been enabled using the **igmp-snooping enable (system view)** command.

Precautions

- This function takes effect only when STP is used as the loop prevention protocol on a Layer 2 network and the STP operation mode is MSTP, RSTP, or STP.
- With this function configured, the switch sets all ports in Forwarding state as router ports when the STP topology changes. In this case, multicast data flows are forwarded to all the router ports before the router ports are aged. This will cause increase in multicast traffic on the network.

Example

Enable fast multicast forwarding path switching upon STP topology changes.

```
<HUAWEI> system-view
[HUAWEI] igmp-snooping enable
[HUAWEI] igmp-snooping over-vxlan enable
[HUAWEI] igmp-snooping fast-switch enable
```

8.11.11 igmp-snooping group-policy(BD view)

Function

The **igmp-snooping group-policy** command configures a multicast group policy in a BD.

The **undo igmp-snooping group-policy** command deletes the multicast group policy from a BD.

By default, no multicast group policy is available in a BD, and hosts in the BD can join any multicast group.

Format

igmp-snooping group-policy *acl-number* [**version** *version-number*]

undo igmp-snooping group-policy

Parameters

Parameter	Description	Value
acl-number	Specifies the number of an ACL used to restrict the range of groups users can join.	The number of a basic ACL is an integer that ranges from 2000 to 2999. The number of an advanced ACL ranges from 3000 to 3999.

Parameter	Description	Value
version *version-number*	Applies the multicast group policy only to the IGMP messages of the specified version. If this parameter is not specified, the multicast group policy applies to all IGMP messages.	The value is an integer that ranges from 1 to 3. ● 1: IGMPv1 ● 2: IGMPv2 ● 3: IGMPv3

Views

BD view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A multicast group policy controls the multicast programs that users can order on a switch with IGMP snooping enabled. When a user orders a multicast program, the user host sends a Report message, requesting to join the multicast group. After the switch receives the message, it checks whether the multicast group matches the multicast group policy applied to the BD. If the messages match the ACL, the switch allows user hosts in the BD to join the group and accepts the Report messages. If the messages do not match the ACL, the switch prevents the user hosts in the BD from joining the group.

Prerequisites

IGMP snooping has been enabled for the VXLAN network using the **igmp-snooping over-vxlan enable** command in the system view.

Precautions

- The configuration takes effect only when IGMP snooping is enabled in the BD using the **igmp-snooping enable (BD view)** command..
- Before running the **igmp-snooping group-policy (BD view)** command, run the **acl** command to configure the ACL that you want to apply to the group policy to limit the range of multicast groups that hosts connected to the BD can join.
  - In the basic ACL view, set **source** in the **rule** command to the range of multicast groups that the BD can join.
  - In the advanced ACL view, set **source** in the **rule** command to the source address that is allowed to send multicast data to the specified multicast groups, and set **destination** to the range of multicast groups that the BD can join.

After the **igmp-snooping group-policy (BD view)** command is executed on the BD:

- The BD filters the received Report messages based on the ACL and maintains memberships only for the multicast groups permitted by the ACL.
- The BD discards the Report messages that are denied by the ACL. If the entries of the multicast groups denied by the ACL exist on the switch, the switch deletes these entries when the aging time of the entries expires.
- If the IGMP version is not specified, the specified ACL applies to IGMPv1, IGMPv2, and IGMPv3 hosts.

Example

Prevent hosts in BD 123 from joining group 225.1.1.123.

```
<HUAWEI> system-view
[HUAWEI] acl number 2000
[HUAWEI-acl-basic-2000] rule deny source 225.1.1.123 0
[HUAWEI-acl-basic-2000] quit
[HUAWEI] igmp-snooping enable
[HUAWEI] igmp-snooping over-vxlan enable
[HUAWEI] bridge-domain 123
[HUAWEI-bd123] igmp-snooping enable
[HUAWEI-bd123] igmp-snooping group-policy 2000
```

Allow hosts in BD 123 to join group 225.1.1.123.

```
<HUAWEI> system-view
[HUAWEI] acl number 2000
[HUAWEI-acl-basic-2000] rule permit source 225.1.1.123 0
[HUAWEI-acl-basic-2000] quit
[HUAWEI] igmp-snooping enable
[HUAWEI] igmp-snooping over-vxlan enable
[HUAWEI] bridge-domain 123
[HUAWEI-bd123] igmp-snooping enable
[HUAWEI-bd123] igmp-snooping group-policy 2000
```

8.11.12 igmp-snooping lastmember-queryinterval

Function

The **igmp-snooping lastmember-queryinterval** command sets the last member query interval in a BD, that is, the interval at which Group-Specific Query messages are sent in the BD.

The **undo igmp-snooping lastmember-queryinterval** command restores the default last member query interval in a BD.

By default, Group-Specific Query messages are sent in a BD at intervals of 1 second.

Format

igmp-snooping lastmember-queryinterval *lastmember-queryinterval*

undo igmp-snooping lastmember-queryinterval

Parameters

Parameter	Description	Value
lastmember-queryinterval	Specifies the interval at which IGMP Group-Specific Query messages are sent.	The value is an integer that ranges from 1 to 5, in seconds.

Views

BD view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

By setting the last member query interval, you can:

- Configure the switch to send IGMP Group-Specific Query messages at intervals when the querier function is enabled.
- Change the aging time of multicast group member ports.

  When the switch receives an IGMP Leave message from a host, the switch starts the aging timer for the corresponding member port. The aging time is calculated using the following formula: Aging time = Last member query interval x Last member query count. The **igmp-snooping lastmember-queryinterval** command sets the last member query interval. The last member query count is set by the **igmp-snooping robust-count** command.

  If the switch (querier) receives Report messages from other hosts within the aging time, it continues to maintain memberships of the multicast group. If the switch does not receive any Report messages within the aging time, it stops maintaining memberships of the multicast group.

Prerequisites

IGMP snooping has been enabled for the VXLAN network using the **igmp-snooping over-vxlan enable** command in the system view.

Precautions

The switch sets the maximum response time field in the Group-Specific Query message to the configured last member query interval. Therefore, the maximum response time for Group-Specific Query messages is the same as the interval at which Group-Specific Query messages are sent.

The configuration takes effect only when all the following conditions are met:

- IGMP snooping is enabled in the BD using the **igmp-snooping enable (BD view)** command.

- The IGMP message version is set to v2 or v3 messages in the BD. (Hosts running IGMPv1 do not send Leave messages when they leave a multicast group.)

Example

Set the last member query interval in BD 123 to 4 seconds.

```
<HUAWEI> system-view
[HUAWEI] igmp-snooping enable
[HUAWEI] igmp-snooping over-vxlan enable
[HUAWEI] bridge-domain 123
[HUAWEI-bd123] igmp-snooping enable
[HUAWEI-bd123] igmp-snooping lastmember-queryinterval 4
```

8.11.13 igmp-snooping learning

Function

The **igmp-snooping learning** command enables learning of multicast group memberships on an interface.

The **undo igmp-snooping learning** command disables learning of multicast group memberships on an interface.

By default, learning of multicast group memberships is enabled on an interface.

Format

igmp-snooping learning vlan { { *vlan-id1* [**to** *vlan-id2*] } &<1-10> | **all** }

undo igmp-snooping learning vlan { { *vlan-id1* [**to** *vlan-id2*] } &<1-10> | **all** }

Parameters

Parameter	Description	Value
vlan { *vlan-id1* [**to** *vlan-id2*] }	Enables learning of multicast group memberships in specified VLANs. The interface must have been added to the specified VLAN. *vlan-id1* [**to** *vlan-id2*] specifies the range of VLAN IDs. • *vlan-id1*: specifies the first VLAN ID. • **to** *vlan-id2*: specifies the last VLAN ID. If **to** *vlan-id2* is not specified, learning of multicast group memberships is enabled only in the VLAN specified by *vlan-id1*.	The values of *vlan-id1* and *vlan-id2* are integers that range from 1 to 4094. The value of *vlan-id2* must be greater than the value of *vlan-id1*. The *vlan-id1* and *vlan-id2* parameters identify a range of VLANs.
all	Enables learning of multicast group memberships in all VLANs that an interface has joined.	-

Views

MultiGE interface view, GE interface view, XGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, port group view, Eth-Trunk interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A group member port is a user-side interface that connects to multicast group members. Group memberships can be learned dynamically or configured statically. An interface is identified as a dynamic group member port when it receives an IGMP Report message.

If users connected to an interface need to receive data of a fixed multicast group, the interface can be statically bound to the multicast group. In this case, run the

undo igmp-snooping learning command on the interface to disable learning of group memberships. This reduces the system resources used for protocol packet exchange.

Prerequisites

IGMP snooping has been enabled for the VXLAN network using the **igmp-snooping over-vxlan enable** command in the system view.

Precautions

The configuration takes effect only when all the following conditions are met:

- The VLAN specified in this command has been bound to a BD, and IGMP snooping has been enabled in the BD using the **igmp-snooping enable (BD view)** command.
- The interface belongs to the specified VLANs.

If you run the **undo igmp-snooping learning** command multiple times, all the configurations take effect.

Example

Disable learning of group memberships on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] igmp-snooping enable
[HUAWEI] igmp-snooping over-vxlan enable
[HUAWEI] bridge-domain 123
[HUAWEI-bd123] l2 binding vlan 100
[HUAWEI-bd123] igmp-snooping enable
[HUAWEI-bd123] quit
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] port link-type trunk
[HUAWEI-GigabitEthernet0/0/1] port trunk allow-pass vlan 100
[HUAWEI-GigabitEthernet0/0/1] undo igmp-snooping learning vlan 100
```

8.11.14 igmp-snooping max-response-time

Function

The **igmp-snooping max-response-time** command sets the maximum response time for IGMP General Query messages in a BD.

The **undo igmp-snooping max-response-time** command restores the default maximum response time for IGMP General Query messages in a BD.

By default, the maximum response time for IGMP General messages in a BD is 10 seconds.

Format

igmp-snooping max-response-time *max-response-time*

undo igmp-snooping max-response-time

Parameters

Parameter	Description	Value
max-response-time	Specifies the maximum response time for IGMP General Query messages.	The value is an integer that ranges from 1 to 25, in seconds. The default value is 10.

Views

BD view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Setting IGMP snooping parameters helps improve the multicast forwarding performance. By setting the maximum response time for IGMP General Query messages, you can:

- Control the deadline for a host to send an IGMP Report message. When hosts are required to respond to IGMP General Query messages quickly, set a short maximum response time. To avoid congestion caused by a large number of IGMP messages sent by hosts, set a long maximum response time.
- Adjust the aging time of member ports. When the switch receives a Report message, it starts the aging timer for the member port. The aging time is calculated using the following formula: Aging time = General query count x General query interval + Maximum response time for General Query messages. The **igmp-snooping max-response-time** command sets the maximum response time. The General query count is set by the **igmp-snooping robust-count** command, and the general query interval is set by the **igmp-snooping query-interval** command.

The switch sets the maximum response time field in General Query messages to the value set by the **igmp-snooping max-response-time** command.

Prerequisites

IGMP snooping has been enabled for the VXLAN network using the **igmp-snooping over-vxlan enable** command in the system view.

Follow-up Procedure

Perform the following operations to improve multicast performance:

- Run the **igmp-snooping query-interval** command to set the interval at which General Query messages are sent.
- Run the **igmp-snooping lastmember-queryinterval** command to set the interval at which Group-Specific Query messages are sent.

Precautions

The configuration takes effect only after you run the **igmp-snooping enable (BD view)** command to enable IGMP snooping in the BD.

The maximum response time for General Query messages must be shorter than the interval at which General Query messages are sent. Otherwise, the switch will delete multicast memberships that should not be deleted.

Example

Set the maximum response time for IGMP Query messages in BD 123 to 20 seconds.

```
<HUAWEI> system-view
[HUAWEI] igmp-snooping enable
[HUAWEI] igmp-snooping over-vxlan enable
[HUAWEI] bridge-domain 123
[HUAWEI-bd123] igmp-snooping enable
[HUAWEI-bd123] igmp-snooping max-response-time 20
```

8.11.15 igmp-snooping over-vxlan enable

Function

The **igmp-snooping over-vxlan enable** command enables IGMP snooping for VXLAN.

The **undo igmp-snooping over-vxlan enable** command disables IGMP snooping for VXLAN.

By default, IGMP snooping for VXLAN is disabled.

Format

igmp-snooping over-vxlan enable

undo igmp-snooping over-vxlan enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Before configuring IGMP snooping in a VXLAN, enable IGMP snooping globally and for VXLAN in the system view.

Prerequisites

IGMP snooping has been enabled for the VXLAN network using the **igmp-snooping over-vxlan enable** command in the system view.

Precautions

When you run the **undo igmp-snooping over-vxlan enable** command in the system view, the system displays a message, asking you whether to disable IGMP snooping for VXLAN. If any IGMP snooping for VXLAN configuration has been made in the system, the device prompts you to delete all the IGMP snooping for VXLAN configuration.

Example

Enable IGMP snooping for VXLAN.

```
<HUAWEI> system-view
[HUAWEI] igmp-snooping enable
[HUAWEI] igmp-snooping over-vxlan enable
```

8.11.16 igmp-snooping prompt-leave

Function

The **igmp-snooping prompt-leave** command enables the fast leave function in a BD so that member ports in the BD can fast leave multicast groups.

The **undo igmp-snooping prompt-leave** command disables the fast leave function in a BD.

By default, the fast leave function is disabled in a BD.

Format

igmp-snooping prompt-leave [**group-policy** *acl-number*]

undo igmp-snooping prompt-leave

Parameters

Parameter	Description	Value
group-policy	Specifies a multicast group policy that allows member ports to fast leave some multicast groups. Before using this parameter, create an ACL and configure filter rules in the ACL.	-

Parameter	Description	Value
acl-number	Specifies the number of an ACL that defines a range of multicast groups. A basic or advanced ACL can be used.	The value is an integer that ranges from 2000 to 3999.

Views

BD view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The fast leave function enables the switch to delete the multicast forwarding entry of a multicast group from an interface immediately after the interface receives an IGMP Leave message for the group. This function saves bandwidth and system resources because the switch does not need to wait until the aging timer of the interface expires.

Prerequisites

IGMP snooping has been enabled for the VXLAN network using the **igmp-snooping over-vxlan enable** command in the system view.

Precautions

When an interface has more than one receiver connected, enabling the fast leave function interrupts multicast traffic of the other receivers in the multicast group. It is recommended that you enable this function only on interfaces with one receiver.

The configuration takes effect only when all the following conditions are met:

- IGMP snooping is enabled in the BD using the **igmp-snooping enable (BD view)** command.
- IGMPv2 or IGMPv3 messages can be processed in the BD.
- If you do not specify **group-policy** when configuring the fast leave function, this function takes effect for all groups. To specify a group policy in the command, create an ACL and configure rules for the ACL before running the command.

Example

Allow member ports in BD 123 to fast leave all groups.

```
<HUAWEI> system-view
[HUAWEI] igmp-snooping enable
```



```
[HUAWEI] igmp-snooping over-vxlan enable
[HUAWEI] bridge-domain 123
[HUAWEI-bd123] igmp-snooping enable
[HUAWEI-bd123] igmp-snooping prompt-leave
```

Allow member ports in BD 123 to fast leave group 225.1.1.123.

```
<HUAWEI> system-view
[HUAWEI] igmp-snooping enable
[HUAWEI] igmp-snooping over-vxlan enable
[HUAWEI] acl number 2000
[HUAWEI-acl-basic-2000] rule permit source 225.1.1.123 0
[HUAWEI-acl-basic-2000] quit
[HUAWEI] bridge-domain 123
[HUAWEI-bd123] igmp-snooping enable
[HUAWEI-bd123] igmp-snooping prompt-leave group-policy 2000
```

Prevent member ports in BD 123 from fast leaving group 225.1.1.123.

```
<HUAWEI> system-view
[HUAWEI] igmp-snooping enable
[HUAWEI] igmp-snooping over-vxlan enable
[HUAWEI] acl number 2000
[HUAWEI-acl-basic-2000] rule deny source 225.1.1.123 0
[HUAWEI-acl-basic-2000] quit
[HUAWEI] bridge-domain 123
[HUAWEI-bd123] igmp-snooping enable
[HUAWEI-bd123] igmp-snooping prompt-leave group-policy 2000
```

8.11.17 igmp-snooping querier enable

Function

The **igmp-snooping querier enable** command enables the IGMP snooping querier function in a BD.

The **undo igmp-snooping querier enable** command disables the IGMP snooping querier function in a BD.

By default, the IGMP snooping querier function is disabled in a BD.

Format

igmp-snooping querier enable

undo igmp-snooping querier enable

Parameters

None

Views

BD view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On an IGMP-capable network, a Layer 3 multicast device functions as a querier to send IGMP Query messages and maintain group memberships on the local network segment. If the Layer 3 multicast device does not run IGMP or it uses only static multicast forwarding entries, it cannot function as a querier. In this case, you can enable IGMP snooping querier on the downstream Layer 2 device so that it acts as a querier to send IGMP Query messages.

On a Layer 2 network that has no Layer 3 devices, multicast sources are connected to Layer 2 devices. IGMP snooping querier needs to be enabled on the Layer 2 devices so that they can maintain multicast group memberships.

Prerequisites

IGMP snooping has been enabled for the VXLAN network using the **igmp-snooping over-vxlan enable** command in the system view.

Follow-up Procedure

Perform the following operations as required on your network:

- Run the **igmp-snooping query-interval** command to set the interval at which General Query messages are sent.
- Run the **igmp-snooping lastmember-queryinterval** command to set the interval at which Group-Specific Query messages are sent.
- Run the **igmp-snooping robust-count** command to set the number of times Query messages are sent.

Configuration Impact

The IGMP snooping querier does not participate in IGMP querier election. However, the IGMP snooping querier on an IGMP-capable multicast network may affect the election result, because the Query messages sent by the IGMP snooping querier may have a smaller source IP address than the Query messages sent by other devices. Therefore, the IGMP snooping querier function is not recommended on an IGMP-capable multicast network.

Precautions

The configuration takes effect only after you run the **igmp-snooping enable (BD view)** command to enable IGMP snooping in the BD.

Example

Enable the querier function in BD 123.

```
<HUAWEI> system-view
[HUAWEI] igmp-snooping enable
[HUAWEI] igmp-snooping over-vxlan enable
[HUAWEI] bridge-domain 123
[HUAWEI-bd123] igmp-snooping enable
[HUAWEI-bd123] igmp-snooping querier enable
Warning: Please confirm that no other querier is configured on the network, otherwise this command may cause querier re-election, continue?[Y/N]:y
```


8.11.18 igmp-snooping query-interval

Function

The **igmp-snooping query-interval** command sets the general query interval in a BD, that is, the interval at which IGMP General Query messages are sent in the BD.

The **undo igmp-snooping query-interval** command restores the default general query interval in a BD.

By default, the general query interval is 125 seconds.

Format

igmp-snooping query-interval *query-interval*

undo igmp-snooping query-interval

Parameters

Parameter	Description	Value
query-interval	Specifies the interval at which IGMP General Query messages are sent.	The value is an integer that ranges from 1 to 65535, in seconds.

Views

BD view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

By setting the general query interval, you can:

- Configure the switch to send IGMP General Query messages at intervals to maintain memberships of interfaces. When a shorter interval is configured, the switch is more sensitive to multicast membership changes, but more bandwidth and system resources are consumed.
- Change the aging time of multicast member ports.

  When receiving an IGMP Report message from a host, the switch starts the aging timer for the multicast member port. The aging time is calculated using the following formula: Aging time = IGMP robustness variable x General query interval + Maximum response time for General Query messages. The **igmp-snooping query-interval** command sets the general query interval. The general query count is set by the **igmp-snooping robust-count** command,

and the maximum response time for General Query messages is set by the **igmp-snooping max-response-time** command.

The general query interval affects the aging time of group member ports. A shorter general query interval results in a shorter aging time of group member ports and therefore a faster update speed of Layer 2 multicast entries. However, when there are many downstream users connected to a device, a short general query interval can cause flapping of multicast entries, leading to a high CPU usage on the device. Therefore, the default general query interval is recommended. If you need to change the interval to suit service deployment, set the value according to the following table.

Number of IGMP Messages Sent from Downstream Users Within Maximum Response Time	Minimum General Query Interval Reference Value (Seconds)
1 to 1024	10
1024 to 2048	20
2048 to 5120	40

NOTE

The default general query interval defined in RFC documents is 125 seconds, but some vendors define their own default general query intervals. It is recommended that all devices on a multicast network use the same general query intervals (including IGMP and IGMP snooping general query intervals). On Huawei fixed switches, the default value of the IGMP general query interval is 60 seconds, and the default value of the IGMP snooping general query interval is 125 seconds.On Huawei modular switches, the default values of the IGMP general query interval and IGMP snooping general query interval are both 60 seconds.

Prerequisites

IGMP snooping has been enabled for the VXLAN network using the **igmp-snooping over-vxlan enable** command in the system view.

Precautions

- The configuration takes effect only after you run the **igmp-snooping enable (BD view)** command to enable IGMP snooping in the BD.
- The interval at which General Query messages are sent must be longer than the maximum response time for General Query messages. Otherwise, the switch will delete multicast memberships that should not be deleted.

Example

Set the general query interval in BD 123 to 100 seconds.

```
<HUAWEI> system-view
[HUAWEI] igmp-snooping enable
[HUAWEI] igmp-snooping over-vxlan enable
[HUAWEI] bridge-domain 123
[HUAWEI-bd123] igmp-snooping enable
[HUAWEI-bd123] igmp-snooping query-interval 100
```


8.11.19 igmp-snooping report-suppress

Function

The **igmp-snooping report-suppress** command enables suppression of IGMP Report and Leave messages in a BD.

The **undo igmp-snooping report-suppress** command disables suppression of IGMP Report and Leave messages in a BD.

By default, IGMP Report and Leave message suppression is disabled in a BD.

Format

igmp-snooping report-suppress

undo igmp-snooping report-suppress

Parameters

None

Views

BD view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When a Layer 2 device receives an IGMP Membership Report message (Report or Leave message) from a group member, the Layer 2 device forwards the message to the directly connected Layer 3 device. A group member host sends a Membership Report message in the following situations:

- When joining a multicast group, a host sends a Report message. When a multicast group has multiple members in a BD, the Layer 3 device receives duplicate Report messages from the member hosts.
- When receiving an IGMP General Query message, a host sends a Report message. Hosts use a timer to suppress duplicate Report messages on the same network segment. However, if the timer values on hosts are the same, the Layer 3 device can still receive duplicate Report messages.
- A host running IGMPv2 or IGMPv3 sends a Leave message when leaving a multicast group. When a multicast group has multiple members in a BD, the Layer 3 device receives duplicate Leave messages from the member hosts.

After Report message suppression is enabled on a Layer 2 device, the device forwards only one IGMP Membership Report message to the upstream device in the following scenarios:

- When the first member joins a multicast group or a host sends a Report message in response to an IGMP Query message, the Layer 2 device forwards a Report message to the upstream device. The upstream device can create or maintain the matching forwarding entry based on the Report message.
- When the last member of a multicast group leaves the group, the Layer 2 device forwards a Leave message to the upstream device. The upstream device then deletes the matching forwarding entry.

This reduces the number of IGMP messages on the network.

Prerequisites

IGMP snooping has been enabled for the VXLAN network using the **igmp-snooping over-vxlan enable** command in the system view.

Configuration Impact

- The configuration takes effect only after you run the **igmp-snooping enable (BD view)** command to enable IGMP snooping in the BD.
- When receiving a Leave message from a group member, the device sends Group-Specific Query messages to check whether the group has other members on the network segment.
- The device can suppress duplicate Report messages even when IGMP message suppression is disabled. The default suppression time is 10 seconds. To change the suppression time, run the **igmp-snooping suppress-time** *suppress-time* command. If the *suppress-time* is set to 0, all the membership packets are forwarded immediately.
- This function cannot suppress IGMPv3 packets.

Example

Enable suppression of Report and Leave messages in BD 123.

```
<HUAWEI> system-view
[HUAWEI] igmp-snooping enable
[HUAWEI] igmp-snooping over-vxlan enable
[HUAWEI] bridge-domain 123
[HUAWEI-bd123] igmp-snooping enable
[HUAWEI-bd123] igmp-snooping report-suppress
```

8.11.20 igmp-snooping require-router-alert

Function

The **igmp-snooping require-router-alert** command configures the switch to drop the IGMP messages without the Router-Alert option in the IP header received from a BD.

The **undo igmp-snooping require-router-alert** command restores the default configuration.

By default, the switch does not check the Router-Alert option of IGMP messages and processes all the received IGMP messages, regardless of whether they carry the Router-Alert option in the IP header.

Format

igmp-snooping require-router-alert

undo igmp-snooping require-router-alert

Parameters

None

Views

BD view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The Router-Alert option identifies the protocol messages that need to be processed by upper-layer routing protocols.

By default, the switch does not check whether IGMP messages contain the Router-Alert option and sends all the IGMP messages to the upper-layer routing protocol. After the **igmp-snooping require-router-alert** command is executed, the switch checks each IGMP message for the Router-Alert option and discards those IGMP messages without this option. This improves device performance, reduces cost, and enhances security of the upper-layer routing protocol

Prerequisites

IGMP snooping has been enabled for the VXLAN network using the **igmp-snooping over-vxlan enable** command in the system view.

Precautions

The configuration takes effect only after you run the **igmp-snooping enable (BD view)** command to enable IGMP snooping in the BD.

Example

Configure the switch to forward only the IGMP messages with the Router-Alert option in the IP header received from BD 123.

```
<HUAWEI> system-view
[HUAWEI] igmp-snooping enable
[HUAWEI] igmp-snooping over-vxlan enable
[HUAWEI] bridge-domain 123
[HUAWEI-bd123] igmp-snooping enable
[HUAWEI-bd123] igmp-snooping require-router-alert
```


8.11.21 igmp-snooping robust-count

Function

The **igmp-snooping robust-count** command sets the IGMP robustness variable in a BD, which specifies how many times IGMP Query messages are sent.

The **undo igmp-snooping robust-count** command restores the default IGMP robustness variable in a BD.

By default, the robustness variable in a BD is 2.

Format

igmp-snooping robust-count *robust-count*

undo igmp-snooping robust-count

Parameters

Parameter	Description	Value
robust-count	Specifies the IGMP robustness variable in a BD.	The value is an integer that ranges from 2 to 5.

Views

BD view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Setting IGMP snooping parameters helps improve the multicast forwarding performance. By setting the IGMP robustness variable, you can:

- Specify the number of times the querier sends a Group-Specific Query message, which prevents packet loss on the network.

  When receiving an IGMP Leave message for a multicast group, the switch sends a Group-Specific Query message a certain number of times (specified by the IGMP robustness variable) to check whether this group has any other members. If the quality of transmission links is low, increase the IGMP robustness variable.
- Change the aging time of multicast group member ports.

  When receiving an IGMP Report message from a host, the switch starts the aging timer for the member port. The aging time is calculated using the following formula: Aging time = IGMP robustness variable x General query

interval + Maximum response time for General Query messages. The **igmp-snooping robust-count** command sets the general query count.

Prerequisites

IGMP snooping has been enabled for the VXLAN network using the **igmp-snooping over-vxlan enable** command in the system view.

Follow-up Procedure

Perform the following operations to optimize multicast service performance:

- Run the **igmp-snooping query-interval** command to set the interval at which General Query messages are sent.
- Run the **igmp-snooping max-response-time** command to set the maximum response time for General Query messages.
- Run the **igmp-snooping lastmember-queryinterval** command to set the interval at which Group-Specific Query messages are sent.

Precautions

The configuration takes effect only after you run the **igmp-snooping enable (BD view)** command to enable IGMP snooping in the BD.

Example

Set the IGMP robustness variable to 5 in BD 123.

```
<HUAWEI> system-view
[HUAWEI] igmp-snooping enable
[HUAWEI] igmp-snooping over-vxlan enable
[HUAWEI] bridge-domain 123
[HUAWEI-bd123] igmp-snooping enable
[HUAWEI-bd123] igmp-snooping robust-count 5
```

8.11.22 igmp-snooping router-aging-time

Function

The **igmp-snooping router-aging-time** command sets the aging time of dynamic router ports in a BD.

The **undo igmp-snooping router-aging-time** command restores the default aging time of dynamic router ports in a BD.

By default, the aging time of dynamic router ports in a BD is 180 seconds or equal to the holdtime value contained in PIM Hello messages.

Format

igmp-snooping router-aging-time *router-aging-time*

undo igmp-snooping router-aging-time

Parameters

Parameter	Description	Value
router-aging-time	Specifies the aging time of dynamic router ports in a BD.	The value is an integer that ranges from 1 to 1000, in seconds.

Views

BD view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When a short-term congestion occurs on the network, it takes a longer time to transmit Query messages from the IGMP querier to the switch. If a router port on the switch ages in this period, the switch does not send Report or Leave messages to router ports. As a result, multicast data forwarding may be interrupted. Therefore, set a long aging time for the router port if the network is unstable.

When a dynamic router port on the switch receives an IGMP Query message or a PIM Hello message, the switch resets the aging time of the router port.

- If the router port receives an IGMP Query message, the switch sets the remaining aging time of the interface to the configured value.
- If the router port receives a PIM Hello message, the switch sets the aging time of the interface to the holdtime value.

Prerequisites

IGMP snooping has been enabled for the VXLAN network using the **igmp-snooping over-vxlan enable** command in the system view.

Precautions

If IGMP snooping is disabled in the specified BD, the configuration succeeds but does not take effect until IGMP snooping is enabled in the BD. To enable IGMP snooping in a BD, run the **igmp-snooping enable (BD view)** command.

If the aging time of a router port is too short, the router port ages frequently, degrading system performance.

Example

Set the aging time of router ports in BD 123 to 300 seconds.

```
<HUAWEI> system-view
[HUAWEI] igmp-snooping enable
[HUAWEI] igmp-snooping over-vxlan enable
```



```
[HUAWEI] bridge-domain 123
[HUAWEI-bd123] igmp-snooping enable
[HUAWEI-bd123] igmp-snooping router-aging-time 300
```

8.11.23 igmp-snooping router-learning (BD view)

Function

The **igmp-snooping router-learning** command enables router port learning in a BD.

The **undo igmp-snooping router-learning** command disables router port learning in a BD.

By default, router port learning is enabled in a BD.

Format

igmp-snooping router-learning

undo igmp-snooping router-learning

Parameters

None

Views

BD view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A router port is located on a Layer 2 device and connects to an upstream Layer 3 device (a multicast router or Layer 3 switch). A switch running IGMP snooping considers an interface as a dynamic router port when the interface receives an IGMP General Query message with any source IP address except 0.0.0.0 or a PIM Hello message. If the switch does not need to receive Query messages or PIM Hello messages from a BD, disable router port learning in the BD. A router port provides the following functions:

- Receives multicast data from the upstream device.
- Forwards IGMP Report/Leave messages. IGMP Report/Leave messages received in a BD are forwarded only to router ports in the BD.

By default, router port learning is enabled on an interface. To prevent interfaces in a BD from becoming a router port, disable router port learning in the BD.

Prerequisites

IGMP snooping has been enabled for the VXLAN network using the **igmp-snooping over-vxlan enable** command in the system view.

Follow-up Procedure

The switch does not listen on IGMP Query messages in a BD after router port learning is disabled in the BD. To ensure normal multicast forwarding in the BD, run the **igmp-snooping static-router-port** command to configure a static router port.

Precautions

If IGMP snooping is disabled in the specified BD, the configuration succeeds but does not take effect until IGMP snooping is enabled in the BD. To enable IGMP snooping in a BD, run the **igmp-snooping enable (BD view)** command.

Example

Disable router port learning in BD 123.

```
<HUAWEI> system-view
[HUAWEI] igmp-snooping enable
[HUAWEI] igmp-snooping over-vxlan enable
[HUAWEI] bridge-domain 123
[HUAWEI-bd123] igmp-snooping enable
[HUAWEI-bd123] undo igmp-snooping router-learning
```

8.11.24 igmp-snooping send-router-alert

Function

The **igmp-snooping send-router-alert** command configures the switch to send IGMP messages with the Router-Alert option in the IP header to a BD.

The **undo igmp-snooping send-router-alert** command configures the switch to send IGMP messages without the Router-Alert option in the IP header to a BD.

By default, the switch sends IGMP messages with the Router-Alert option in the IP header.

Format

igmp-snooping send-router-alert

undo igmp-snooping send-router-alert

Parameters

None

Views

BD view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The Router-Alert option identifies the protocol messages that need to be processed by upper-layer routing protocols.

By default, the switch sends IGMP messages with the Router-Alert option. If some devices in the same BD as the switch can process only the IGMP messages without the Router-Alert option, use the **undo igmp-snooping send-router-alert** command to configure the switch to send IGMP messages without the Router-Alert option.

The switch adds the Router-Alert option only to locally originated IGMP messages and does not add this option to IGMP messages received from other devices.

Prerequisites

IGMP snooping has been enabled for the VXLAN network using the **igmp-snooping over-vxlan enable** command in the system view.

Precautions

If IGMP snooping is disabled in the specified BD, the configuration succeeds but does not take effect until IGMP snooping is enabled in the BD. To enable IGMP snooping in a BD, run the **igmp-snooping enable (BD view)** command.

Example

Configure the switch to send IGMP messages that do not contain the Router-Alert option in the IP header to BD 123.

```
<HUAWEI> system-view
[HUAWEI] igmp-snooping enable
[HUAWEI] igmp-snooping over-vxlan enable
[HUAWEI] bridge-domain 123
[HUAWEI-bd123] igmp-snooping enable
[HUAWEI-bd123] undo igmp-snooping send-router-alert
```

8.11.25 igmp-snooping ssm-mapping

Function

The **igmp-snooping ssm-mapping** command configures the mapping between a multicast group and a multicast source in a BD.

The **undo igmp-snooping ssm-mapping** command deletes the mapping between a multicast group and a multicast source in a BD.

By default, no mappings between multicast groups and multicast sources exist in a BD.

Format

igmp-snooping ssm-mapping *group-address* { *group-mask* | *mask-length* } *source-address*

undo igmp-snooping ssm-mapping *group-address* { *group-mask* | *mask-length* } *source-address*

Parameters

Parameter	Description	Value
group-address	Specifies the IP address of a multicast group.	The value is in dotted decimal notation, and the value range is specified by the **igmp-snooping ssm-policy** command.
group-mask	Specifies the mask of the multicast group address.	The value is in dotted decimal notation.
mask-length	Specifies the mask length of the multicast group address.	The value is an integer that ranges from 4 to 32.
source-address	Specifies the IP address of the multicast source mapped to a multicast group.	The value is in dotted decimal notation.

Views

BD view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The SSM mapping mechanism converts IGMPv1 and IGMPv2 Report messages into messages with (S, G) information. This mechanism enables hosts that do not support IGMPv3 to work with SSM. To use this mechanism, enable SSM mapping and configure mappings between a multicast group G and multicast sources such as S1, S2 on the Layer 2 device connected to user hosts. When the Layer 2 device receives IGMPv1 and IGMPv2 Report messages for a multicast group, it checks the group address of the messages. If the group address is in the SSM group range, the Layer 2 device converts the messages into one or more IGMPv3 IS_IN (S1, S2...) messages with the group address G.

Prerequisites

IGMP snooping has been enabled for the VXLAN network using the **igmp-snooping over-vxlan enable** command in the system view.

Precautions

Before configuring the mapping between a multicast group and a multicast source:

- IGMP snooping has been enabled in the specified BD using the **igmp-snooping enable (BD view)** command.
- The IGMP message version is set to IGMPv3 using the **igmp-snooping version** command in the BD.
- SSM mapping has been enabled using the **igmp-snooping ssm-mapping enable** command.
- An SSM group policy has been configured using the **igmp-snooping ssm-policy** command in the BD to add the multicast group address to the SSM group range. This prerequisite is required when the multicast group address is an any-source multicast (ASM) address.

Example

Map multicast groups 238.1.1.1 through 238.1.1.255 to multicast source 10.1.1.1 in BD 123.

```
<HUAWEI> system-view
[HUAWEI] igmp-snooping enable
[HUAWEI] igmp-snooping over-vxlan enable
[HUAWEI] bridge-domain 123
[HUAWEI-bd123] igmp-snooping enable
[HUAWEI-bd123] igmp-snooping version 3
[HUAWEI-bd123] igmp-snooping ssm-mapping enable
[HUAWEI-bd123] igmp-snooping ssm-mapping 238.1.1.0 24 10.1.1.1
```

8.11.26 igmp-snooping ssm-mapping enable

Function

The **igmp-snooping ssm-mapping enable** command enables Source-Specific Multicast (SSM) mapping in a BD.

The **undo igmp-snooping ssm-mapping enable** command disables SSM mapping in a BD.

By default, SSM mapping is disabled in a BD.

Format

igmp-snooping ssm-mapping enable

undo igmp-snooping ssm-mapping enable

Parameters

None

Views

BD view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On an SSM network, hosts running IGMPv1 or IGMPv2 cannot select multicast sources when they join a multicast group. To provide SSM services for these hosts, enable SSM mapping on the Layer 2 devices connected to the hosts.

Prerequisites

IGMP snooping has been enabled for the VXLAN network using the **igmp-snooping over-vxlan enable** command in the system view.

Follow-up Procedure

Run the **igmp-snooping ssm-mapping** command to configure group-source mappings.

Precautions

- If IGMP snooping is disabled in the specified BD, the configuration succeeds but does not take effect until IGMP snooping is enabled in the BD. To enable IGMP snooping in a BD, run the **igmp-snooping enable (BD view)** command.
- SSM mapping is applicable only to the BDs where IGMP snooping can process IGMPv3 messages. To set the IGMP message version to v3, use the **igmp-snooping version** command in the BD.
- If the multicast group address is an Any-Source Multicast (ASM) address, configure an SSM group policy to add the multicast group address to the SSM group range using the **igmp-snooping ssm-policy** command in the BD view.

Example

Enable SSM mapping in BD 123.

```
<HUAWEI> system-view
[HUAWEI] igmp-snooping enable
[HUAWEI] igmp-snooping over-vxlan enable
[HUAWEI] bridge-domain 123
[HUAWEI-bd123] igmp-snooping enable
[HUAWEI-bd123] igmp-snooping version 3
[HUAWEI-bd123] igmp-snooping ssm-mapping enable
```

8.11.27 igmp-snooping ssm-policy

Function

The **igmp-snooping ssm-policy** command configures an SSM group policy in a BD to specify the range of SSM groups.

The **undo igmp-snooping ssm-policy** command deletes the SSM group policy from a BD.

By default, no SSM group policy is available in a BD.

Format

igmp-snooping ssm-policy *basic-acl-number*

undo igmp-snooping ssm-policy

Parameters

Parameter	Description	Value
basic-acl-number	Specifies the number of a basic ACL that defines the range of SSM groups.	The value is an integer that ranges from 2000 to 2999.

Views

BD view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

SSM allows multicast group addresses in the range of 232.0.0.0 to 232.255.255.255. If hosts need to join multicast groups out of this range or they are allowed to join only some of multicast groups in the range, configure an SSM group range for the hosts.

Prerequisites

IGMP snooping has been enabled for the VXLAN network using the **igmp-snooping over-vxlan enable** command in the system view.

Precautions

The **igmp-snooping ssm-policy** command takes effect only when the following configurations are complete:

- IGMP snooping has been enabled in the specified BD using the **igmp-snooping enable (BD view)** command.
- SSM mapping has been enabled in the specified BD using the **igmp-snooping ssm-mapping enable** command.
- If IGMPv1 or IGMPv2 packets are sent by user hosts, the IGMP message version is set to IGMPv3 using the **igmp-snooping version** command in the BD.
- The ACL has been created and configured rules for the ACL. By default, the ACL applied to an SSM group policy denies all multicast groups. Therefore, to exclude specific group addresses from the SSM group address range, use a **rule permit source any** rule with **deny** rules in the ACL. For details about ACL configuration commands, see **14.1 ACL Configuration Commands**.

Example

Specify multicast group 225.1.1.123 as an SSM group in BD 123.


```
<HUAWEI> system-view
[HUAWEI] acl number 2000
[HUAWEI-acl-basic-2000] rule permit source 225.1.1.123 0
[HUAWEI-acl-basic-2000] quit
[HUAWEI] igmp-snooping enable
[HUAWEI] igmp-snooping over-vxlan enable
[HUAWEI] bridge-domain 123
[HUAWEI-bd123] igmp-snooping enable
[HUAWEI-bd123] igmp-snooping ssm-mapping enable
[HUAWEI-bd123] igmp-snooping ssm-policy 2000
```

8.11.28 igmp-snooping static-group suppress-dynamic-join

Function

The **igmp-snooping static-group suppress-dynamic-join** command disables a device from forwarding IGMP Report and Leave messages that are received from a BD and contain a static group address to upstream Layer 3 devices configured with the static group address.

The **undo igmp-snooping static-group suppress-dynamic-join** command enables a device to forward IGMP Report and Leave messages that are received from a BD and contain a static group address to upstream Layer 3 devices configured with the static group address.

By default, a device forwards IGMP Report and Leave messages that are received from a BD and contain a static group address to upstream Layer 3 devices configured with the static group address.

Format

igmp-snooping static-group suppress-dynamic-join

undo igmp-snooping static-group suppress-dynamic-join

Parameters

None

Views

BD view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If the upstream Layer 3 multicast device is a non-Huawei device and a static group is configured on its interface connected to the device, users cannot dynamically join or leave the multicast group. You must disable the device from sending Report and Leave messages that contain static group addresses to the Layer 3 multicast device.

This function takes effect only for IGMPv1 and IGMPv2 message and is invalid for IGMPv3 messages.

Prerequisites

IGMP snooping has been enabled for the VXLAN network using the **igmp-snooping over-vxlan enable** command in the system view.

Precautions

If IGMP snooping is disabled in the specified BD, the configuration succeeds but does not take effect until IGMP snooping is enabled in the BD. To enable IGMP snooping in a BD, run the **igmp-snooping enable (BD view)** command.

Example

Disable a device from forwarding IGMP Report and Leave messages that are received from BD 123 and contain a static group address to upstream Layer 3 devices configured with the static group address.

```
<HUAWEI> system-view
[HUAWEI] igmp-snooping enable
[HUAWEI] igmp-snooping over-vxlan enable
[HUAWEI] bridge-domain 123
[HUAWEI-bd123] igmp-snooping enable
[HUAWEI-bd123] igmp-snooping static-group suppress-dynamic-join
```

8.11.29 igmp-snooping static-router-port

Function

The **igmp-snooping static-router-port** command configures an interface as a static router port in specified BDs.

The **undo igmp-snooping static-router-port** command cancels the router port configuration in specified BDs.

By default, an interface is not a static router port.

Format

igmp-snooping static-router-port vlan { *vlan-id1* [**to** *vlan-id2*] } &<1-10>

undo igmp-snooping static-router-port vlan { { *vlan-id1* [**to** *vlan-id2*] } &<1-10> | **all** }

Parameters

Parameter	Description	Value
vlan { *vlan-id1* [**to** *vlan-id2*] } &<1-10>	Specifies VLAN IDs. This parameter specifies in which VLANs the current interface functions as a router port. ● *vlan-id1* specifies the first VLAN ID. ● **to** *vlan-id2* specifies the last VLAN ID. If **to** *vlan-id2* is not specified, the interface functions as a router port only in the VLAN specified by *vlan-id1*.	The value is an integer that ranges from 1 to 4094. The value of vlan-id2 must be greater than the value of vlan-id1. The vlan-id1 and vlan-id2 parameters identify a range of VLANs.
all	Cancels the static router port configuration in all VLANs on the interface.	-

Views

GE interface view, MultiGE interface view, XGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, port group view, Eth-Trunk interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When an interface needs to keep forwarding IGMP Report/Leave messages for a long time, configure the interface as a static router port.

Prerequisites

IGMP snooping has been enabled for the VXLAN network using the **igmp-snooping over-vxlan enable** command in the system view.

Precautions

- This command can be configured only on access-side interfaces of a VXLAN network, but not on tunnel-side interfaces of a VXLAN network.
- The VLAN specified in this command has been created, and the interface on which the command needs to be executed has been added to the VLAN.

- The VLAN specified in this command has been bound to a BD, and IGMP snooping has been enabled in the BD.
- If you run the **igmp-snooping static-router-port** command multiple times, all the configurations take effect.

Example

Configure GE0/0/1 as a static router port.

```
<HUAWEI> system-view
[HUAWEI] igmp-snooping enable
[HUAWEI] igmp-snooping over-vxlan enable
[HUAWEI] bridge-domain 123
[HUAWEI-bd123] l2 binding vlan 100
[HUAWEI-bd123] igmp-snooping enable
[HUAWEI-bd123] quit
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] igmp-snooping static-router-port vlan 100
```

8.11.30 igmp-snooping suppress-time

Function

The **igmp-snooping suppress-time** command sets the IGMP message suppression time in a BD.

The **undo igmp-snooping suppress-time** command restores the default IGMP message suppression time in a BD.

By default, the IGMP message suppression time is 10 seconds.

Format

igmp-snooping suppress-time *suppress-time*

undo igmp-snooping suppress-time

Parameters

Parameter	Description	Value
suppress-time	Specifies the IGMP message suppression time in a BD.	The value is an integer that ranges from 0 to 300, in seconds. The value 0 indicates that IGMP messages are not suppressed.

Views

BD view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To reduce the IGMP messages sent from a Layer 2 device to the upstream Layer 3 device and protect the Layer 3 device from attacks, enable the Layer 2 device to suppress IGMP Report and IGMP Leave messages sent by hosts in a BD. After this function is enabled, the Layer 2 device processes IGMP Report and IGMP Leave messages as follows:

- After receiving an IGMP Report/Leave message and forwarding the message, the Layer 2 device does not forward the same type of messages to the router port within the suppression time.
- If the Layer 2 device receives an IGMP General Query message or Group-Specific message, it does not suppress the first IGMP Report message that responds to the General Query message. In addition, the Layer 2 device resets the suppression timer when it receives the first IGMP Report message.

Prerequisites

IGMP snooping has been enabled for the VXLAN network using the **igmp-snooping over-vxlan enable** command in the system view.

Follow-up Procedure

Run the **igmp-snooping max-response-time** command to set the maximum response time for General Query messages. It is recommended that the suppression time be the same as the maximum response time for IGMP Query messages in a BD.

Precautions

The configuration takes effect only after you run the **igmp-snooping enable (BD view)** command to enable IGMP snooping in the BD.

The configured suppression time is invalid for IGMPv3 messages.

Example

Set the IGMP message suppression time in BD 123 to 15 seconds.

```
<HUAWEI> system-view
[HUAWEI] igmp-snooping enable
[HUAWEI] igmp-snooping over-vxlan enable
[HUAWEI] bridge-domain 123
[HUAWEI-bd123] igmp-snooping enable
[HUAWEI-bd123] igmp-snooping suppress-time 15
```

8.11.31 igmp-snooping version

Function

The **igmp-snooping version** command configures the version of IGMP messages that IGMP snooping can process in a BD.

The **undo igmp-snooping version** command restores the default IGMP message version.

By default, the IGMP snooping version is 2, indicating that IGMP snooping can process IGMPv1 and IGMPv2 messages.

Format

igmp-snooping version *version*

undo igmp-snooping version

Parameters

Parameter	Description	Value
version	Specifies the version of IGMP messages that can be processed in a BD.	The value is an integer ranging from 1 to 3. • 1: indicates that IGMP snooping processes only IGMPv1 messages. • 2: indicates that IGMP snooping processes IGMPv1 and IGMPv2 messages. • 3: indicates that IGMP snooping processes IGMPv1, IGMPv2, and IGMPv3 messages.

Views

BD view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The IGMP protocol maintains group memberships between Layer 3 multicast devices and hosts. IGMP has three versions: v1, v2, and v3. This command specifies the version of IGMP messages that IGMP snooping can process. Generally, configure the same version on the Layer 2 device as that on the upstream Layer 3 multicast device. If IGMP is not enabled on the Layer 3 multicast device, configure the IGMP message version on the Layer 2 device to be later than or equal to the version running on downstream hosts.

When hosts in a BD run different IGMP versions, run the **igmp-snooping version** command to enable the Layer 2 device to process IGMP messages sent from all the hosts.

Prerequisites

IGMP snooping has been enabled for the VXLAN network using the **igmp-snooping over-vxlan enable** command in the system view.

Precautions

If IGMP snooping is disabled in the specified BD, the configuration succeeds but does not take effect until IGMP snooping is enabled in the BD. To enable IGMP snooping in a BD, run the **igmp-snooping enable (BD view)** command.

If the IGMP message version is changed from IGMPv3 to IGMPv2, the system deletes all the dynamic IGMP snooping entries when the aging time expires and processes static IGMP snooping entries as follows:

- Does not delete static entries that have only multicast groups and no multicast sources.
- Deletes the static entries that have both multicast groups and multicast sources. When the IGMP message version is restored to IGMPv3, the system restores these entries.

Example

Set the version of the IGMP messages that can be processed by IGMP snooping to IGMPv1 in BD 123.

```
<HUAWEI> system-view
[HUAWEI] igmp-snooping enable
[HUAWEI] igmp-snooping over-vxlan enable
[HUAWEI] bridge-domain 123
[HUAWEI-bd123] igmp-snooping enable
[HUAWEI-bd123] igmp-snooping version 1
```

8.11.32 l2-multicast static-group

Function

The **l2-multicast static-group** command configures static group memberships on an interface.

The **undo l2-multicast static-group** command deletes static group memberships from an interface.

By default, no static group membership is configured on an interface.

Format

Configure a single static multicast group:

l2-multicast static-group [**source-address** *source-ip-address*] **group-address** *group-ip-address* **vlan** { *vlan-id1* [**to** *vlan-id2*] } &<1-10>

undo l2-multicast static-group [**source-address** *source-ip-address*] **group-address** *group-ip-address* **vlan** { **all** | { *vlan-id1* [**to** *vlan-id2*] } &<1-10> }

Configure a series of static multicast groups:

l2-multicast static-group [**source-address** *source-ip-address*] **group-address** *group-ip-address1* **to** *group-ip-address2* **vlan** *vlan-id*

undo l2-multicast static-group [**source-address** *source-ip-address*] **group-address** *group-ip-address1* **to** *group-ip-address2* **vlan** *vlan-id*

undo l2-multicast static-group [**source-address** *source-ip-address*] **group-address all vlan** { **all** | { *vlan-id1* [**to** *vlan-id2*] } &<1-10> }

Parameters

Parameter	Description	Value
source-address *source-ip-address*	Specifies the IP address of a multicast source.	The value of *source-ip-address* can be any Class A, Class B, or Class C address, in dotted decimal notation.
group-address *group-ip-address*	Specifies the IP address of a multicast group.	The value of *group-ip-address* ranges from 224.0.1.0 to 239.255.255.255 in dotted decimal notation.
vlan { *vlan-id1* [**to** *vlan-id2*] }	Specifies the VLANs that the interface belongs to. *vlan-id1* [**to** *vlan-id2*] specifies a range of VLAN IDs. • *vlan-id1* specifies the first VLAN ID. • **to** *vlan-id2* specifies the last VLAN ID. If **to** *vlan-id2* is not specified, the interface is bound only to the multicast group in the VLAN specified by *vlan-id1*.	The values of *vlan-id1* and *vlan-id2* are integers that range from 1 to 4094. *vlan-id2* must be larger than *vlan-id1*.
all	Deletes all group memberships from the interface. • In **group-address all**, **all** indicates that the interface is removed from all multicast groups. • In **vlan** { **all** | {*vlan-id1* [**to** *vlan-id2*] } &<1-10> }, **all** indicates that the interface is removed from multicast groups in all VLANs.	-

Parameter	Description	Value
group-ip-address1 **to** *group-ip-address2*	Configures multiple static group memberships on the interface. *group-ip-address1* and *group-ip-address2* identify a range of multicast group addresses.	The value ranges from 224.0.1.0 to 239.255.255.255, in dotted decimal notation. The values of *group-ip-address1* and *group-ip-address2* must be in the same network segment (with a 24-bit mask).

Views

GE interface view, MultiGE interface view, XGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, port group view, Eth-Trunk interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In addition to dynamic multicast forwarding entries generated by Layer 2 multicast protocols, you can configure static Layer 2 multicast forwarding entries by binding interfaces to multicast groups. After an interface is statically bound to a multicast group, users connected to this interface can receive multicast data of the multicast group over a long time. The interface then becomes a static member interface.

Configuring static member interfaces has the following advantages:

- Protects the system against attacks from protocol packets.
- Reduces the network delay by directly forwarding multicast packets based on static forwarding entries.
- Prevents unregistered users from receiving multicast flows, improving information security and protecting service providers' interests.

Prerequisites

IGMP snooping has been enabled for the VXLAN network using the **igmp-snooping over-vxlan enable** command in the system view.

Precautions

This command can be configured only on access-side interfaces of a VXLAN network, but not on tunnel-side interfaces of a VXLAN network.

The configuration takes effect only when both the following conditions are met:

- The specified VLANs have been created and the interface has been added to these VLANs.
- The VLAN specified in this command has been bound to a BD, and IGMP snooping has been enabled in the BD using the **igmp-snooping enable (BD view)** command.
- The specified group address is not a reserved group address.

Example

Configure a static multicast group 224.1.1.1 on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] igmp-snooping enable
[HUAWEI] igmp-snooping over-vxlan enable
[HUAWEI] bridge-domain 123
[HUAWEI-bd123] l2 binding vlan 2
[HUAWEI-bd123] igmp-snooping enable
[HUAWEI-bd123] quit
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] port link-type trunk
[HUAWEI-GigabitEthernet0/0/1] port trunk allow-pass vlan 2
[HUAWEI-GigabitEthernet0/0/1] l2-multicast static-group group-address 224.1.1.1 vlan 2
```

Configure static multicast groups 224.1.1.1 to 224.1.1.3 on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] igmp-snooping enable
[HUAWEI] igmp-snooping over-vxlan enable
[HUAWEI] bridge-domain 123
[HUAWEI-bd123] l2 binding vlan 2
[HUAWEI-bd123] igmp-snooping enable
[HUAWEI-bd123] quit
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] port link-type trunk
[HUAWEI-GigabitEthernet0/0/1] port trunk allow-pass vlan 2
[HUAWEI-GigabitEthernet0/0/1] l2-multicast static-group group-address 224.1.1.1 to 224.1.1.3 vlan 2
```

Delete static multicast group 224.1.1.1 from GE0/0/1 in all VLANs.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo l2-multicast static-group group-address 224.1.1.1 vlan all
```

8.11.33 multicast drop-unknown

Function

The **multicast drop-unknown** command configures the switch to drop unknown multicast flows in a BD.

The **undo multicast drop-unknown** command restores the default measure taken for unknown multicast flows.

By default, a switch broadcasts unknown multicast packets in a BD.

Format

multicast drop-unknown

undo multicast drop-unknown

Parameters

None

Views

BD view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Unknown multicast flows are those that do not match any entry in the multicast forwarding table or match multicast forwarding entries with an empty outbound interface list. These flows are not requested by users. By default, a switch broadcasts unknown multicast flows. To reduce bandwidth usage, you can configure the **multicast drop-unknown** command to discard unknown multicast flows.

Configuration Impact

After the **multicast drop-unknown** command is executed, all unknown IPv4 multicast packets in a BD are dropped.

Example

Drop unknown multicast flows in BD 123.

```
<HUAWEI> system-view
[HUAWEI] bridge-domain 123
[HUAWEI-bd123] multicast drop-unknown
```

8.11.34 reset igmp-snooping group

Function

The **reset igmp-snooping group** command deletes dynamic group memberships learned by IGMP snooping.

Format

reset igmp-snooping group bridge-domain { *bd-id* [[**source-address** *source-address*] **group-address** *group-address*] | **all** }

Parameters

Parameter	Description	Value
all	Deletes IGMP dynamic group memberships of all BDs.	-

Parameter	Description	Value
bd-id	Deletes the dynamic group memberships of a specified BD.	The value is an integer that ranges from 1 to 16777215.
source-address *source-address*	Deletes the dynamic group memberships of a specified source address.	The multicast source address is a Class A, Class B, or Class C IP address on a nature network segment. The value is in dotted decimal notation.
group-address *group-address*	Deletes the dynamic group memberships of a specified group address.	The value of *group-address* ranges from 224.0.1.0 to 239.255.255.255 in dotted decimal notation.

Views

User view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When multicast groups on a network change, the switch generates new Layer 2 multicast forwarding entries until the aging time of member ports expire. To enable the switch to generate new multicast forwarding entries immediately, use the **reset igmp-snooping group** command to delete existing group memberships.

Precautions

This command cannot delete static group memberships.

NOTICE

Deleting group memberships in a BD temporarily interrupts multicast forwarding in the BD. The switch generates new forwarding entries only when receiving IGMP Report messages from hosts in the BD. The hosts can then receive multicast data.

Example

Delete dynamic group memberships in BD 123.

```
<HUAWEI> reset igmp-snooping group bridge-domain 123
```


8.11.35 reset igmp-snooping statistics

Function

The **reset igmp-snooping statistics** command clears IGMP snooping statistics.

Format

reset igmp-snooping statistics bridge-domain { *bd-id* | **all** }

Parameters

Parameter	Description	Value
all	Clears IGMP snooping statistics of all BDs.	-
bd-id	Clears IGMP snooping statistics of a specified BD.	The value is an integer that ranges from 1 to 16777215.

Views

User view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To analyze the IGMP snooping statistics collected in a certain period, run this command to clear the previous statistics. After a while, run the **display igmp-snooping statistics** command to view the IGMP snooping statistics.

Precautions

NOTICE

The cleared IGMP snooping statistics cannot be restored.

Example

Clear IGMP snooping statistics of BD 123.

```
<HUAWEI> reset igmp-snooping statistics bridge-domain 123
Warning: If reset statistical information, the information will be unrecoverable, continue?[Y/N]:y
```


8.12 MLD Snooping Configuration Commands

8.12.1 Command Support

Commands provided in this section and all the parameters in the commands are supported by all switch models (except the S5731-L and S5731S-L), unless otherwise specified. For details, see specific commands.

8.12.2 display l2-multicast forwarding-mode

Function

The **display l2-multicast forwarding-mode** command displays the Layer 2 multicast forwarding mode in VLANs.

Format

display l2-multicast forwarding-mode vlan [*vlan-id*]

Parameters

Parameter	Description	Value
vlan [*vlan-id*]	Displays the Layer 2 multicast forwarding mode in a specified VLAN. If *vlan-id* is not specified, the system displays the Layer 2 multicast forwarding mode in all VLANs.	The value is an integer ranging from 1 to 4094.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

After Layer 2 multicast is enabled on the switch, the switch maintains a Layer 2 multicast forwarding table. When receiving a multicast packet, the switch searches the Layer 2 multicast forwarding table for the outbound interface based on the multicast address of the packet. The switch determines the outbound interface based on the IP multicast address or IP multicast MAC address, depending on the configured Layer 2 multicast forwarding mode.

To check which Layer 2 multicast forwarding mode is used, run the **display l2-multicast forwarding-mode** command.

Precautions

You can change the forwarding mode using the **l2-multicast forwarding-mode** command.

Example

Display the Layer 2 multicast forwarding mode in all VLANs.

```
<HUAWEI> display l2-multicast forwarding-mode vlan
VLAN                Forwarding-mode       Router-discard
------------------------------------------------------------------
1                   IP                    disable
2                   IP                    disable
3                   MAC                     disable
```

Table 8-136 Description of the **display l2-multicast forwarding-mode vlan** command output

Item	Description
VLAN	VLAN ID.
Forwarding-mode	Forwarding mode used in a VLAN, which can be: ● MAC address-based forwarding ● IP address-based forwarding This parameter can be configured using the **l2-multicast forwarding-mode** { **ip** | **mac** } command.
Router-discard	Whether the switch is configured not to forward multicast data packets to router ports in a VLAN. ● enable: The switch does not forward multicast data packets to router ports in the VLAN. ● disable: The switch forwards multicast data packets to router ports in the VLAN. This function is configured using the **l2-multicast router-port-discard** command.

8.12.3 display mld-snooping

Function

The **display mld-snooping** command displays the MLD snooping running parameters in a VLAN.

Format

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

Parameters

Parameter	Description	Value
vlan *vlan-id*	Displays the MLD snooping running parameters in a specified VLAN. If this parameter is not specified, the system displays the MLD running parameters in all VLANs with MLD snooping configured.	The value is an integer that ranges from 1 to 4094.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

You can use this command to view the MLD snooping running parameters. If you run this command after configuring MLD snooping parameters, the command displays the configured parameter values.

To view the MLD snooping configuration, run the **display mld-snooping configuration** command.

Precautions

This command can display the MLD snooping configuration in a VLAN only when at least one interface in the VLAN is in Up state and MLD snooping is enabled in the VLAN.

Example

Display the MLD snooping running parameters in VLAN 3.

```
<HUAWEI> display mld-snooping vlan 3
MLD Snooping Vlan Information for VLAN 3
  MLD Snooping is Enabled
  MLD Version is Set to default 1
  MLD Query Interval is Set to default 125s
  MLD Max Response Interval is Set to default 10s
  MLD Robustness is Set to default 2
  MLD Last Member Query Interval is Set to default 1s
```



```
MLD Router Port Aging Interval is Set to 180s or holdtime in hello
MLD Filter Group-Policy is not set
MLD Prompt Leave Disable
MLD Router Alert is Not Required
MLD Send Router Alert Enable
MLD Snooping proxy is disabled
MLD Snooping report-suppress is disabled
MLD Snooping Querier is disabled
```

Table 8-137 Description of the **display mld-snooping vlan 3** command output

Item	Description
MLD Snooping Vlan Information for VLAN 3	The following information displayed is the MLD snooping running parameters in VLAN 3.
MLD Snooping is Enabled	MLD snooping is enabled in the VLAN. By default, MLD snooping is disabled in a VLAN. MLD snooping can be enabled using the **mld-snooping enable** command.
MLD Version is Set to default 1	Version of MLD messages that can be processed in the VLAN. In this example, the default version 1 is displayed. This parameter is configured using the **mld-snooping version** command.
MLD Query Interval is Set to default 125s	Interval at which MLD General Query messages are sent. In this example, the default value (125 seconds) is displayed. This parameter is configured using the **mld-snooping query-interval** command.
MLD Max Response Interval is Set to default 10s	Maximum response time for MLD General Query messages. In this example, the default value (10 seconds) is displayed. This parameter is configured using the **mld-snooping max-response-time** command.
MLD Robustness is Set to default 2	MLD robustness variable. In this example, the default value 2 is displayed. This parameter is configured using the **mld-snooping robust-count** command.
MLD Last Member Query Interval is Set to default 1s	Interval at which MLD Group-Specific Query messages are sent. In this example, the default value (1 second) is displayed. This parameter is configured using the **mld-snooping last-listener-query-interval** command.

Item	Description
MLD Router Port Aging Interval is Set to 180s or holdtime in hello	Aging time of a router port. In this example, the default value (180 seconds or the holdtime value contained in PIM Hello messages) is displayed. This parameter is configured using the **mld-snooping router-aging-time** command.
MLD Filter Group-Policy is not set	Multicast group policy. In this example, the default configuration is displayed. That is, no policy is configured. A multicast group policy is configured using the **mld-snooping group-policy (VLAN view)** command.
MLD Prompt Leave Disable	The fast leave function is disabled for interfaces in the VLAN (default configuration). The fast leave function can be enabled using the **mld-snooping prompt-leave** command.
MLD Router Alert is Not Required	The switch does not require that MLD messages received from the VLAN contain the Router-Alert option in the IP header (default configuration). The switch can be configured to discard MLD messages without the Router-Alert option using the **mld-snooping require-router-alert** command.
MLD Send Router Alert Enable	The switch sends MLD messages with the Router-Alert option to the VLAN (default configuration). The switch can be configured to send MLD messages with the Router-Alert option using the **mld-snooping send-router-alert** command.
MLD Snooping proxy is disabled	MLD snooping proxy is disabled (default configuration). MLD snooping proxy can be enabled using the **mld-snooping proxy** command.
MLD Snooping report-suppress is disabled	MLD snooping report suppression is disabled (default configuration). MLD snooping report suppression can be enabled using the **mld-snooping report-suppress** command.
MLD Snooping Querier is disabled	MLD snooping querier is disabled (default configuration). MLD snooping querier can be enabled using the **mld-snooping querier enable** command.

8.12.4 display mld-snooping configuration

Function

The **display mld-snooping configuration** command displays the MLD snooping configuration.

Format

display mld-snooping [**vlan** *vlan-id*] **configuration**

Parameters

Parameter	Description	Value
vlan *vlan-id*	Displays the MLD snooping configuration in a specified VLAN. If this parameter is not specified, the system displays the MLD snooping configuration in all VLANs.	The value is an integer that ranges from 1 to 4094.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

This command displays only the MLD snooping configuration so that you can check whether the MLD snooping configuration made in the system is proper.

To check all MLD snooping running parameters, run the **display mld-snooping** command.

Precautions

Before running the **display mld-snooping configuration** command, run the **mld-snooping enable** commands to enable IGMP snooping globally and in the VLAN. Otherwise, no information is displayed.

Example

Display the MLD snooping configuration in all VLANs.

```
<HUAWEI> display mld-snooping configuration
 MLD Snooping Configuration for VLAN 20
```



```
    mld-snooping enable
    mld-snooping version 2
MLD Snooping Configuration for VLAN 90
    mld-snooping enable
```

Table 8-138 Description of the **display mld-snooping configuration** command output

Item	Description
MLD Snooping Configuration for VLAN	The following information displayed is the MLD snooping configuration in a specific VLAN.
mld-snooping enable	MLD snooping is enabled in the VLAN. By default, MLD snooping is disabled in a VLAN. MLD snooping can be enabled using the **mld-snooping enable** command.
mld-snooping version 2	MLDv1 and MLDv2 messages can be processed in the VLAN. By default, only MLDv1 messages can be processed in a VLAN. This parameter is configured using the **mld-snooping version** command.

8.12.5 display mld-snooping forwarding-table

Function

The **display mld-snooping forwarding-table** command displays the Layer 2 multicast forwarding table.

Format

display mld-snooping forwarding-table vlan [*vlan-id* [[**source-address** *source-ipv6-address*] **group-address** { *group-ipv6-address* | **router-group** }]]

Parameters

Parameter	Description	Value
vlan [*vlan-id*]	Displays Layer 2 multicast forwarding entries in a specified VLAN. If *vlan-id* is not specified, information about the MLD snooping forwarding table of all VLANs.	The value is an integer that ranges from 1 to 4094.

Parameter	Description	Value
source-address *source-ipv6-address*	Displays the forwarding entries of a specified Layer 2 multicast source.	The address is a 32-digit hexadecimal number, in the format X:X:X:X:X:X:X:X.
group-address *group-ipv6-address*	Displays multicast forwarding entries of a specified Layer 2 multicast group.	The address is a 32-digit hexadecimal number, in the format X:X:X:X:X:X:X:X. An IPv6 multicast address starts with FF.
router-group	Displays Layer 2 multicast forwarding entries of all router ports.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

After completing MLD snooping configuration, you can use the **display mld-snooping forwarding-table** command to view the MLD snooping forwarding table. This command displays statically configured and dynamically learned multicast forwarding entries.

Each entry contains the multicast source, multicast group, list of outbound interfaces, and VLAN ID of multicast data packets. When the MLD snooping version is set to v2 in a VLAN or when the MLD snooping version is set to v2, the **display mld-snooping forwarding-table** command displays (S, G) entries.

Precautions

This command displays Layer 2 multicast forwarding entries in a VLAN only when at least one interface in the VLAN is in Up state.

Example

Display multicast forwarding entries in VLAN 10.

```
<HUAWEI> display mld-snooping forwarding-table vlan 10
VLAN ID : 10, Forwarding Mode : IP
Total Group(s): 2
------------------------------------------------------------------------------
                (Source, Group)    Interface                Out-Vlan
------------------------------------------------------------------------------
```



```
                Router-port    GigabitEthernet0/0/1          10
(*, ff1e:0:0:0:0:0:0:1)    GigabitEthernet0/0/1          10
                               GigabitEthernet0/0/2          10
(*, ff1e:0:0:0:0:0:0:2)    GigabitEthernet0/0/1          10
                               GigabitEthernet0/0/2          10
------------------------------------------------------------------------------
```

Table 8-139 Description of the **display mld-snooping forwarding-table** command output

Item	Description
VLAN ID	VLAN ID of the forwarding entries.
Forwarding Mode	Multicast forwarding mode in the VLAN, which can be: • IP • MAC The multicast forwarding mode is configured using the **l2-multicast forwarding-mode** command.
(Source, Group)	(S, G) entry, specifying the multicast source and multicast group. The Router-port field indicates a router port.
Interface	Outbound interface. The value **Stream** indicates an unknown flow entry.
Out-Vlan	VLAN ID of packets.
Router-port	Router port in the VLAN.
Total Group(s)	Total number of multicast forwarding entries.

8.12.6 display mld-snooping port-info

Function

The **display mld-snooping port-info** command displays information about multicast group member ports.

Format

display mld-snooping port-info [**vlan** *vlan-id* [**group-address** *ipv6-group-address*]] [**verbose**]

Parameters

Parameter	Description	Value
vlan *vlan-id*	Displays multicast group member ports in a specified VLAN. If this parameter is not specified, the system displays multicast group member ports in all VLANs.	The value is an integer that ranges from 1 to 4094.
group-address *ipv6-group-address*	Displays member ports of a specified multicast group. If this parameter is not specified, the system displays member ports of all multicast groups.	The value is an IPv6 multicast address, which is a 32-digit hexadecimal number in X:X:X:X:X:X:X:X format. The first two digits are FF.
verbose	Displays detailed information about multicast group member ports. If this parameter is not specified, the system displays the summary of multicast group member ports.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

MLD snooping creates and maintains a Layer 2 multicast forwarding table by listening on MLD messages exchanged between hosts and a Layer 3 device. The **display mld-snooping port-info** command shows member ports in the Layer 2 multicast forwarding table. According to the command output, you can know which downlink interfaces have multicast users connected, and control multicast services conveniently.

Precautions

This command can display member port information only when MLD snooping is enabled globally and in a VLAN using the **mld-snooping enable** command and

the VLAN is in Up state. If interfaces in the VLAN are dynamic group member ports, the command can display information about these member port information only after they receive MLD Report messages and before their aging time expires.

Example

Display information about multicast group member ports.

```
<HUAWEI> display mld-snooping port-info
--------------------------------------------------------------------------------
                        (Source, Group)  Port                      Flag
                        Flag: S:Static    D:Dynamic
--------------------------------------------------------------------------------
VLAN 10, 1 Entry(s)
                  (*, ff1e:0:0:0:0:0:0:1)  GE0/0/1                 S--
                                             1 port(s) include
--------------------------------------------------------------------------------
```

Table 8-140 Description of the **display mld-snooping port-info** command output

Item	Description
(Source, Group)	An (S, G) entry, specifying the multicast source and multicast group.
Port	Multicast group member port. **include** and **exclude** indicate the multicast source filtering mode.
Flag	Type of a member port, which can be: • **S**: static member port, which is configured using the **mld-snooping static-group** command • **D**: dynamic member port learned through MLD

8.12.7 display mld-snooping router-port

Function

The **display mld-snooping router-port** command displays information about router ports, including static and dynamic router ports.

Format

display mld-snooping router-port [**vlan** *vlan-id*]

Parameters

Parameter	Description	Value
vlan *vlan-id*	Displays the router interfaces in a specified VLAN. If this parameter is not specified, the system displays router ports in all VLANs.	The value is an integer that ranges from 1 to 4094.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

A router port is a switch port connected to an upstream Layer 3 multicast device. Router ports can be statically configured or dynamically created after receiving an MLD Query message or a PIM Hello message. A router port receives multicast data packets from the upstream multicast device and forwards the packets to group member ports.

The **display mld-snooping router-port** command displays information about router ports, including the type, name, age, and aging time of each router port.

Precautions

This command can display router port information only when MLD snooping is enabled globally and in a VLAN using the **mld-snooping enable** command and the VLAN is in Up state.

Example

Display information about router ports.

```
<HUAWEI> display mld-snooping router-port
 Total Number of Router Port on VLAN 2 is 1
  Port Name            UpTime         Expires        Flags
  GE0/0/1              00:00:06       --             STATIC
```


Table 8-141 Description of the **display mld-snooping router-port** command output

Item	Description
Total Number of Router Port on VLAN 2 is 1	Number of router ports in VLAN 2.
Port Name	Type and number of a router port.
UpTime	Age of a router port, that is, time that elapsed since the interface became a router port.
Expires	Aging time of the router port. • The aging time is displayed for a dynamic router port. • For a static router interface, "--" is displayed, indicating that the interface will never age out.
Flags	Type of the router port, which can be: • **STATIC**: static router port, which is configured using the **mld-snooping static-router-port** command • **DYNAMIC**: dynamic router port

8.12.8 display mld-snooping forwarding-table statistics

Function

The **display mld-snooping forwarding-table statistics** command displays statistics about Layer 2 multicast forwarding entries.

Format

display mld-snooping forwarding-table statistics

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

After configuring MLD snooping, you can use this command to view statistics about Layer 2 multicast forwarding entries.

Example

Display statistics about Layer 2 multicast forwarding entries.

```
<HUAWEI> display mld-snooping forwarding-table statistics
------------------------------------------------------------------------------
0 Stream entries are calculated in statistics
1 IP entries are calculated in statistics
0 MAC entries are calculated in statistics
1 VLAN entries are calculated in statistics
------------------------------------------------------------------------------
```

Table 8-142 Description of the **display mld-snooping forwarding-table statistics** command output

Item	Description
Stream entries are calculated in statistics	Number of unknown stream entries in a VLAN.
IP entries are calculated in statistics	Number of entries for IP address-based forwarding in a VLAN.
MAC entries are calculated in statistics	Number of entries for MAC address-based forwarding in a VLAN.
VLAN entries are calculated in statistics	Number of entries for IP address-based and MAC address-based forwarding in a VLAN.

8.12.9 display mld-snooping statistics

Function

The **display mld-snooping statistics** command displays MLD snooping statistics.

Format

display mld-snooping statistics [**vlan** *vlan-id*]

Parameters

Parameter	Description	Value
vlan *vlan-id*	Displays MLD snooping statistics in a specified VLAN. If this parameter is not specified, the system displays MLD snooping statistics in all VLANs.	The value is an integer that ranges from 1 to 4094.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

After completing MLD snooping configuration, you can use the **display mld-snooping statistics** command to view MLD snooping statistics, including the number of MLD messages sent, number of MLD messages received, number of PIM Hello messages received in each VLAN, and number of Layer 2 events that have occurred in all VLANs. Layer 2 events include changes in interface status, changes in VLAN status, changes in VLAN member interfaces (interfaces join or leave VLANs), and MSTP events. When a multicast fault occurs, the MLD snooping statistics help you identify the cause of the fault.

Precautions

This command displays information only when global MLD snooping is enabled using the **mld-snooping enable** command.

Example

Display MLD snooping statistics in all VLANs.

```
<HUAWEI> display mld-snooping statistics
MLD Snooping Events Counter
    Recv VLAN Up Event Times      1027
    Recv VLAN Down Event Times    5
    Recv VLAN Del Event Times     0
    Recv Port Up Event Times      12
    Recv Port Down Event Times    12
    Recv Port Del Event Times     0
    Recv Port Inc Event Times     3069
    Recv Port Exc Event Times     1023
    Recv MSTP Block Event Times   7
    Recv MSTP Forward Event Times 7
    Recv LINK Change Event Times  0
 MLD Snooping Packets Counter
  Statistics for VLAN 10
    Recv V1 Report 16
    Recv V2 Report 8768
    Recv V1 Query  0
    Recv V2 Query  2243
    Recv Done     215
    Recv Pim Hello 0
    Send Query(S=0) 0
    Send Query(S!=0)0
    Send General Query              0
    Send Group-Specific Query       0
    Send Group-Source-Specific Query 0
```

Display MLD snooping in VLAN 20.

```
<HUAWEI> display mld-snooping statistics vlan 20
 MLD Snooping Packets Counter
  Statistics for VLAN 20
```



```
  Recv V1 Report  0
  Recv V2 Report  0
  Recv V1 Query   0
  Recv V2 Query   0
  Recv Done       0
  Recv Pim Hello  0
  Send Query(S=0) 0
  Send Query(S!=0)0
  Send General Query              0
  Send Group-Specific Query       0
  Send Group-Source-Specific Query 0
```

Table 8-143 Description of the **display mld-snooping statistics** command output

Item	Description
MLD Snooping Events Counter	Statistics about MLD snooping events.
Recv VLAN Up Event Times	Number of VLAN Up events.
Recv VLAN Down Event Times	Number of VLAN Down events.
Recv VLAN Del Event Times	Number of VLAN deletion events.
Recv Port Up Event Times	Number of interface Up events.
Recv Port Down Event Times	Number of interface Down events.
Recv Port Del Event Times	Number of interface deletion events.
Recv Port Inc Event Times	Number of times interfaces join VLANs.
Recv Port Exc Event Times	Number of times interfaces leave VLANs.
Recv MSTP Block Event Times	Number of times static groups fail to be created on interfaces that are blocked by MSTP and cannot forward multicast packets.
Recv MSTP Forward Event Times	Number of times static groups are successfully created on interfaces that are in MSTP forwarding state and can forward multicast packets normally.
Recv LINK Change Event Times	Number of link change events.
MLD Snooping Packets Counter	Statistics about MLD snooping packets.
Statistics for VLAN 10	Packet statistics in VLAN 10.
Recv V1 Report	Number of MLDv1 Report messages received.
Recv V2 Report	Number of MLDv2 Report messages received.
Recv V1 Query	Number of MLDv1 Query messages received.
Recv V2 Query	Number of MLDv2 Query messages received.
Recv Done	Number of MLD Leave messages received.
Recv Pim Hello	Number of PIM Hello messages received.

Item	Description
Send Query(S=0)	Number of MLD Query messages sent with the source address of ::.
Send Query(S!=0)	Number of MLD Query messages with sent source addresses other than ::.
Send General Query	Number of General Query messages sent.
Send Group-Specific Query	Number of Group-Specific Query messages sent.
Send Group-Source-Specific Query	Number of Group-Source-Specific Query messages sent.

8.12.10 l2-multicast forwarding-mode

Function

The **l2-multicast forwarding-mode** command configures the forwarding mode of multicast data in a VLAN.

The **undo l2-multicast forwarding-mode** command restores the default forwarding mode of multicast data.

By default, multicast data is forwarded in a VLAN based on IP addresses.

Format

l2-multicast forwarding-mode { **ip** | **mac** }

undo l2-multicast forwarding-mode mac

Parameters

Parameter	Description	Value
ip	Forwards multicast data based on IP addresses.	-
mac	Forwards multicast data based on MAC addresses.	-

Views

VLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After Layer 2 multicast is enabled on a Layer 2 device, the Layer 2 device maintains a Layer 2 multicast forwarding table. When receiving a multicast packet, the Layer 2 device searches the Layer 2 multicast forwarding table for the outbound interface based on the multicast address of the packet. The Layer 2 device determines the outbound interface based on the IP multicast address or IP multicast MAC address, depending on the configured Layer 2 multicast forwarding mode.

Multiple multicast IP addresses may be mapped to one MAC address. If multicast data is forwarded based on MAC addresses, multicast data may be sent to the users who do not require the multicast data. To prevent this problem, use the IP address-based forwarding mode on devices with Layer 3 functions.

Configuration Impact

To set the IGMP snooping version to IGMPv3 or the MLD snooping version to MLDv2, do not change the default forwarding mode using this command.

After the multicast data forwarding mode is set to MAC address-based forwarding in a VLAN using this command, the VLAN cannot be configured as a multicast VLAN.

Precautions

- This command can only be used in VLANs with Layer 2 multicast snooping disabled. After running this command in a VLAN, enable Layer 2 multicast snooping in the VLAN for the configuration to take effect.
  - On an IPv4 network, run the **igmp-snooping enable (VLAN view)** command to enable IGMP snooping in the VLAN.
  - On an IPv6 network, run the **mld-snooping enable** command to enable MLD snooping in the VLAN.

Example

After IGMP snooping is enabled globally, configure the switch to forward multicast data in VLAN 100 based on MAC addresses.

```
<HUAWEI> system-view
[HUAWEI] igmp-snooping enable
[HUAWEI] vlan 100
[HUAWEI-vlan100] l2-multicast forwarding-mode mac
[HUAWEI-vlan100] igmp-snooping enable
```

After MLD snooping is enabled globally, configure the switch to forward multicast data in VLAN 100 based on MAC addresses.

```
<HUAWEI> system-view
[HUAWEI] mld-snooping enable
[HUAWEI] vlan 100
[HUAWEI-vlan100] l2-multicast forwarding-mode mac
[HUAWEI-vlan100] mld-snooping enable
```


8.12.11 l2-multicast router-port-discard

Function

The **l2-multicast router-port-discard** command disables the switch from sending multicast data to routed ports in a VLAN.

The **undo l2-multicast router-port-discard** command restores the default configuration.

By default, multicast data can be forwarded to routed ports in a VLAN.

Format

l2-multicast router-port-discard

undo l2-multicast router-port-discard

Parameters

None

Views

VLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In some scenarios, multicast data does not need to be forwarded to routed ports in a VLAN. For example, when all interfaces on a switch are configured as static router ports in a VLAN, you can use this command to conserve bandwidth by preventing multicast data from being sent to these interfaces.

Precautions

This command can only be used in VLANs with Layer 2 multicast snooping disabled. After running this command in a VLAN, enable Layer 2 multicast snooping in the VLAN for the configuration to take effect.

- On an IPv4 network, run the **igmp-snooping enable (VLAN view)** command to enable IGMP snooping in the VLAN.
- On an IPv6 network, run the **mld-snooping enable** command to enable MLD snooping in the VLAN.

Example

Disable the switch from forwarding multicast data to routed ports in VLAN 10 on an IPv4 network.


```
<HUAWEI> system-view
[HUAWEI] igmp-snooping enable
[HUAWEI] vlan 10
[HUAWEI-vlan10] l2-multicast router-port-discard
[HUAWEI-vlan10] igmp-snooping enable
```

Disable the switch from forwarding multicast data to routed ports in VLAN 10 on an IPv6 network.

```
<HUAWEI> system-view
[HUAWEI] mld-snooping enable
[HUAWEI] vlan 10
[HUAWEI-vlan10] l2-multicast router-port-discard
[HUAWEI-vlan10] mld-snooping enable
```

8.12.12 mld-snooping enable

Function

The **mld-snooping enable** command enables MLD snooping globally or in a VLAN.

The **undo mld-snooping enable** command disables MLD snooping globally or in a VLAN.

By default, MLD snooping is disabled.

Format

System view

mld-snooping enable [**vlan** { *vlan-id1* [**to** *vlan-id2*] } &<1-10>]

undo mld-snooping enable [**vlan** { **all** | { *vlan-id1* [**to** *vlan-id2*] } &<1-10> }]

VLAN view

mld-snooping enable

undo mld-snooping enable

Parameters

Parameter	Description	Value
vlan *vlan-id1* [**to** *vlan-id2*]	Disables MLD snooping on the specified VLANs. *vlan-id1* and *vlan-id2* identify a range of VLANs. If VLAN IDs are specified, MLD snooping is enabled in the specified VLANs. If no VLAN ID is specified, MLD snooping is enabled globally.	The values of *vlan-id1* and *vlan-id2* are integers that range from 1 to 4094. *vlan-id2* must be larger than *vlan-id1*.

Parameter	Description	Value
all	Disables MLD snooping on all VLANs.	-

Views

System view, VLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

MLD snooping runs on a Layer 2 device between a Layer 3 multicast device and hosts, and listens on multicast protocol packets exchanged between the Layer 3 device and hosts to maintain a Layer 2 multicast forwarding table. The Layer 2 device manages and controls Layer 2 multicast forwarding based on this forwarding table.

Before configuring MLD snooping, enable global MLD snooping using the **mld-snooping enable** command in the system view. Other MLD snooping configuration commands can be used only after global MLD snooping is enabled.

You can enable MLD snooping in multiple VLANs by using the **mld-snooping enable** command in the system view.

Precautions

After MLD snooping is enabled in a VLAN, IPv6 Layer 3 multicast cannot be configured on the corresponding VLANIF interface. To use the two functions simultaneously, configure IPv6 Layer 3 multicast on the VLANIF interface before enabling MLD snooping in the VLAN.

After you run the **undo mld-snooping enable** command to disable global MLD snooping, all MLD snooping configurations on the switch are deleted. After you run the **mld-snooping enable** command to enable global MLD snooping again, the switch uses the default MLD snooping configuration.

Multicast functions (Layer 2 and Layer 3 multicast) and the flow control function (configured using the **flow-control** command) are mutually exclusive on the following models: S2730S-S, S5735-L-I, S5735-L1, S300, S5735-L, S5735S-L1, S5735S-L, S5735S-L-M, S500, S5735-S, S5735S-S, S5735-S-I

Example

Enable global MLD snooping.

```
<HUAWEI> system-view
[HUAWEI] mld-snooping enable
```

Enable MLD snooping in multiple VLANs in the system view.


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

Enable MLD snooping in VLAN 10.

```
<HUAWEI> system-view
[HUAWEI] vlan 10
[HUAWEI-vlan10] mld-snooping enable
```

8.12.13 mld-snooping group-policy (interface view)

Function

The **mld-snooping group-policy** command configures an IPv6 multicast group policy on an interface.

The **undo mld-snooping group-policy** command deletes an IPv6 multicast group policy from an interface.

By default, no IPv6 multicast group policy is available on an interface, and hosts connected to the interface can join any IPv6 multicast group.

Format

mld-snooping group-policy *acl6-number* **vlan** *vlan-id* [**version** *mld-version*]

undo mld-snooping group-policy [*acl6-number*] **vlan** *vlan-id*

Parameters

Parameter	Description	Value
acl6-number	Specifies the number of an IPv6 ACL that defines a range of multicast groups.	The number of a basic ACL is an integer that ranges from 2000 to 2999. The number of an advanced ACL ranges from 3000 to 3999.
vlan *vlan-id*	Applies the IPv6 multicast group policy to a specified VLAN on an interface.	The value is an integer that ranges from 1 to 4094.
version *mld-version*	Specifies an MLD version. The multicast group policy is applied only to the MLD messages of this version. If this parameter is not specified, the multicast group policy applies to all MLD messages.	The value is 1 or 2. • 1: MLDv1 • 2: MLDv2

Views

Ethernet interface view, GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, port group view, Eth-Trunk interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

An IPv6 multicast group policy controls the multicast programs that users can order on a Layer 2 device with MLD snooping enabled. When a user orders a multicast program, the user host sends a Report message, requesting to join the multicast group. When the Layer 2 device receives the message, it checks whether the multicast group matches the multicast group policy applied to the interface. If the Report messages match the filter rule, the Layer 2 device allows the hosts in the VLAN to join the group and forwards the Report messages. If the Report messages do not match the filter rule, the Layer 2 device prevents the hosts from joining the group and drops the Report messages.

Prerequisites

MLD snooping has been enabled globally using the **mld-snooping enable** command.

Precautions

The configured multicast group policy takes effect only when all the following conditions are met:

- The interface has been added to the specified VLAN.
- MLD snooping is enabled in the VLAN using the **mld-snooping enable** command.
- The ACL specified in the command has been created and had filtering rules configured.
- Run the **acl** command to configure the ACL.
  - In the basic ACL view, set **source** in the **rule** command to the range of multicast groups that the interface can join.
  - In the advanced ACL view, set **source** in the **rule** command to the source address that is allowed to send multicast data to the specified multicast groups, and set **destination** to the range of multicast groups that the interface can join.

  After the **mld-snooping group-policy (interface view)** command is executed on the interface:
  - The interface filters the received Report messages based on the ACL and maintains memberships only for the multicast groups permitted by the ACL.
  - The interface discards the Report messages that are denied by the ACL. If the entries of the multicast groups denied by the ACL exist on the switch,

the switch deletes these entries when the aging time of the entries expires.

– If the IGMP version is not specified, the specified ACL applies to IGMPv1, IGMPv2, and IGMPv3 hosts.

An IPv6 multicast group policy can also be configured in the VLAN view (using the **mld-snooping group-policy (VLAN view)** command) to control the multicast groups that users in the VLAN can join. An IPv6 multicast group policy configured in the interface view controls the multicast groups that users in one or more VLANs on the interface can join. If you configure multicast group policies for the same VLAN in the interface view and VLAN view, the system first uses the policy configured in the interface view and then the policy configured in the VLAN view to determine the groups that user hosts can join.

Example

Prevent hosts in VLAN 10 on GE0/0/1 from joining IPv6 multicast group ff1c::3/32.

```
<HUAWEI> system-view
[HUAWEI] acl ipv6 number 2000
[HUAWEI-acl6-basic-2000] rule deny source ff1c::3/32
[HUAWEI-acl6-basic-2000] quit
[HUAWEI] mld-snooping enable
[HUAWEI] vlan 10
[HUAWEI-vlan10] mld-snooping enable
[HUAWEI-vlan10] quit
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] port link-type trunk
[HUAWEI-GigabitEthernet0/0/1] port trunk allow-pass vlan 10
[HUAWEI-GigabitEthernet0/0/1] mld-snooping group-policy 2000 vlan 10
```

Allow hosts in VLAN 10 connected to GE0/0/1 to join IPv6 multicast group ff1c::3/32.

```
<HUAWEI> system-view
[HUAWEI] acl ipv6 number 2000
[HUAWEI-acl6-basic-2000] rule permit source ff1c::3/32
[HUAWEI-acl6-basic-2000] quit
[HUAWEI] mld-snooping enable
[HUAWEI] vlan 10
[HUAWEI-vlan10] mld-snooping enable
[HUAWEI-vlan10] quit
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] port link-type trunk
[HUAWEI-GigabitEthernet0/0/1] port trunk allow-pass vlan 10
[HUAWEI-GigabitEthernet0/0/1] mld-snooping group-policy 2000 vlan 10
```

8.12.14 mld-snooping group-policy (VLAN view)

Function

The **mld-snooping group-policy** command configures an IPv6 multicast group policy in a VLAN.

The **undo mld-snooping group-policy** command deletes an IPv6 multicast group policy from a VLAN.

By default, no IPv6 multicast group policy is available in a VLAN, and hosts in the VLAN can join any IPv6 multicast group.

Format

mld-snooping group-policy *acl6-number* [**version** *mld-version*]

undo mld-snooping group-policy

Parameters

Parameter	Description	Value
acl6-number	Specifies the number of an IPv6 ACL that defines a range of multicast groups.	The number of a basic ACL is an integer that ranges from 2000 to 2999. The number of an advanced ACL ranges from 3000 to 3999.
mld-version	Applies the multicast group policy only to the MLD messages of the specified version. If this parameter is not specified, the multicast group policy applies to all MLD messages.	The value is 1 or 2. • 1: MLDv1 • 2: MLDv2

Views

VLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

An IPv6 multicast group policy controls the multicast programs that users can order on a Layer 2 device with MLD snooping enabled. When a user orders a multicast program, the user host sends a Report message, requesting to join the multicast group. When the Layer 2 device receives the message, it checks whether the multicast group matches the multicast group policy applied to the VLAN. If the Report messages match the filter rule, the Layer 2 device allows the hosts in the VLAN to join the group and forwards the Report messages. If the Report messages do not match the filter rule, the Layer 2 device prevents the hosts from joining the group and drops the Report messages.

Prerequisites

MLD snooping has been enabled globally using the **mld-snooping enable** command.

Precautions

The configured multicast group policy takes effect only when both the following conditions are met:

- MLD snooping is enabled in the VLAN using the **mld-snooping enable** command.
- Run the **acl** command to configure the ACL.
  - In the basic ACL view, set **source** in the **rule** command to the range of multicast groups that the VLAN can join.
  - In the advanced ACL view, set **source** in the **rule** command to the source address that is allowed to send multicast data to the specified multicast groups, and set **destination** to the range of multicast groups that the VLAN can join.

  After the **mld-snooping group-policy (VLAN view)** command is executed on the interface:
  - The VLAN filters the received Report messages based on the ACL and maintains memberships only for the multicast groups permitted by the ACL.
  - The VLAN discards the Report messages that are denied by the ACL. If the entries of the multicast groups denied by the ACL exist on the switch, the switch deletes these entries when the aging time of the entries expires.
  - If the IGMP version is not specified, the specified ACL applies to IGMPv1, IGMPv2, and IGMPv3 hosts.

An IPv6 multicast group policy can also be configured in the interface view using the **mld-snooping group-policy (interface view)** command to control the multicast groups that users in one or more VLANs on the interface can join. An IPv6 multicast group policy configured in the interface view controls the multicast groups that users in one or more VLANs on the interface can join. If you configure multicast group policies for the same VLAN in the interface view and VLAN view, the system first uses the policy configured in the interface view and then the policy configured in the VLAN view to determine the groups that user hosts can join.

Example

Prevent hosts in VLAN 4 from joining IPv6 multicast group ff1e::1/32.

```
<HUAWEI> system-view
[HUAWEI] acl ipv6 number 2001
[HUAWEI-acl6-basic-2001] rule deny source ff1e::1/32
[HUAWEI-acl6-basic-2001] quit
[HUAWEI] mld-snooping enable
[HUAWEI] vlan 4
[HUAWEI-vlan4] mld-snooping enable
[HUAWEI-vlan4] mld-snooping group-policy 2001
```

Allow hosts in VLAN 4 to join IPv6 multicast group ff1e::1/32.

```
<HUAWEI> system-view
[HUAWEI] acl ipv6 number 2001
[HUAWEI-acl6-basic-2001] rule permit source ff1e::1/32
[HUAWEI-acl6-basic-2001] quit
[HUAWEI] mld-snooping enable
[HUAWEI] vlan 4
[HUAWEI-vlan4] mld-snooping enable
[HUAWEI-vlan4] mld-snooping group-policy 2001
```


8.12.15 mld-snooping last-listener-query-interval

Function

The **mld-snooping last-listener-query-interval** command sets the last listener query interval, that is, the interval at which Multicast-Address-Specific Query messages are sent in MLD snooping.

The **undo mld-snooping last-listener-query-interval** command restores the default interval.

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

Format

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

undo mld-snooping last-listener-query-interval

Parameters

Parameter	Description	Value
query-interval	Specifies interval at which Multicast-Address-Specific Query messages are sent.	The value ranges from 1 to 5, in seconds.

Views

VLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

By configuring the last listener query interval, you can:

- Adjust the interval at which the querier sends Multicast-Address-Specific Query messages.

  When MLD snooping querier is enabled, you can use the **mld-snooping last-listener-query-interval** command to set the interval at which the querier sends Multicast-Address-Specific Query messages.
- Change the aging time of member ports.

  When a Layer 2 device receives an MLD Done message from a host, it starts an aging timer for the corresponding member port. The aging time is calculated using the following formula: Aging time = Last listener query

interval x Last listener query count. This command sets the last listener query interval in the formula. The last listener query count is set by the **mld-snooping robust-count** command.

If the querier receives Report messages from other hosts within the aging time, it continues to maintain the memberships of the multicast group. If the querier does not receive any Report messages within the aging time, it stops maintaining memberships of the multicast group.

Prerequisites

MLD snooping has been enabled globally using the **mld-snooping enable** command.

Precautions

The querier sets the maximum response time field in the Multicast-Address-Specific Query messages to the configured last listener query interval. Therefore, the maximum response time for Multicast-Address-Specific Query messages is the same as the interval at which Multicast-Address-Specific Query messages are sent.

The configuration takes effect only when both the following conditions are met:

- MLD snooping is enabled in the VLAN using the **mld-snooping enable** command.
- The local device is enabled to send Query messages using the **mld-snooping querier enable** or **mld-snooping proxy** command.

Example

Set the last listener query interval to 2 seconds in VLAN 4.

```
<HUAWEI> system-view
[HUAWEI] mld-snooping enable
[HUAWEI] vlan 4
[HUAWEI-vlan4] mld-snooping enable
[HUAWEI-vlan4] mld-snooping last-listener-query-interval 2
```

8.12.16 mld-snooping learning

Function

The **mld-snooping learning** command enables learning of multicast group memberships on an interface.

The **undo mld-snooping learning** command disables learning of multicast group memberships on an interface.

By default, learning of multicast group memberships is enabled on an interface.

Format

mld-snooping learning vlan { { *vlan-id1* [**to** *vlan-id2*] } &<1-10> | **all** }

undo mld-snooping learning vlan { { *vlan-id1* [**to** *vlan-id2*] } &<1-10> | **all** }

Parameters

Parameter	Description	Value
vlan { *vlan-id1* [**to** *vlan-id2*] }	Enables learning of multicast group memberships in specified VLANs. The interface must have been added to the specified VLAN. *vlan-id1* [**to** *vlan-id2*] specifies the range of VLAN IDs. ● *vlan-id1*: specifies the first VLAN ID. ● *vlan-id2*: specifies the last VLAN ID. If **to** *vlan-id2* is not specified, learning of multicast group memberships is enabled only in the VLAN specified by *vlan-id1*.	The values of *vlan-id1* and *vlan-id2* are integers that range from 1 to 4094. The value of *vlan-id2* must be greater than the value of *vlan-id1*. The *vlan-id1* and *vlan-id2* parameters identify a range of VLANs.
all	Enables learning of multicast group memberships in all VLANs that an interface has joined.	-

Views

Ethernet interface view, GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, port group view, Eth-Trunk interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A group member interface is a user-side interface that connects to multicast group members. Group memberships can be learned dynamically or configured statically. After MLD snooping is enabled in a VLAN, all interfaces in the VLAN are enabled to learn forwarding entries from multicast packets. An interface is identified as a dynamic group member interface when it receives an MLD Report message.

Prerequisites

MLD snooping has been enabled globally using the **mld-snooping enable** command.

Precautions

The configuration takes effect only when all the following conditions are met:

- MLD snooping is enabled in the VLAN using the **mld-snooping enable** command.
- The interface belongs to the specified VLANs.

An interface can be statically bound to a multicast group using the **mld-snooping static-group** command. Then you can run the **undo mld-snooping learning** command on the interface to disable learning of group memberships. This reduces the system resources used for protocol packet exchange.

Example

Disable learning of group memberships in VLAN 3 and VLAN 4 on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] mld-snooping enable
[HUAWEI] vlan 3
[HUAWEI-vlan3] mld-snooping enable
[HUAWEI-vlan3] quit
[HUAWEI] vlan 4
[HUAWEI-vlan4] mld-snooping enable
[HUAWEI-vlan4] quit
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] port link-type trunk
[HUAWEI-GigabitEthernet0/0/1] port trunk allow-pass vlan 3 to 4
[HUAWEI-GigabitEthernet0/0/1] undo mld-snooping learning vlan 3 to 4
```

8.12.17 mld-snooping max-response-time

Function

The **mld-snooping max-response-time** command sets the maximum response time for MLD General Query messages in a VLAN.

The **undo mld-snooping max-response-time** command restores the maximum response time for MLD General Query messages in a VLAN to the default value.

By default, the maximum response time for MLD Listener Query messages is 10 seconds.

Format

mld-snooping max-response-time *max-response-time*

undo mld-snooping max-response-time

Parameters

Parameter	Description	Value
max-response-time	Specifies the maximum response time for General Query messages.	The value is an integer that ranges from 1 to 25, in seconds. The default value is 10.

Views

VLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Setting MLD snooping parameters helps improve the multicast forwarding performance on the switch. By setting the maximum response time for MLD General messages, you can:

- Control the deadline for a host to send a Report message. When hosts are required to respond to Query messages quickly, set a short maximum response time. To avoid congestion caused by a large number of Report messages sent by hosts, set a long maximum response time.
- Adjust the aging time of member ports. When the switch receives a Report message from a host, it starts the aging timer for the corresponding member port. The aging time is calculated using the following formula: Aging time = General query count x General query interval + Maximum response time for General Query messages. This command sets the maximum response time in the formula. The number of times General Query messages are sent is set by the **mld-snooping robust-count** command, and the general query interval is set by the **mld-snooping query-interval** command.

The switch sets the maximum response time field in General Query messages to the value configured by the **mld-snooping max-response-time** command.

Prerequisites

MLD snooping has been enabled globally using the **mld-snooping enable** command.

Follow-up Procedure

Perform the following operations to improve multicast performance:

- Run the **mld-snooping query-interval** command to set the interval at which General Query messages are sent.
- Run the **mld-snooping last-listener-query-interval** command to set the interval at which Multicast-Address-Specific Query messages are sent.

Precautions

To make the configured maximum response time effective in a VLAN, run the **mld-snooping enable** command to enable MLD snooping in the VLAN.

The interval at which General Query messages are sent must be longer than the maximum response time for General Query messages. Otherwise, the switch will delete multicast memberships that should not be deleted.

Example

Set the maximum response time for General Query messages in VLAN 3 to 20 seconds.

```
<HUAWEI> system-view
[HUAWEI] mld-snooping enable
[HUAWEI] vlan 3
[HUAWEI-vlan3] mld-snooping enable
[HUAWEI-vlan3] mld-snooping max-response-time 20
```

8.12.18 mld-snooping prompt-leave

Function

The **mld-snooping prompt-leave** command enables the fast leave function in a VLAN so that member ports in the VLAN can fast leave multicast groups.

The **undo mld-snooping prompt-leave** command disables the fast leave function in a VLAN.

By default, the fast leave function is disabled in a VLAN.

Format

mld-snooping prompt-leave [**group-policy** *acl6-number*]

undo mld-snooping prompt-leave

Parameters

Parameter	Description	Value
group-policy *acl6-number*	Allows member ports to fast leave the multicast groups matching an ACL6. *acl6-number* specifies the number of an ACL6. A basic or advanced ACL6 can be used.	The value is an integer that ranges from 2000 to 3999.

Views

VLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The fast leave function enables the switch to delete the multicast forwarding entry of a multicast group from an interface immediately after the interface receives a Done message for the group. This function saves bandwidth and system resources because the switch does not need to wait until the aging timer of the interface expires.

Prerequisites

MLD snooping has been enabled globally using the **mld-snooping enable** command.

Precautions

When an interface has more than one receiver connected, enabling the fast leave function interrupts multicast traffic of the other receivers in the multicast group. It is recommended that you enable this function only on interfaces with one receiver.

The configuration takes effect only when both the following conditions are met:

- MLD snooping is enabled in the VLAN using the **mld-snooping enable** command.
- If you do not specify **group-policy** when configuring the fast leave function, this function takes effect for all groups. To specify a group policy in the command, create an ACL and configure rules for the ACL before running the command. For details about ACL configuration commands, see **14.1 ACL Configuration Commands** in "Security Commands."

Example

Allow member ports in VLAN 2 to fast leave all multicast groups.

```
<HUAWEI> system-view
[HUAWEI] mld-snooping enable
[HUAWEI] vlan 2
[HUAWEI-vlan2] mld-snooping enable
[HUAWEI-vlan2] mld-snooping prompt-leave
```

Allow member ports in VLAN 3 to fast leave multicast group 0xff13::0001:0002.

```
<HUAWEI> system-view
[HUAWEI] mld-snooping enable
[HUAWEI] acl ipv6 number 2000
[HUAWEI-acl6-basic-2000] rule permit source ff13::0001:0002 128
[HUAWEI-acl6-basic-2000] quit
[HUAWEI] vlan 3
[HUAWEI-vlan3] mld-snooping enable
[HUAWEI-vlan3] mld-snooping prompt-leave group-policy 2000
```

Prevent member ports in VLAN 3 from fast leaving multicast group 0xff13::0001:0002.

```
<HUAWEI> system-view
[HUAWEI] mld-snooping enable
[HUAWEI] acl ipv6 number 2000
```



```
[HUAWEI-acl6-basic-2000] rule deny source ff13::0001:0002 128
[HUAWEI-acl6-basic-2000] quit
[HUAWEI] vlan 3
[HUAWEI-vlan3] mld-snooping enable
[HUAWEI-vlan3] mld-snooping prompt-leave group-policy 2000
```

8.12.19 mld-snooping proxy

Function

The **mld-snooping proxy** command enables Multicast Listener Discovery (MLD) snooping proxy in a VLAN.

The **undo mld-snooping proxy** command disables MLD snooping proxy in a VLAN.

By default, MLD snooping proxy is disabled in a VLAN.

Format

mld-snooping proxy

undo mld-snooping proxy

Parameters

None

Views

VLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After MLD snooping is enabled, the switch forwards Report messages to router ports and broadcasts Query messages in a VLAN. The MLD snooping proxy function allows the switch to send Query messages in place of the upstream Layer 3 device and send Report/Done messages in place of downstream hosts. This saves the bandwidth on the link between the Layer 3 device and switch. The switch sends a Report/Done message to the upstream Layer 3 device only in the following situations:

- When the first member joins a multicast group or a host sends a Report message in response to an MLD Query message, the Layer 2 device forwards a Report message to the upstream device. The upstream device can create or maintain the matching forwarding entry based on the Report message.
- When the last member of a multicast group leaves the group, the Layer 2 device forwards a Done message to the upstream device. The upstream device then deletes the matching forwarding entry.

An upstream Layer 3 device does not send Query messages as a querier when MLD is not enabled for some reasons, for example, the Layer 3 device has only static multicast groups. In this case, the switch cannot create or maintain group memberships even though MLD snooping is enabled. The MLD snooping proxy function enables the switch to send Query messages to downstream hosts. For the hosts, the switch is a querier.

Prerequisites

MLD snooping has been enabled globally using the **mld-snooping enable** command.

Configuration Impact

If MLD is enabled on the upstream Layer 3 device, enabling the MLD snooping proxy function on the switch may affect the querier election result. This is because the General Query messages sent by the switch may have a smaller source IP address than the General Query messages sent by the Layer 3 device. Therefore, MLD snooping proxy is not recommended on an MLD-capable multicast network.

Precautions

- The configuration takes effect only after you run the **mld-snooping enable** command to enable MLD snooping in the VLAN.
- MLD snooping proxy cannot be enabled in a VLAN if the corresponding VLANIF interface has IPv6 Layer 3 multicast function (such as MLD and IPv6 PIM) enabled.
- After MLD snooping proxy is enabled in a VLAN, MLD snooping querier and MLD message suppression cannot be enabled in the VLAN.
- If multicast VLAN replication is configured on the switch, the MLD snooping proxy function cannot be enabled in user VLANs.

Example

Enable MLD snooping proxy in VLAN 100.

```
<HUAWEI> system-view
[HUAWEI] mld-snooping enable
[HUAWEI] vlan 100
[HUAWEI-vlan100] mld-snooping enable
[HUAWEI-vlan100] mld-snooping proxy
```

8.12.20 mld-snooping querier enable

Function

The **mld-snooping querier enable** command enables the MLD snooping querier in a VLAN.

The **undo mld-snooping querier enable** command disables the MLD snooping querier in a VLAN.

By default, the MLD snooping querier is disabled in a VLAN.

Format

mld-snooping querier enable

undo mld-snooping querier enable

Parameters

None.

Views

VLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On an MLD-capable network, a Layer 3 multicast device functions as the querier to send MLD Query messages and maintain group memberships on the local network segment. If the Layer 3 multicast device does not run MLD or it uses only static multicast forwarding entries, it cannot function as a querier. You can enable MLD snooping querier on the downstream Layer 2 device so that the device can act as a querier to send MLD Query messages.

On a Layer 2 network that has no Layer 3 devices, multicast sources are connected to Layer 2 devices. MLD snooping querier needs to be enabled on the Layer 2 devices so that they can maintain multicast group memberships.

Prerequisites

MLD snooping has been enabled globally using the **mld-snooping enable** command.

Follow-up Procedure

Perform the following operations as required on your network:

- Set the interval at which the MLD snooping querier sends General Query messages using the **mld-snooping query-interval** command.
- Set the interval at which the MLD snooping querier sends Multicast-Address-Specific Query messages using the **mld-snooping last-listener-query-interval** command.
- Set the query count using the **mld-snooping robust-count** command.

Configuration Impact

The MLD snooping querier does not participate in MLD querier election. However, the MLD snooping querier on an MLD-capable multicast network may affect the election result, because the Query messages sent by the MLD snooping querier may have a smaller source IP address than the Query messages sent by other devices. Therefore, the MLD snooping querier function is not recommended on an MLD-enabled multicast network.

Precautions

- The configuration takes effect only after you run the **mld-snooping_enable** command to enable MLD snooping in the VLAN.
- The MLD snooping querier function cannot be enabled in a VLAN if the corresponding VLANIF interface has IPv6 Layer 3 multicast function (such as MLD and IPv6 PIM) enabled.
- The MLD snooping querier function and MLD snooping proxy cannot be enabled in the same VLAN.
- If multicast VLAN replication is configured, the MLD snooping querier function cannot be enabled in user VLANs.

Example

Enable the MLD snooping querier in VLAN 3.

```
<HUAWEI> system-view
[HUAWEI] mld-snooping enable
[HUAWEI] vlan 3
[HUAWEI-vlan3] mld-snooping enable
[HUAWEI-vlan3] mld-snooping querier enable
```

8.12.21 mld-snooping query-interval

Function

The **mld-snooping query-interval** command sets the general query interval in a VLAN, that is, the interval at which MLD General Query messages are sent in the VLAN.

The **undo mld-snooping query-interval** command restores the default general query interval in a VLAN.

By default, MLD General Query messages are sent at an interval of 125 seconds.

Format

mld-snooping query-interval *query-interval*

undo mld-snooping query-interval

Parameters

Parameter	Description	Value
query-interval	Specifies the interval at which General Query messages are sent.	The value is an integer that ranges from 10 to 65535, in seconds.

Views

VLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

By setting the MLD general query interval, you can:

- Specify the interval at which the querier sends MLD General Query messages.

  When the querier function is enabled in a VLAN, you can use this command to set the general query interval. Then the querier sends General Query messages at the configured interval to maintain group memberships. The querier is more sensitive when it sends General Query messages at a smaller interval, but more bandwidth and resources are consumed.
- Change the aging time of member ports.

  When receiving an MLD Report message from a host, the switch starts the aging timer for the corresponding member port. The aging time is calculated using the following formula: Aging time = General query count x General query interval + Maximum response time for General Query messages. The **mld-snooping query-interval** command sets the general query interval. The general query count is set by the **mld-snooping robust-count** command, and the maximum response time for General Query messages is set by the **mld-snooping max-response-time** command.

NOTE

The default general query interval defined in RFC documents is 125 seconds, but some vendors define their own default general query intervals. It is recommended that all devices on a multicast network use the same general query intervals (including MLD and MLD snooping general query intervals). On Huawei fixed switches, the default values of the MLD general query interval and MLD snooping general query interval are both 125 seconds.

Prerequisites

MLD snooping has been enabled globally using the **mld-snooping enable** command.

Precautions

The configuration takes effect only after you run the **mld-snooping_enable** command to enable MLD snooping in the VLAN.

Use this command only when the switch can send MLD Query message. The switch can send MLD Query messages only when MLD snooping proxy is enabled using the **mld-snooping proxy** command, or MLD snooping querier is enabled using the **mld-snooping querier enable** command.

The interval at which General Query messages are sent must be longer than the maximum response time for General Query messages. Otherwise, the switch will delete multicast memberships that should not be deleted.

Example

Set the general MLD query interval in VLAN 3 to 100 seconds.


```
<HUAWEI> system-view
[HUAWEI] mld-snooping enable
[HUAWEI] vlan 3
[HUAWEI-vlan3] mld-snooping enable
[HUAWEI-vlan3] mld-snooping query-interval 100
```

8.12.22 mld-snooping report-suppress

Function

The **mld-snooping report-suppress** command enables suppression of MLD Report and Done messages in a VLAN.

The **undo mld-snooping report-suppress** command disables suppression of MLD Report and Done messages in a VLAN.

By default, MLD Report and Done message suppression is disabled in a VLAN.

Format

mld-snooping report-suppress

undo mld-snooping report-suppress

Parameters

None

Views

VLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When a Layer 2 device receives an MLD Membership Report message (Report or Done message) from a group member, the Layer 2 device forwards the message to the directly connected Layer 3 device. A group member host sends a Membership Report message in the following situations:

- When joining a multicast group, a host sends a Report message. When a multicast group has multiple members in a VLAN, the Layer 3 device receives duplicate Report messages from the member hosts.
- When receiving an MLD General Query message, a host sends a Report message. Hosts use a timer to suppress duplicate Report messages on the same network segment. However, if the timer values on hosts are the same, the Layer 3 device can still receive duplicate Report messages.
- When leaving a multicast group, a host sends a Done message. When a multicast group has multiple members in a VLAN, the Layer 3 device receives duplicate Done messages from the member hosts.

When MLD Report suppression is configured on the Layer 2 device, the Layer 2 device sends only one copy of MLD Report message when members join or leave a group. When the first member joins a multicast group or a host sends a Report message in response to a Query message, the Layer 2 device forwards a Report message to the upstream device. The upstream device can create or maintain the matching forwarding entry based on the Report message. When the last member of a multicast group leaves the group, the Layer 2 device forwards a Done message to the upstream device. The upstream device then deletes the matching forwarding entry. This reduces the number of MLD messages on the network.

Prerequisites

MLD snooping has been enabled globally using the **mld-snooping_enable** command.

Precautions

- The configuration takes effect only after you run the **mld-snooping_enable** command to enable MLD snooping in the VLAN.
- When receiving a Done message from a group member, the device sends Group-Specific Query messages to check whether the group has other members on the network segment.
- MLD Report message suppression cannot be configured in a VLAN if the corresponding VLANIF interface has IPv6 Layer 3 multicast function (such as MLD and IPv6 PIM) enabled.
- MLD snooping proxy and MLD Report message suppression cannot be configured in the same VLAN.
- If multicast VLAN replication is configured, the MLD message suppression function cannot be enabled in user VLANs.
- The switch can suppress duplicate Report messages even when MLD message suppression is disabled. The default suppression time is 10 seconds. To change the suppression time, run the **mld-snooping suppression-time** *suppression-time* command. If *suppression-time* is set to 0, all membership packets are forwarded immediately.
- This function cannot suppress MLDv2 packets.

Example

Enable suppression of Report and Done messages in VLAN 2.

```
<HUAWEI>system view
[HUAWEI] mld-snooping enable
[HUAWEI] vlan 2
[HUAWEI-vlan2] mld-snooping enable
[HUAWEI-vlan2] mld-snooping report-suppress
```

8.12.23 mld-snooping require-router-alert

Function

The **mld-snooping require-router-alert** command configures the switch to check the received MLD messages for the Router-Alert option and discard the MLD messages without the Router-Alert option.

The **undo mld-snooping require-router-alert** command restores the default configuration.

By default, the switch processes the received MLD messages regardless of whether the messages contain the Router-Alert option.

Format

mld-snooping require-router-alert

undo mld-snooping require-router-alert

Parameters

None

Views

VLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The Router-Alert option identifies the protocol messages that need to be processed by upper-layer routing protocols.

By default, the switch does not check whether MLD messages contain the Router-Alert option and sends all the MLD messages to the upper-layer routing protocol. After the **mld-snooping require-router-alert** command is executed, the switch checks each MLD message for the Router-Alert option and discards those MLD messages without this option. This improves device performance, reduces cost, and enhances security of the upper-layer routing protocol.

Prerequisites

MLD snooping has been enabled globally using the **mld-snooping enable** command.

Precautions

If MLD snooping is disabled in the specified VLAN, the configuration succeeds but does not take effect until MLD snooping is enabled in the VLAN. To enable MLD snooping in a VLAN, run the **mld-snooping enable** command in the VLAN view.

Example

Configure the switch to accept only MLD messages with the Router-Alert option in VLAN 3.

```
<HUAWEI> system-view
[HUAWEI] mld-snooping enable
[HUAWEI] vlan 3
```



```
[HUAWEI-vlan3] mld-snooping enable
[HUAWEI-vlan3] mld-snooping require-router-alert
```

8.12.24 mld-snooping robust-count

Function

The **mld-snooping robust-count** command sets the MLD robustness variable in a VLAN.

The **undo mld-snooping robust-count** command restores the default MLD robustness variable in a VLAN.

By default, the MLD robustness variable in a VLAN is 2.

Format

mld-snooping robust-count *robust-count*

undo mld-snooping robust-count

Parameters

Parameter	Description	Value
robust-count	Specifies the MLD robustness variable.	The value is an integer that ranges from 2 to 5.

Views

VLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Setting MLD snooping parameters helps improve the multicast forwarding performance. By setting the MLD robustness variable, you can:

- Set the last listener query count for the querier to prevent packet loss.

  When receiving an MLD Done message of a multicast group, the querier sends Multicast-Address-Specific Query messages a certain number of times specified by the robustness variable to check whether the multicast has members. If the quality of transmission links is low, increase the MLD robustness variable.
- Change the aging time of member ports.

  When receiving an MLD Report message from a host, the switch starts the aging timer for the corresponding member port. The aging time is calculated

using the following formula: Aging time = MLD robustness variable x General query interval + Maximum response time for General Query messages. The **mld-snooping robust-count** command sets the MLD robustness variable.

Prerequisites

MLD snooping has been enabled globally using the **mld-snooping enable** command.

Follow-up Procedure

Perform the following operations to optimize multicast service performance:

- Run the **mld-snooping query-interval** command to set the interval at which General Query messages are sent.
- Run the **mld-snooping max-response-time** command to set the maximum response time for General Query messages.
- Run the **mld-snooping last-listener-query-interval** command to set the interval at which Multicast-Address-Specific Query messages are sent.

Precautions

The configuration takes effect only after you run the **mld-snooping_enable** command to enable MLD snooping in the VLAN.

Example

Set the robustness variable to 5 in VLAN 3.

```
<HUAWEI> system-view
[HUAWEI] mld-snooping enable
[HUAWEI] vlan 3
[HUAWEI-vlan3] mld-snooping enable
[HUAWEI-vlan3] mld-snooping robust-count 5
```

8.12.25 mld-snooping router-aging-time

Function

The **mld-snooping router-aging-time** command sets the aging time of dynamic router ports in a VLAN.

The **undo mld-snooping router-aging-time** command restores the default aging time of dynamic router ports in a VLAN.

By default, the aging time of dynamic router ports in a VLAN is 180 seconds or equal to the holdtime value contained in PIM Hello messages.

Format

mld-snooping router-aging-time *router-aging-time*

undo mld-snooping router-aging-time

Parameters

Parameter	Description	Value
router-aging-time	Indicates the aging time of a router port.	The value is an integer that ranges from 1 to 1000, in seconds.

Views

VLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When a short-term congestion occurs on a network, it takes a longer time to transmit Query messages from the MLD querier to a Layer 2 device. If a router port on the Layer 2 device ages out within this period, the Layer 2 device does not send Report or Done messages to the router port. As a result, multicast data forwarding may be interrupted. To solve this problem, set a longer aging time for router ports if the network is unstable.

When a dynamic router port receives an MLD Query message or PIM Hello message, the Layer 2 device sets the aging time of the router port as follows:

- If the router port receives an MLD Query message, the Layer 2 device sets the aging time of the router port to the configured value.
- If the router port receives a PIM Hello packet, the Layer 2 device sets the aging time of the router port to the Holdtime value contained in the PIM Hello packet.

Prerequisites

MLD snooping has been enabled globally using the **mld-snooping enable** command.

Precautions

The configuration takes effect only after you run the **mld-snooping_enable** command to enable MLD snooping in the VLAN.

If the aging time of a router port is too short, the router port ages frequently, degrading system performance.

Example

Set the aging time of router ports in VLAN 3 to 300 seconds.

```
<HUAWEI> system-view
[HUAWEI] mld-snooping enable
```



```
[HUAWEI] vlan 3
[HUAWEI-vlan3] mld-snooping enable
[HUAWEI-vlan3] mld-snooping router-aging-time 300
```

8.12.26 mld-snooping router-learning

Function

The **mld-snooping router-learning** command enables router port learning in a VLAN.

The **undo mld-snooping router-learning** command disables router port learning in a VLAN.

By default, router port learning is enabled in a VLAN.

Format

mld-snooping router-learning vlan { { *vlan-id1* [**to** *vlan-id2*] } &<1-10> | **all** }

undo mld-snooping router-learning vlan { { *vlan-id1* [**to** *vlan-id2*] } &<1-10> | **all** }

Parameters

Parameter	Description	Value
vlan *vlan-id1* [**to** *vlan-id2*]	Enables an interface to function as a router port in the specified VLANs.	*vlan-id1* and *vlan-id2* are integers that range from 1 to 4094.
all	Enables an interface to function as a router port in all the VLANs.	-

Views

Ethernet interface view, GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, port group view, Eth-Trunk interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A router port is located on a Layer 2 device and connects to an upstream Layer 3 device (a multicast router or Layer 3 switch). A switch running MLD snooping considers an interface as a router port when the interface receives an MLD General Query message with any source IP address except 0.0.0.0 or a PIM Hello message. A router port provides the following functions:

- Receives multicast data from the upstream device.
- Forwards MLD Report/Done messages. MLD Report/Done messages received in a VLAN are forwarded only to router ports in the VLAN.

Prerequisites

MLD snooping has been enabled globally using the **mld-snooping enable** command.

Follow-up Procedure

The switch does not listen on MLD Query or PIM Hello messages in a VLAN after router port learning is disabled in the VLAN. To ensure normal multicast forwarding in the VLAN, run the **mld-snooping static-router-port** command to configure a static router port.

Precautions

This command takes effect only when the interface has been added to the specified VLANs and MLD snooping has been enabled in these VLANs using the **mld-snooping enable** command.

Example

Disable router port learning on GE0/0/1 in VLAN 10.

```
<HUAWEI> system-view
[HUAWEI] mld-snooping enable
[HUAWEI] vlan 10
[HUAWEI-vlan10] mld-snooping enable
[HUAWEI-vlan10] quit
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo mld-snooping router-learning vlan 10
```

8.12.27 mld-snooping send-query enable

Function

The **mld-snooping send-query enable** command enables the switch to send MLD General Query messages to non-router ports when receiving Layer 2 topology change events.

The **undo mld-snooping send-query enable** command disables the switch from sending MLD General Query messages when receiving Layer 2 topology change events.

By default, the switch does not send MLD General Query messages when receiving Layer 2 topology change events.

Format

mld-snooping send-query enable

undo mld-snooping send-query enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the network topology changes, the switch receives a topology change event. By default, the switch does not send MLD General Query messages in this case. The network topology change triggers recalculation of the ring network protocol used (such as STP, MSTP, RRPP, SEP, and Smart Link). If the switch cannot respond to the topology change immediately, multicast data traffic cannot be switched to the new path in a timely manner. The **mld-snooping send-query enable** command enables the switch to send MLD General Query messages to update group memberships when the network topology changes. This ensures that multicast data traffic can be switched to the new transmission path.

Prerequisites

MLD snooping has been enabled globally using the **mld-snooping enable** command.

Follow-up Procedure

This command is used on a ring network. When the ring network topology changes, the switch sends MLD General Query messages with source IPv6 address FE80::. When this address has been occupied by another device on the network, run the **mld-snooping send-query source-address** command to set the source IPv6 address to FE80::.

Precautions

Use this command only when a ring network protocol is enabled on the switch.

Example

Enable the switch to send MLD General Query messages to non-router ports when receiving Layer 2 topology change events.

```
<HUAWEI> system-view
[HUAWEI] mld-snooping enable
[HUAWEI] mld-snooping send-query enable
```

8.12.28 mld-snooping send-query source-address

Function

The **mld-snooping send-query source-address** command sets the source IPv6 address of MLD General Query.

The **undo mld-snooping send-query source-address** command restores source IPv6 address of MLD General Query messages.

By default, the source IPv6 address of MLD General Query messages is FE80::.

Format

mld-snooping send-query source-address *ipv6-address*

undo mld-snooping send-query source-address

Parameters

Parameter	Description	Value
ipv6-address	Specifies the source IPv6 address of MLD General Query messages.	The address is a 32-digit hexadecimal number, in the format X:X:X:X:X:X:X:X, and the network prefix must be FE80::/64.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A Layer 2 device sends two types of MLD General Query messages:

- MLD General Query messages sent by the querier when the querier function is enabled using the **mld-snooping proxy** or **mld-snooping querier enable** command.
- MLD General Query messages that the Layer 2 device sends after receiving Layer 2 topology change events (configured using the **mld-snooping send-query enable** command).

By default, MLD General Query messages sent from a Layer 2 device use the source IPv6 address FE80::. When this IPv6 address is used by another device on the network, run the **mld-snooping send-query source-address** command to change the source IPv6 address of MLD General Query messages.

When multiple Layer 2 devices exist on a shared network, you can set source IPv6 addresses of MLD Query messages to identify the devices. For example, when multiple devices with different performance need to participate in querier election, you must configure a different source IPv6 address of MLD Query messages for each device.

When the MLD proxy function is enabled on a device using the **mld-snooping proxy** command or the function of suppressing Report and Leave messages is

enabled in a VLAN using the **mld-snooping report-suppress** command, the device sends MLD Report and MLD Done messages on behalf of downstream users, with the default source IP address of the MLD Report and MLD Done messages being FE80::. You can run this command to change the source IP address of MLD Report and MLD Done messages.

Prerequisites

MLD snooping has been enabled globally using the **mld-snooping enable** command.

Example

Set the source IPv6 address of MLD General Query messages to FE80::1.

```
<HUAWEI> system-view
[HUAWEI] mld-snooping enable
[HUAWEI] mld-snooping send-query source-address fe80::1
```

8.12.29 mld-snooping send-router-alert

Function

The **mld-snooping send-router-alert** command configures the switch to send MLD messages with the Router-Alert option in the IPv6 header to a VLAN.

The **undo mld-snooping send-router-alert** command configures the switch to send MLD messages without the Router-Alert option to a VLAN.

By default, the MLD messages sent by the switch contain the Router-Alert option.

Format

mld-snooping send-router-alert

undo mld-snooping send-router-alert

Parameters

None

Views

VLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The Router-Alert option identifies the protocol messages that need to be processed by upper-layer routing protocols.

By default, the switch sends MLD messages with the Router-Alert option. If some devices in the same VLAN as the switch can process only the MLD messages without the Router-Alert option, use the **undo igmp-snooping send-router-alert** command to configure the switch to send MLD messages without the Router-Alert option.

The switch adds the Router-Alert option only to locally originated MLD messages and does not add this option to MLD messages received from other devices.

Prerequisites

MLD snooping has been enabled globally using the **mld-snooping enable** command.

Precautions

The configuration takes effect only after you run the **mld-snooping_enable** command to enable MLD snooping in the VLAN.

Example

Configure the switch to send MLD messages that do not contain the Router-Alert option in the IPv6 header to VLAN 3.

```
<HUAWEI> system-view
[HUAWEI] mld-snooping enable
[HUAWEI] vlan 3
[HUAWEI-vlan3] mld-snooping enable
[HUAWEI-vlan3] undo mld-snooping send-router-alert
```

8.12.30 mld-snooping static-group

Function

The **mld-snooping static-group** command configures static IPv6 group memberships on an interface.

The **undo mld-snooping static-group** command deletes the static IPv6 group memberships on an interface.

By default, no static IPv6 group membership is configured on an interface.

Format

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

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

Parameters

Parameter	Description	Value
group-ipv6-address	Specifies the IPv6 address of a multicast group.	The address is a 32-digit hexadecimal number, in the format X:X:X:X:X:X:X:X. An IPv6 multicast address starts with FF.
source *source-ipv6-address*	Specifies the IPv6 address of a multicast source.	The address is a 32-digit hexadecimal number, in the format X:X:X:X:X:X:X:X.
vlan *vlan-id*	Specifies a VLAN ID.	The value is an integer that ranges from 1 to 4094.
all	Deletes all static group memberships from an interface.	-

Views

Ethernet interface view, GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, port group view, Eth-Trunk interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In addition to dynamic multicast forwarding entries generated by Layer 2 multicast protocol, you can configure static Layer 2 multicast forwarding entries by binding interfaces to multicast groups. After an interface is statically bound to a multicast group, users connected to this interface can keep receiving multicast data of the multicast group for a long time. The interface then becomes a static member interface.

Configuring static member interfaces has the following advantages:

- Protects the system against attacks from protocol packets.
- Reduces the network delay by directly forwarding multicast packets based on static forwarding entries.
- Prevents unregistered users from receiving multicast flows, improving information security and protecting service providers' interests.

Prerequisites

MLD snooping has been enabled globally using the **mld-snooping enable** command.

Precautions

The configuration takes effect only when both the following conditions are met:

- MLD snooping is enabled in the specified VLAN using the **mld-snooping enable** command.
- The specified VLAN has been created and the interface has been added to the VLAN.

Multicast group addresses starting with FFx1 or FFx2 (x is any value) cannot be configured as static multicast group addresses.

If a device is configured to forward Layer 2 multicast traffic on a network configured with MUX VLAN using the **multicast-snooping mux-vlan enable** command, the VLAN specified in the **mld-snooping static-group** command must not be a MUX VLAN (include principal VLAN and subordinate VLAN).

Example

Statically bind GE0/0/1 in VLAN 2 to multicast group ff1a::1.

```
<HUAWEI> system-view
[HUAWEI] mld-snooping enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] port link-type trunk
[HUAWEI-GigabitEthernet0/0/1] port trunk allow-pass vlan 2
[HUAWEI-GigabitEthernet0/0/1] mld-snooping static-group ff1a::1 vlan 2
```

8.12.31 mld-snooping static-router-port

Function

The **mld-snooping static-router-port** command configures a static router port in a VLAN.

The **undo mld-snooping static-router-port** command deletes a static router port in a VLAN.

By default, no static router port is configured in a VLAN.

Format

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

undo mld-snooping static-router-port { **all** | **vlan** *vlan-id* }

Parameters

Parameter	Description	Value
vlan *vlan-id*	Specifies a VLAN ID. This parameter specifies in which VLAN the current interface functions as a router port.	The value is an integer that ranges from 1 to 4094.
all	Disables the interface from functioning as a router port in all VLANs.	-

Views

Ethernet interface view, GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, port group view, Eth-Trunk interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When an interface needs to keep receiving or forwarding multicast data packets for a long time, configure the interface as a static router port.

Prerequisites

MLD snooping has been enabled globally using the **mld-snooping enable** command.

Precautions

This command takes effect only when the interface is added to the specified VLAN.

Example

Configure GE0/0/1 as a router port in VLAN 2.

```
<HUAWEI> system-view
[HUAWEI] mld-snooping enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] mld-snooping static-router-port vlan 2
```


8.12.32 mld-snooping suppression-time

Function

The **mld-snooping suppression-time** command sets the MLD message suppression time.

The **undo mld-snooping suppression-time** command restores the default MLD message suppression time.

By default, the MLD message suppression time is 10 seconds.

Format

mld-snooping suppression-time *suppression-time*

undo mld-snooping suppression-time

Parameters

Parameter	Description	Value
suppression-time	Specifies the MLD message suppression time.	The value is an integer ranging from 0 to 300, in seconds. The value 0 indicates that MLD messages are not suppressed.

Views

system view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To protect an upstream Layer 3 device from attacks and reduce the load on the Layer 3 device, a Layer 2 device can suppress duplicate MLD Report messages. The default MLD message suppression time is 10 seconds. You can change the MLD message suppression time using the **mld-snooping suppression-time** command.

After you set the MLD message suppression time on a Layer 2 multicast device, the device acts as follows:

- After the Layer 2 device receives an MLD Report message, it does not forward identical MLD Report messages to the router port within the suppression time.

- If the Layer 2 device receives an MLD General Query message or Multicast-Address-Specific Query message within the suppression time, it does not suppress the first MLD Report message sent in response to the Query message. In addition, the Layer 2 device resets the suppression timer when it receives the first MLD Report message.

Prerequisites

MLD snooping has been enabled globally using the **mld-snooping enable** command.

Precautions

You can run this command for MLDv1 Done and MLDv2 packets, but the command does not take effect.

Example

Set the MLD message suppression time to 15 seconds.

```
<HUAWEI> system-view
[HUAWEI] mld-snooping enable
[HUAWEI] mld-snooping suppression-time 15
```

8.12.33 mld-snooping table limit

Function

The **mld-snooping table limit** command sets the maximum number of MLD snooping entries that can be learned on an interface.

The **undo mld-snooping table limit** command cancels the limit on the number of MLD snooping entries that can be learned on an interface.

By default, the number of multicast entries that an interface can learn is not limited.

Format

mld-snooping table limit *limit* **vlan** *vlan-id*

undo mld-snooping table limit [*limit*] **vlan** *vlan-id*

Parameters

Parameter	Description	Value
limit	Specifies the maximum number of MLD snooping entries that can be learned on an interface.	The value is an integer and the value range depends on the product model: • SS1720GW-E, S1720GWR-E, S5720-LI, S5720S-LI, S5731-S, S5731S-S, and S5720I-SI: 1 to 1024 • S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S500, S5735-S, S5735-S-I, and S5735S-S: 1 to 1500 • S5735S-H, S5736-S, and S6720S-S: 1 to 1536 • S5731-H, S5731S-H, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S: 1 to 4096
vlan *vlan-id*	Specifies a VLAN ID.	The value is an integer ranging from 1 to 4094.

Views

Ethernet interface view, GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, port group view, Eth-Trunk interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The maximum number of MLD snooping entries on an interface limits the number of programs that users on the interface can order. You can set this limit to control the multicast data traffic on an interface.

Prerequisites

MLD snooping has been enabled globally using the **mld-snooping enable** command.

Configuration Impact

If the number of multicast entries on the interface already exceeds the configured threshold, the number of multicast entries on the interface does not change and the interface cannot learn new multicast entries.

Precautions

The configuration takes effect only after you run the **mld-snooping_enable** command to enable MLD snooping in the VLAN.

Example

Set the maximum number of MLD snooping entries that can be learned on GE0/0/1 in VLAN 5 to 100. (GE0/0/1 has been added to VLAN 5, and MLD snooping has been enabled globally and in VLAN 5.)

```
<HUAWEI> system view
[HUAWEI] mld-snooping enable
[HUAWEI] vlan 5
[HUAWEI-vlan5] mld-snooping enable
[HUAWEI-vlan5] quit
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] mld-snooping table limit 100 vlan 5
```

8.12.34 mld-snooping version

Function

The **mld-snooping version** command sets the version of MLD messages that MLD snooping can process in a VLAN.

The **undo mld-snooping version** command restores the default MLD message version.

By default, MLD snooping can process only MLDv1 messages.

Format

mld-snooping version *version*

undo mld-snooping version

Parameters

Parameter	Description	Value
version	Specifies the version of MLD messages that MLD snooping can process.	The value is 1 or 2. • 1: Only MLDv1 messages can be processed. • 2: Both MLDv1 and MLDv2 messages can be processed.

Views

VLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The MLD protocol maintains group memberships between Layer 3 multicast devices and hosts. MLD has two versions: v1 and v2. This command specifies the version of MLD messages that MLD snooping can process. Generally, configure the same version on the Layer 2 device as that on the upstream Layer 3 multicast device. If MLD is not enabled on the Layer 3 multicast device, configure the MLD message version on the Layer 2 device to be later than or equal to the MLD version running on downstream hosts.

When hosts in a VLAN run different MLD versions, run the **mld-snooping version** command to enable the Layer 2 device to process MLD messages sent from all the hosts.

Prerequisites

MLD snooping has been enabled globally using the **mld-snooping enable** command.

Precautions

This command cannot be used in user VLANs of a multicast VLAN.

When the MLD snooping version is set to MLDv2:

- The switch can use only the default Layer 2 multicast forwarding mode.
- The S1720GW-E, S1720GWR-E, S5720-LI, S5720S-LI, S5720I-SI, S5735S-H, S5736-S, and S6720S-S forward multicast data by looking up the forwarding table according to the VLAN ID and group address.

The configuration takes effect only after you run the **mld-snooping enable** command to enable MLD snooping in the VLAN.

Example

Set the MLD message version to 2 in VLAN 2.

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

8.12.35 multicast drop-unknown

Function

The **multicast drop-unknown** command configures the switch to discard unknown multicast flows in a VLAN.

The **undo multicast drop-unknown** command restores the default measure taken for unknown multicast flows.

The default method that a switch uses to process unknown multicast flows depends on whether Layer 2 multicast is enabled and which Layer 2 multicast forwarding mode is used.

Format

multicast drop-unknown

undo multicast drop-unknown

Parameters

None

Views

VLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Unknown multicast flows are those that do not match any entry in the multicast forwarding table or match multicast forwarding entries with an empty outbound interface list. These flows are not requested by users. When MLD snooping is disabled, the switch broadcasts unknown IPv6 multicast flows in the corresponding VLAN. After MLD snooping is enabled, the switch broadcasts unknown IPv6 multicast flows in the corresponding VLAN in MAC address-based forwarding mode. If IP address-based forwarding is used, the following switch models broadcast unknown IPv6 multicast flows in the corresponding VLAN and other switch models discard unknown IPv6 multicast flows: S5735S-H, S5736-S (except S5736-S48S4X-A, S5736-S48S4X-D, and S5736-S24UM4XC).. If a switch

broadcasts unknown multicast flows in a VLAN, you can configure the switch to drop unknown multicast flows, reducing instant bandwidth usage.

Configuration Impact

After the **multicast drop-unknown** command is executed, all unknown IPv4 and IPv6 multicast packets are discarded, including the protocol packets that are transparently transmitted within the VLAN and use the reserved multicast address.

For the S2730S-S, S5735-L-I, S5735-L1, S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735-S-I, and S5735S-S, if MAC address-based forwarding is configured as the Layer 2 multicast forwarding mode and the **multicast drop-unknown** command is executed, unknown multicast packets destined for the following reserved network segments and IP address cannot be dropped: 239.0.0.0/8, 224.0.0.0/24, 224.0.1.0/24, FF0X:0:0:0:0:0:0:0/96, FF0X::DB8:0:0/96, and the IPv6 address with the last 32 bits being 0000:00XX. To drop such unknown multicast packets, configure a traffic policy.

Example

Discard unknown multicast packets in VLAN 10.

```
<HUAWEI> system-view
[HUAWEI] vlan 10
[HUAWEI-vlan10] multicast drop-unknown
```

8.12.36 multicast-snooping mux-vlan enable

Function

The **multicast-snooping mux-vlan enable** command enables a device to transmit Layer 2 multicast traffic on a network configured with MUX VLAN.

The **undo multicast-snooping mux-vlan enable** command disables a device from transmitting Layer 2 multicast traffic on a network configured with MUX VLAN.

By default, a device is disabled from transmitting Layer 2 multicast traffic on a network configured with MUX VLAN.

Format

multicast-snooping mux-vlan enable

undo multicast-snooping mux-vlan enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

By default, on a network configured with MUX VLAN, Layer 2 multicast traffic cannot be transmitted between the principal VLAN and subordinate VLANs. You can run the **multicast-snooping mux-vlan enable** command to enable Layer 2 multicast traffic to be transmitted on the network configured with MUX VLAN.

Precautions

If a MUX VLAN is bound to a static multicast group using the **l2-multicast static-group** or **mld-snooping static-group** command, the **multicast-snooping mux-vlan enable** command cannot be executed. You must delete the association between the MUX VLAN and static multicast group before running the **multicast-snooping mux-vlan enable** command.

After the **multicast-snooping mux-vlan enable** command is configured, you cannot run the **l2-multicast static-group** or **mld-snooping static-group** command to bind a MUX VLAN to a static multicast group.

Example

Enable a device to forward Layer 2 multicast traffic on a network configured with MUX VLAN.

```
<HUAWEI> system-view
[HUAWEI] multicast-snooping mux-vlan enable
```

8.12.37 multicast-source-deny

Function

The **multicast-source-deny** command discards multicast data packets sent from specified VLANs on an interface.

The **undo multicast-source-deny** command restores multicast forwarding in specified VLANs on an interface.

By default, multicast data packets from all VLANs are forwarded on an interface.

Format

multicast-source-deny [**vlan** { *vlan-id1* [**to** *vlan-id2*] } &<1-10>]

undo multicast-source-deny [**vlan** { *vlan-id1* [**to** *vlan-id2*] } &<1-10>]

Parameters

Parameter	Description	Value
vlan *vlan-id1* [**to** *vlan-id2*]	Specifies a VLAN ID. • *vlan-id1* specifies the first VLAN ID. • **to** *vlan-id2* specifies the last VLAN ID. *vlan-id2* must be larger than *vlan-id1*. *vlan-id1* and *vlan-id2* specify a range of VLANs. If you do not specify **to** *vlan-id2*, only one VLAN is specified.	The value is an integer that ranges from 1 to 4094.

Views

MultiGE interface view, Ethernet interface view, GE interface view, XGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, port group view, Eth-Trunk interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After you run the **multicast-source-deny** command on an interface, multicast packets received from specified VLANs are discarded on the interface. You may need to use this command in the following scenarios:

- A user-side interface receives multicast packets, but the switch does not need to receive multicast data packets from user-side interfaces. Discarding multicast data packets received on a user-side interface protects the system against forged multicast flows sent from malicious users.
- Multiple multicast sources in different VLANs are connected to the switch through a Layer 2 network, but the switch only needs to receive multicast data from some of the multicast sources.
- In some situations, for example, multicast services for users connected to an interface have expired and need to be stopped, the network administrator can use this command on this interface. Then multicast data packets from specified VLANs cannot be sent to the users.

Precautions

If you run the **multicast-source-deny** command multiple times, all the configurations take effect.

When using the **multicast-source-deny** command on an interface, ensure that the interface has been added to the specified VLANs. Otherwise, the configuration does not take effect.

This command can discard only multicast data packets that meet both of the following conditions:

- The destination MAC address is an IP multicast MAC address (IPv4 MAC address starting with 0x01-00-5e or IPv6 multicast MAC address starting with 0x3333).
- The packet encapsulation protocol is UDP.

Example

Discard multicast data packets sent from VLANs 100 to 105 on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet0/0/1
[HUAWEI-GigabitEthernet0/0/1] multicast-source-deny vlan 100 to 105
```

8.12.38 reset mld-snooping group

Function

The **reset mld-snooping group** command deletes dynamic group memberships learned by MLD snooping.

Format

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

Parameters

Parameter	Description	Value
all	Deletes dynamic group memberships learned by MLD snooping.	-
vlan *vlan-id*	Deletes dynamic group memberships in a specified VLAN.	The value of *vlan-id* is an integer that ranges from 1 to 4094.
group-ipv6-address	Deletes the dynamic group memberships of a specified source address.	The address is a 32-digit hexadecimal number, in the format X:X:X:X:X:X:X:X. An IPv6 multicast address starts with FF.

Parameter	Description	Value
source-address *source-ipv6-address*	Deletes the dynamic group memberships of a specified source address.	The address is a 32-digit hexadecimal number, in the format X:X:X:X:X:X:X:X.

Views

User view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When multicast groups change on a network, the switch generates new Layer 2 multicast forwarding entries until the aging time of member ports expire. To enable the switch to generate new multicast forwarding entries immediately, use the **reset mld-snooping group** command to delete old memberships.

Precautions

NOTICE

Deleting group memberships in a VLAN temporarily interrupts multicast forwarding in the VLAN. The switch generates new forwarding entries only when receiving MLD Report messages from hosts in the VLAN. The hosts can then receive multicast data.

This command cannot delete static group memberships.

This command is valid only for VLANs with MLD snooping enabled and is invalid for a VLAN if MLD is enabled on the corresponding VLANIF interface.

Example

Delete dynamic group memberships in VLAN 2.

```
<HUAWEI> reset mld-snooping group vlan 2
```

8.12.39 reset mld-snooping statistics

Function

The **reset mld-snooping statistics** command clears MLD snooping statistics.

Format

reset mld-snooping statistics [**vlan** *vlan-id*]

Parameters

Parameter	Description	Value
vlan *vlan-id*	Clears the MLD snooping statistics in a specified VLAN.	The value is an integer that ranges from 1 to 4094.

Views

User view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To analyze the MLD snooping statistics collected in a certain period, run this command to clear the previous statistics. After a while, run the **display mld-snooping statistics** command to view the MLD snooping statistics.

Precautions

NOTICE

The cleared MLD snooping statistics cannot be restored.

Example

Clear MLD snooping statistics in VLAN 2.

```
<HUAWEI> reset mld-snooping statistics vlan 2
```

8.13 Static Multicast MAC Address Configuration Commands

8.13.1 Command Support

Commands provided in this section and all the parameters in the commands are supported by all switch models (except the S5731-L and S5731S-L), unless otherwise specified. For details, see specific commands.

8.13.2 display mac-address multicast

Function

The **display mac-address multicast** command displays the static multicast MAC address entries.

Format

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

Parameters

Parameter	Description	Value
mac-address	Specifies a multicast MAC address. If this parameter is not specified, the system displays all the configured multicast MAC address entries.	The value is in the H-H-H format. An H contains 1 to 4 hexadecimal digits.
vlan *vlan-id*	Displays multicast MAC address entries in a specified VLAN. If this parameter is not specified, the system displays multicast MAC address entries in all VLANs.	The value is an integer that ranges from 1 to 4094.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

This command displays static multicast MAC address entries. To configure a static multicast MAC address on the device, use the **mac-address multicast interface** or **mac-address multicast** command.

Example

Display static multicast MAC address entries in VLAN 10.

```
<HUAWEI> display mac-address multicast vlan 10
------------------------------------------------------------------------------
```



```
MAC Address       VLANID       Out-Interface                Status
--------------------------------------------------------------------------------
0111-1111-2222    10           GigabitEthernet0/0/1         InActive
                               GigabitEthernet0/0/2         InActive
                                   2 port(s)
--------------------------------------------------------------------------------
Total Group(s) : 1
```

Table 8-144 Description of the **display mac-address multicast vlan 10** command output

Item	Description
MAC Address	Static multicast MAC address.
VLANID	VLAN that the interface bound to the multicast MAC address belongs to.
Out-Interface	Interface bound to the multicast MAC address.
Status	Status of a VLAN. InActive indicates that the VLAN has not been created or no physical interface is added to the VLAN after it is created. Active indicates that the VLAN has been created and has physical interfaces in it.
Total Group(s)	Total number of multicast groups.

8.13.3 display mac-address multicast total-number

Function

The **display mac-address multicast total-number** command displays the number of static multicast MAC address entries.

Format

display mac-address multicast [**vlan** *vlan-id*] **total-number**

Parameters

Parameter	Description	Value
vlan *vlan-id*	Displays the number of static multicast MAC address entries in a specified VLAN. If this parameter is not specified, the system displays the total number of static multicast MAC address entries in all VLANs.	The value is an integer that ranges from 1 to 4094.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenarios

The **display mac-address multicast total-number** displays the number of static multicast MAC address entries.

Precautions

If no static MAC address entry is configured, the total number of MAC address entries is displayed as 0. You can use the **mac-address multicast** command to statically bind a multicast MAC address to an interface or use the **mac-address multicast interface** command to statically bind a MAC address to multiple interfaces.

Example

Display the number of static multicast MAC address entries in VLAN 10.

```
<HUAWEI> display mac-address multicast vlan 10 total-number
Total number of mac-address : 3
```

Table 8-145 Description of the **display mac-address multicast vlan 10 total-number** command output

Item	Description
Total number of mac-address	Number of static multicast MAC address entries.

8.13.4 mac-address multicast

Function

The **mac-address multicast** command configures a static multicast MAC address on an interface.

The **undo mac-address multicast** command deletes the static MAC address from an interface.

By default, no static multicast MAC address is configured on an interface.

Format

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

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

Parameters

Parameter	Description	Value
mac-address	Specifies a multicast MAC address.	The value is in H-H-H format. An H contains 1 to 4 hexadecimal digits.
vlan *vlan-id*	Specifies the VLAN that the interface belongs to.	The value is an integer that ranges from 1 to 4094.

Views

MultiGE interface view, Ethernet interface view, GE interface view, XGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, port group view, Eth-Trunk interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

By default, the switch broadcasts received multicast packets in a VLAN, wasting network bandwidth and threatens network security. To reduce broadcasting of multicast packets, configure IGMP snooping or MLD snooping on the switch so that the switch can generate Layer 2 multicast forwarding entries. Alternatively, configure static multicast MAC address entries by binding multicast MAC addresses to interfaces.

After a static multicast MAC address is configured on an interface, multicast packets destined for this multicast MAC address are forwarded only to the interface in the specified VLAN.

Prerequisites

- The specified VLAN exists and the interfaces have been added to the VLAN.
- The switch has been configured to forward multicast data based on MAC addresses using the **l2-multicast forwarding-mode mac** command.

Precautions

- The MAC address specified in the command must be a multicast MAC address with the rightmost bit as 1 (xxxx xxx1).
- The VLAN specified in the command cannot be a super-VLAN, control VLAN of an Ethernet Ring Protection Switching (ERPS) ring, control VLAN of a Smart Ethernet Protocol (SEP) segment, or control VLAN of a Rapid Ring Protection Protocol (RRPP) ring.

- When the static multicast MAC address configured on an interface is an IPv4 multicast MAC address starting with 0x01-00-5e or an IPv6 multicast MAC address starting with 0x3333, Layer 2 multicast snooping cannot be enabled in the VLANs on the interface.
- Before configuring static multicast MAC addresses on an interface of the SS1720GW-E, S1720GWR-E, S5720-LI, S5720S-LI, S5720I-SI, S5735S-H, S5736-S, and S6720S-S, set the multicast data forwarding mode to MAC address-based mode in the VLAN to which the interface belongs.

Example

Configure static MAC address 0100-2100-2200 on GE0/0/1 in VLAN 10.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] port link-type trunk
[HUAWEI-GigabitEthernet0/0/1] port trunk allow-pass vlan 10
[HUAWEI-GigabitEthernet0/0/1] mac-address multicast 0100-2100-2200 vlan 10
```

8.13.5 mac-address multicast interface

Function

Using the **mac-address multicast interface** command, you can bind a multicast MAC address to multiple interfaces. Multicast packets destined for the specified multicast MAC address are forwarded by these interfaces.

Using the **undo mac-address multicast interface** command, you can delete a MAC address from multiple interfaces.

Format

mac-address multicast *mac-address* **interface** { *interface-type interface-number1* [**to** *interface-type interface-number2*] } &<1-10> **vlan** *vlan-id*

undo mac-address multicast *mac-address* **interface** { *interface-type interface-number1* [**to** *interface-type interface-number2*] } &<1-10> **vlan** *vlan-id*

undo mac-address multicast { **all** | [*mac-address*] **vlan** *vlan-id* }

Parameters

Parameter	Description	Value
mac-address	Specifies a multicast MAC address.	The value is in the H-H-H format. H is a hexadecimal number of 1 to 4 digits.
interface-type interface-number1	Specifies the start interface to which the MAC address is bound.	-

Parameter	Description	Value
to *interface-type interface-number2*	Specifies the end interface to which the MAC address is bound. The specified interfaces and *interface-number2* must be greater than *interface-number1*.	-
all	Deletes the multicast MAC address from all interfaces.	-
vlan *vlan-id*	Specifies the VLAN that the interfaces belong to.	The value is an integer that ranges from 1 to 4094.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenarios

If Layer 2 multicast snooping is disabled on a switch, the switch broadcasts all the received multicast data packets in corresponding VLANs. This wastes network bandwidth and threatens network security.

Configuring static multicast MAC addresses on interfaces can solve this problem. This configuration ensures that multicast packets destined for a multicast MAC address are forwarded only to interfaces configured with this multicast MAC address in the VLAN.

Precautions

- If you run the **mac-address multicast** command multiple times, all the configurations take effect.
- Before running this command, ensure that the VLAN has been created, and the interface where the multicast MAC address is configured has been added to this VLAN. Otherwise, configuration of this command does not take effect.
- The MAC address specified in the command must be a multicast MAC address with the rightmost bit as 1 (xxxx xxx1).
- The VLAN specified in the command cannot be a super-VLAN, control VLAN of an Ethernet Ring Protection Switching (ERPS) ring, control VLAN of a Smart Ethernet Protocol (SEP) segment, or control VLAN of a Rapid Ring Protection Protocol (RRPP) ring.

- When the static multicast MAC address configured on an interface is an IPv4 multicast MAC address starting with 0x01-00-5e or an IPv6 multicast MAC address starting with 0x3333, Layer 2 multicast snooping cannot be enabled in the VLANs on the interface.
- Before configuring static multicast MAC addresses on an interface of the SS1720GW-E, S1720GWR-E, S5720-LI, S5720S-LI, S5720I-SI, S5735S-H, S5736-S, and S6720S-S, set the multicast data forwarding mode to MAC address-based mode in the VLAN to which the interface belongs.

Example

Bind multicast MAC address 0100-2100-2200 to interfaces GE0/0/1 to GE0/0/4 in VLAN 10.

```
<HUAWEI> system-view
[HUAWEI] mac-address multicast 0100-2100-2200 interface gigabitethernet 0/0/1 to gigabitethernet 0/0/4 vlan 10
```

8.13.6 multicast mac-ip check enable

Function

The **multicast mac-ip check enable** command enables the function of checking the mapping between multicast IP and MAC addresses.

The **undo multicast mac-ip check enable** command disables the function of checking the mapping between multicast IP and MAC addresses.

By default, the function of checking the mapping between multicast IP and MAC addresses is disabled.

Product	Support
S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S	Supported

Product	Support
SS1720GW-E, S1720GWR-E, S5720I-SI, S5720-LI, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5720S-LI, S5735-S, S500, S5735S-S, S5735-S-I, S5735S-H, S5736-S, and S6720S-S	Not supported The S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735-S-I, and S5735S-S check the mapping between multicast IP and MAC addresses for received packets by default. On these models, Layer 2 multicast packets with incorrect mappings cannot be forwarded based on IP addresses but can be forwarded based on MAC addresses; Layer 3 multicast packets with incorrect mappings are discarded. Other switch models do not perform this check on multicast packets. They simply forward Layer 2 multicast packets and discard Layer 3 multicast packets.

Format

multicast mac-ip check enable

undo multicast mac-ip check enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

To enable multicast sources and group members to communicate, network-layer multicast services must be provided using multicast IP addresses. To enable multicast data to be correctly transmitted on the local physical network, link-layer multicast services must be provided using multicast MAC addresses. The destination address of a multicast data packet is a group with unknown members but not a specific receiver. Therefore, multicast IP addresses must be mapped to multicast MAC addresses. For the detailed mapping between multicast IP and MAC addresses, see Multicast Addresses under **IP Multicast Configuration Guide** > **Understanding IP Multicast** in the *S300, S500, S2700, S5700, and S6700 V200R023C00 Configuration Guide*.

By default, the function of checking the mapping between multicast IP and MAC addresses is disabled. Therefore, packets with incorrect mapping will be processed normally. After the mapping between multicast IP and MAC addresses is enabled, different products process multicast packets in different modes. The following table provides the details.

Table 8-146 Methods used by different products to process multicast packets

Product	How Multicast Packets Are Processed
S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S	Packets with incorrect IP and MAC address mapping are discarded.
S6720-EI, S6735-S, and S6720S-EI	If no MAC address entries are available for the packets with incorrect IP and MAC address mapping, the packets are forwarded as unknown multicast packets. For the forwarding process of unknown multicast packets, see **multicast drop-unknown**.

Example

Enable the function of checking the mapping between multicast IP and MAC addresses.

```
<HUAWEI> system-view
[HUAWEI] multicast mac-ip check enable
```

8.14 Multicast VLAN Configuration Commands

8.14.1 Command Support

Commands provided in this section and all the parameters in the commands are supported by all switch models (except the S5731-L and S5731S-L), unless otherwise specified. For details, see specific commands.

8.14.2 display l2-multicast-bind

Function

The **display l2-multicast-bind** command displays bindings between multicast VLANs and user VLANs.

Format

display l2-multicast-bind [**mvlan** *vlan-id*]

Parameters

Parameter	Description	Value
mvlan *vlan-id*	Displays the binding between user VLANs and a specified multicast VLAN. *vlan-id* specifies a multicast VLAN ID.	The value is an integer that ranges from 1 to 4094.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

After configuring multicast VLAN replication on an interface, you can run the **display l2-multicast-bind** command to view the configuration. This command can be used for fault location when multicast VLAN replication fails.

Precautions

If there is no binding between any multicast VLAN and user VLAN, the **display l2-multicast-bind** command does not display any information.

Example

Display bindings between user VLANs and multicast VLAN 400.

```
<HUAWEI> display l2-multicast-bind mvlan 400
------------------------------------------------------------------------------
Port                        Startvlan       Endvlan         Mvlan
------------------------------------------------------------------------------
GigabitEthernet0/0/1            222             --          400
------------------------------------------------------------------------------
Total Table(s) : 1
```

Table 8-147 Description of the **display l2-multicast-bind** command output

Item	Description
Port	Interface where user VLANs are bound to the multicast VLAN.
Startvlan	First user VLAN ID.
Endvlan	Last user VLAN ID. If "--" is displayed, only one user VLAN is bound to the multicast VLAN.

Item	Description
Mvlan	Multicast VLAN ID.
Total Table(s)	Total number of multicast VLAN binding entries.

8.14.3 display multicast static-flow

Function

The **display multicast static-flow** command displays the configuration of the static flow in a multicast VLAN.

Format

display multicast static-flow [**vlan** *vlan-id*]

Parameters

Parameter	Description	Value
vlan *vlan-id*	Displays static multicast flows in a specified VLAN.	The value is an integer that ranges from 1 to 4094.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

When a static flow is configured in a multicast VLAN, you can run the **display multicast static-flow** command to view the mapping between the multicast VLAN and (S, G) entry.

Example

Display the static flow configured in multicast VLAN 10.

```
<HUAWEI> display multicast static-flow vlan 10
-------------------------------------------------------------
   Vlan           (Source, Group)
-------------------------------------------------------------
    10           (*,  225.0.0.1)
-------------------------------------------------------------
Total Table(s): 1
```


Table 8-148 Description of the **display multicast static-flow** command output

Item	Description
Vlan	VLAN where the static flow is configured.
(Source, Group)	(S, G) entry, specifying the multicast source and multicast group.
Total Table(s)	Total number of static multicast flows.

8.14.4 display multicast-vlan

Function

The **display multicast-vlan** command displays information about multicast VLANs.

Format

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

Parameters

Parameter	Description	Value
vlan [*vlan-id*]	Specifies the ID of a multicast VLAN. • If *vlan-id* is specified, detailed information about the specified multicast VLAN and its user VLANs is displayed. • If *vlan-id* is not specified, brief information about all the multicast VLANs is displayed.	The value is an integer that ranges from 1 to 4094.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The **display multicast-vlan** command displays configuration of multicast VLANs. You can run the **display multicast-vlan** command to check whether any user VLAN is bound to the multicast VLAN and whether IGMP snooping or MLD snooping is enabled in the multicast VLAN and user VLAN. This command can be used to locate faults when the multicast service fails.

Example

Display information about all multicast VLANs and user VLANs.

```
<HUAWEI> display multicast-vlan vlan
 Total multicast vlan   2
 multicast-vlan     user-vlan number     snooping-state
 ---------------------------------------------------------------------
 5                  1                    IGMP Enable /MLD Disable
 7                  2                    IGMP Enable /MLD Disable
```

Table 8-149 Description of the **display multicast-vlan vlan** command output

Item	Description
Total multicast vlan	Number of multicast VLANs.
multicast-vlan	ID of a multicast VLAN.
user-vlan number	Number of user VLANs bound to a multicast VLAN.
snooping-state	Whether IGMP snooping and MLD snooping is enabled in a multicast VLAN.

Display information about multicast VLAN 7 and its user VLANs.

```
<HUAWEI> display multicast-vlan vlan 7
 Multicast-vlan         : 7
 User-vlan Number       : 2
 IGMP snooping state    : Enable
 MLD  snooping state    : Disable
 User-vlan              Snooping-state
 Prune-source-port state: Disable
 ---------------------------------------
 8                    IGMP Enable /MLD Disable
 9                    IGMP Enable /MLD Disable
```

Table 8-150 Description of the **display multicast-vlan vlan** *vlan-id* command output

Item	Description
Multicast-vlan	ID of a multicast VLAN.
User-vlan Number	Number of user VLANs bound to a multicast VLAN.
IGMP snooping state	Whether IGMP snooping is enabled in a multicast VLAN.

Item	Description
MLD snooping state	Whether MLD snooping is enabled in a multicast VLAN.
User-vlan	ID of a user VLAN.
Prune-source-port state	Whether permits Query messages received in a multicast VLAN to be sent back to from the upstream interface through user VLANs.
Snooping-state	Whether IGMP snooping and MLD snooping are enabled in a user VLAN.

8.14.5 display user-vlan

Function

Using the **display user-vlan** command, you can view information about a user VLAN.

Format

display user-vlan vlan [*vlan-id*]

Parameters

Parameter	Description	Value
vlan [*vlan-id*]	Specifies the ID of a user VLAN. If *vlan-id* is specified, information about the specified user VLAN is displayed. If *vlan-id* is not specified, information about all user VLANs is displayed.	The value is an integer that ranges from 1 to 4094.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After binding a user VLAN to a multicast VLAN, you can run the **display user-vlan** command to verify the configuration and check whether IGMP snooping or MLD

Snooping is enabled. This command can be used to locate faults when the multicast service fails.

Example

Display information about all user VLANs.

```
<HUAWEI> display user-vlan vlan
 Total user vlan   3
 user-vlan  snooping-state           multicast-vlan  snooping-state
 ------------------------------------------------------------------------------
 8          IGMP Disable/MLD Disable  7              IGMP Enable /MLD Disable
 9          IGMP Disable/MLD Disable  7              IGMP Enable /MLD Disable
 11          IGMP Disable/MLD Disable  7              IGMP Enable /MLD Disable
```

Display information about user VLAN 8.

```
<HUAWEI> display user-vlan vlan 8
 user-vlan  snooping-state           multicast-vlan
 ------------------------------------------------------
 8          IGMP Disable/MLD Disable   7
```

Table 8-151 Description of the **display user-vlan** command output

Item	Description
Total user vlan	Number of user VLANs.
user-vlan	ID of a user VLAN.
multicast-vlan	ID of the multicast VLAN that a user VLAN belongs to.
snooping-state	Whether IGMP snooping and MLD snooping are enabled in a multicast VLAN or a user VLAN.

8.14.6 l2-multicast-bind vlan

Function

The **l2-multicast-bind vlan** command binds user VLANs to a multicast VLAN on an interface.

The **undo l2-multicast-bind vlan** command restores the default setting.

By default, no user VLAN is bound to a multicast VLAN on an interface.

Format

l2-multicast-bind vlan *vlan-id1* [**to** *vlan-id2*] **mvlan** *mvlan-id*

undo l2-multicast-bind vlan { *vlan-id1* [**to** *vlan-id2*] | **all** }

Parameters

Parameter	Description	Value
vlan *vlan-id1* [**to** *vlan-id2*]	Specifies the ID of a user VLAN.	The value is an integer that ranges from 1 to 4094.
mvlan *mvlan-id*	Specifies the ID of a multicast VLAN.	The value is an integer that ranges from 1 to 4094.
all	Unbinds all user VLANs from the multicast VLAN on an interface.	-

Views

MultiGE interface view, Ethernet interface view, GE interface view, XGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, port group view, Eth-Trunk interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A carrier provides the multicast service for multiple Internet service providers (ISPs), and each ISP is assigned a multicast VLAN to isolate multicast data and routes of different ISPs. Users connected to different user-side interfaces of the switch may order multicast services of different ISPs but belong to the same user VLAN. If multicast replication based on user VLANs is used in this case, users may receive multicast data they do not require. This affects the income of the ISPs.

To solve this problem, bind the user VLAN to multicast VLANs of the ISPs whose services are ordered on user-side interfaces. Then the user-side interfaces accept only the data from multicast VLANs of the specified ISPs.

Prerequisites

IGMP snooping has been enabled using the **igmp-snooping enable (VLAN view)** command on the multicast VLAN.

Precautions

Before running this command, run the **vlan** command to create the corresponding user VLAN and multicast VLAN. Otherwise, configuration of this command does not take effect.

On an interface, a user VLAN can be bound to only one multicast VLAN.

Currently, the binding of user VLANs to a multicast VLAN on an interface is only supported on IPv4 networks.

Example

Bind user VLAN100 to multicast VLAN20 on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] igmp-snooping enable
[HUAWEI] vlan 100
[HUAWEI-vlan100] igmp-snooping enable
[HUAWEI-vlan100] quit
[HUAWEI] vlan 20
[HUAWEI-vlan20] igmp-snooping enable
[HUAWEI-vlan20] quit
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] l2-multicast-bind vlan 100 mvlan 20
```

8.14.7 l2-multicast user-vlan limit

Function

The **l2-multicast user-vlan limit** command sets the number of user VLANs that are allowed.

The **undo l2-multicast user-vlan limit** command restores the default configuration.

By default, 512 user VLANs can be configured.

Format

l2-multicast user-vlan limit *number*

undo l2-multicast user-vlan limit

NOTE

This command is supported only on the S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735-S-I, and S5735S-S.

Parameters

Parameter	Description	Value
number	Specifies the number of user VLANs that can be configured.	The value is an integer in the range from 1 to 1000.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

User VLANs and the Layer 3 VLANIF service share resources. Too large a number of user VLANs will affect the specification of VLANIF interfaces. You can run the **l2-multicast user-vlan limit** command to adjust the number of user VLANs that can be configured based on your service requirements.

Example

Set the number of user VLANs that can be configured to 300.

```
<HUAWEI> system-view
[HUAWEI] l2-multicast user-vlan limit 300
```

8.14.8 multicast flow-trigger enable

Function

The **multicast flow-trigger enable** command enables the triggering of multicast flows in a VLAN.

The **undo multicast flow-trigger enable** command disables the triggering of multicast flows in a VLAN.

By default, the triggering of multicast flows is disabled in VLANs.

Format

multicast flow-trigger enable

undo multicast flow-trigger enable

Parameters

None

Views

VLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When a user VLAN (for example, UVLAN) needs to join multiple multicast VLANs (for example, MVLAN1 to MVLAN*n*), you need to perform the following operations to ensure that N-to-N mappings based on {UVLAN, Source, Group} can be created between UVLANs and MVLANs and multicast entries can be generated when UVLANs send VOD requests to the MVLANs:

1. Run the **multicast flow-trigger enable** command in the UVLAN to enable triggering of multicast flows.

2. Run the **multicast-vlan user-vlan** command in each MVLAN to configure mappings between the UVLAN and MVLANs.
3. Run the **multicast static-flow** command in each MVLAN to configure a static flow.

Precautions

The **multicast flow-trigger enable** and **multicast-vlan enable** commands cannot be configured in the same VLAN.

Example

Enable the triggering of multicast flows in VLAN 100.

```
<HUAWEI> system-view
[HUAWEI] vlan 100
[HUAWEI-vlan100] multicast flow-trigger enable
```

8.14.9 multicast static-flow

Function

The **multicast static-flow** command configures static flows in a multicast VLAN.

The **undo multicast static-flow** command deletes static flows from a multicast VLAN.

By default, no static flow is configured in multicast VLANs.

Format

multicast static-flow { *ipv4-group-address1* [**to** *ipv4-group-address2*] [**source** *ipv4-source-address*] | **ipv6** *ipv6-group-address1* [**to** *ipv6-group-address2*] [**source** *ipv6-source-address*] }

undo multicast static-flow { *ipv4-group-address1* [**to** *ipv4-group-address2*] [**source** *ipv4-source-address*] | **ipv6** *ipv6-group-address1* [**to** *ipv6-group-address2*] [**source** *ipv6-source-address*] | **all** }

Parameters

Parameter	Description	Value
ipv4-group-address1 [**to** *ipv4-group-address2*]	Specifies the IPv4 address of a multicast group.	The value ranges from 224.0.1.0 to 239.255.255.255, in dotted decimal notation.
source *ipv4-source-address*	Specifies the source IPv4 address.	The value is in dotted decimal notation.

Parameter	Description	Value
ipv6 *ipv6-group-address1* [**to** *ipv6-group-address2*]	Specifies the IPv6 address of a multicast group.	The address is a 32-digit hexadecimal number, in the format X:X:X:X:X:X:X:X. An IPv6 multicast address starts with FF.
source *ipv6-source-address*	Specifies the source IPv6 address.	The address is a 32-digit hexadecimal number, in the format X:X:X:X:X:X:X:X.
all	Deletes all static multicast flows in a VLAN.	-

Views

VLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When a user VLAN (for example, UVLAN) needs to join multiple multicast VLANs (for example, MVLAN1 to MVLANn), you need to run the **multicast flow-trigger enable** command in the view of user VLAN to enable the triggering of multicast flows, and then configure static flows in each multicast VLAN. In this manner, the many-to-many mapping based on {UVLAN, Source, Group} is set up between user VLANs and multicast VLANs.

Precautions

Any two static flows in a multicast VLAN cannot be the same. Note that flows of the same multicast group with different source IP addresses are considered as different flows.

When you use the **multicast static-flow** { *ipv4-group-address1* **to** *ipv4-group-address2* | *ipv6-group-address1* **to** *ipv6-group-address2* } command to configure static multicast flows in batches, a maximum of 256 flows can be configured each time. When configuring an IPv4 multicast address segment, ensure that the consecutive addresses are in a multicast address segment with a 24-bit mask. When configuring an IPv6 multicast address segment, ensure that the consecutive addresses are in a multicast address segment with a 120-bit prefix. For example, the **multicast static-flow 225.0.0.255 to 225.0.1.1** command will not take effect because the addresses belong to two different segments: 225.0.0.0/24 and 225.0.1.0/24.

Example

Configure a static flow with the source address being 10.0.0.1 and group address being 232.0.0.1 in multicast VLAN 10.

```
<HUAWEI> system-view
[HUAWEI] igmp-snooping enable
[HUAWEI] vlan 10
[HUAWEI-vlan10] igmp-snooping enable
[HUAWEI-vlan10] igmp-snooping version 3
[HUAWEI-vlan10] multicast-vlan enable
[HUAWEI-vlan10] multicast static-flow 232.0.0.1 source 10.0.0.1
```

Configure a static flow with the source address being FE80::1 and group address being FF23::123 in multicast VLAN 20.

```
<HUAWEI> system-view
[HUAWEI] vlan 20
[HUAWEI-vlan20] mld-snooping enable
[HUAWEI-vlan20] mld-snooping version 2
[HUAWEI-vlan20] multicast-vlan enable
[HUAWEI-vlan20] multicast static-flow ipv6 ff23::123 source fe80::1
```

8.14.10 multicast-vlan enable

Function

The **multicast-vlan enable** command configures a VLAN as a multicast VLAN.

The **undo multicast-vlan enable** command restores the default configuration.

By default, a VLAN is a common VLAN.

Format

multicast-vlan enable

undo multicast-vlan enable

Parameters

None

Views

VLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Generally, a switch needs to replicate multicast packets for each VLAN when users in different VLANs need to receive multicast data from the same multicast source. If a multicast VLAN is configured and the VLANs that users belong to are

configured as the user VLANs of the multicast VLAN, the switch only needs to replicate the multicast data for the multicast VLAN. Multicast data is then replicated to the user VLANs by the multicast VLAN. This reduces load on the upstream router and separates the multicast source from the users.

Prerequisites

IGMP snooping or MLD snooping has been enabled in a VLAN using the **igmp-snooping enable (VLAN view)** or **mld-snooping enable** command.

Follow-up Procedure

Run the **multicast-vlan user-vlan** command to bind user VLANs to the multicast VLAN.

Precautions

- A multicast VLAN cannot be configured as a user VLAN. A user VLAN cannot be configured as a multicast VLAN.
- If MAC address-based forwarding is configured using the **l2-multicast forwarding-mode** command in a VLAN, the VLAN cannot be configured as a multicast VLAN.
- Before running the **undo multicast-vlan enable** command in a multicast VLAN, delete all the user VLANs from the multicast VLAN. If OAM is bound to the multicast VLAN, unbind OAM from the multicast VLAN first.
- The **multicast flow-trigger enable** and **multicast-vlan enable** commands cannot be configured in the same VLAN.

Example

Configure VLAN 2 as a multicast VLAN.

```
<HUAWEI> system-view
[HUAWEI] igmp-snooping enable
[HUAWEI] vlan 2
[HUAWEI-vlan2] igmp-snooping enable
[HUAWEI-vlan2] multicast-vlan enable
```

8.14.11 multicast-vlan send-query prune-source-port

Function

The **multicast-vlan send-query prune-source-port** command prevents the upstream interface from sending Query messages received in a multicast VLAN back to upstream devices through user VLANs.

The **undo multicast-vlan send-query prune-source-port** command restores the default configuration.

By default, an upstream interface can send Query messages received in a multicast VLAN back to upstream devices through user VLANs.

Format

multicast-vlan send-query prune-source-port

undo multicast-vlan send-query prune-source-port

Parameters

None

Views

VLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In multicast VLAN application, an upstream interface usually belongs to a multicast VLAN and user VLANs bound to the multicast VLAN. By default, an upstream interface can send Query messages received in a multicast VLAN back to upstream devices through user VLANs.

To prevent Query messages from being sent back to upstream devices, run this command in the multicast VLAN.

Prerequisites

The multicast VLAN function has been enabled using the **multicast-vlan enable** command in the VLAN view.

Example

Prevent the upstream interface from sending Query messages received in multicast VLAN 10 back to upstream devices through user VLANs.

```
<HUAWEI> system-view
[HUAWEI] igmp-snooping enable
[HUAWEI] vlan 10
[HUAWEI-vlan10] igmp-snooping enable
[HUAWEI-vlan10] multicast-vlan enable
[HUAWEI-vlan10] multicast-vlan send-query prune-source-port
```

8.14.12 multicast-vlan user-vlan

Function

The **multicast-vlan user-vlan** command binds user VLANs to a multicast VLAN.

The **undo multicast-vlan user-vlan** command unbinds user VLANs from a multicast VLAN.

By default, a multicast VLAN does not have any user VLAN.

Format

multicast-vlan user-vlan { *vlan-id1* [**to** *vlan-id2*] } &<1-10>

undo multicast-vlan user-vlan { **all** | { *vlan-id1* [**to** *vlan-id2*] } &<1-10> }

Parameters

Parameter	Description	Value
vlan-id1 [**to** *vlan-id2*]	Specifies IDs of the user VLANs. ● *vlan-id1* specifies the start VLAN ID. ● *vlan-id2* specifies the end VLAN ID. The value of *vlan-id2* must be greater than the value of *vlan-id1*. The *vlan-id1* and *vlan-id2* parameters identify a range of VLANs. If **to** *vlan-id2* is not specified, only one user VLAN is bound to the multicast VLAN.	The settings of the parameters are as follows: ● The value of *vlan-id1* is an integer that ranges from 1 to 4094. ● The value of *vlan-id2* is an integer that ranges from 1 to 4094.
all	Deletes all the user VLANs from a multicast VLAN.	-

Views

VLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After configuring a multicast VLAN, you can use the **multicast-vlan user-vlan** command to bind user VLANs to the multicast VLAN. The Layer 3 device replicates multicast data only in the multicast VLAN and sends the multicast data to the Layer 2 device. This saves bandwidth and reduces load on the Layer 3 device because it does not need to replicate multicast data in every user VLAN.

Prerequisites

- Before running this command, run the **igmp-snooping enable** or **mld-snooping enable** command to enable IGMP snooping or MLD snooping globally, in the user VLANs, and in the multicast VLAN.
- Before running this command, run the **multicast-vlan enable** command to enable the multicast VLAN function in the multicast VLAN.

Precautions

- A user VLAN cannot be configured as a multicast VLAN.
- The user VLANs must exist.
- For the S6720-EI, S6735-S, and S6720S-EI, if the received multicast packets carry double VLAN tags, the inner VLAN tag will be removed and the double VLAN tags will be replaced with a single user VLAN tag when the multicast-vlan user-vlan command is run to bind user VLANs to the multicast VLAN.

Example

Bind user VLAN 10 to multicast VLAN 2.

```
<HUAWEI> system-view
[HUAWEI] vlan batch 2 10
[HUAWEI] igmp-snooping enable
[HUAWEI] vlan 10
[HUAWEI-vlan10] igmp-snooping enable
[HUAWEI-vlan10] quit
[HUAWEI] vlan 2
[HUAWEI-vlan2] igmp-snooping enable
[HUAWEI-vlan2] multicast-vlan enable
[HUAWEI-vlan2] multicast-vlan user-vlan 10
```

Bind user VLANs 3 to 10 to multicast VLAN 2.

```
<HUAWEI> system-view
[HUAWEI] vlan batch 2 to 10
[HUAWEI] igmp-snooping enable
[HUAWEI] igmp-snooping enable vlan 2 to 10
[HUAWEI] vlan 2
[HUAWEI-vlan2] multicast-vlan enable
[HUAWEI-vlan2] multicast-vlan user-vlan 3 to 10
```

8.15 Controllable Multicast Configuration Commands

8.15.1 Command Support

Commands provided in this section and all the parameters in the commands are supported by all switch models (except the S5731-L and S5731S-L), unless otherwise specified. For details, see specific commands.

8.15.2 add multicast-group

Function

The **add multicast-group** command adds multicast groups to a multicast group list.

The **undo add multicast-group** command removes multicast groups from a multicast group list.

By default, no multicast group is contained in a multicast group list.

Format

add multicast-group { **name** *group-name* | **index** *start-index* **to** *end-index* }

undo add multicast-group { **name** *group-name* | **index** *start-index* **to** *end-index* }

Parameters

Parameter	Description	Value
name *group-name*	Specifies the name of a multicast group.	The value is a string of 1 to 31 case-insensitive characters without spaces.
index *start-index* **to** *end-index*	Specifies the index of a multicast group. *start-index* specifies the start index of a multicast group, and *end-index* specifies the end index of a multicast group.	The value is an integer that ranges from 1 to 1024.

Views

Multicast group list view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A multicast group is at the lowest level of the three-level control mechanism for controllable multicast. A multicast group corresponds to a multicast address such as 224.1.1.1. A multicast group can be regarded as a channel or program of IPTV. When configuring controllable multicast, you must create a multicast group and add the group to a multicast group list.

Prerequisites

The specified multicast group has been created.

Example

Add the multicast group named **test** to the multicast group list **list1**.

```
<HUAWEI> system-view
[HUAWEI] btv
[HUAWEI-btv] multicast-group test ip-address 225.1.1.1
[HUAWEI-btv] multicast-list list1
[HUAWEI-btv-list-list1] add multicast-group name test
```

Add the multicast groups whose indexes range from 2 to 4 to the multicast group list **list1**.

```
<HUAWEI> system-view
[HUAWEI] btv
```



```
[HUAWEI-btv] multicast-list list1
[HUAWEI-btv-list-list1] add multicast-group index 2 to 4
```

8.15.3 add multicast-list

Function

The **add multicast-list** command adds multicast group lists in a multicast profile.

The **undo add multicast-list** command removes multicast group lists from a multicast profile.

By default, no multicast group list is referenced in a multicast profile.

Format

add multicast-list { **name** *list-name* | **index** *start-index* **to** *end-index* } { **preview** | **watch** }

undo add multicast-list { **name** *list-name* | **index** *start-index* **to** *end-index* }

Parameters

Parameter	Description	Value
name *list-name*	Indicates the name of a multicast group list.	The value is a string of 1 to 31 case-insensitive characters without spaces.
index *start-index* **to** *end-index*	Specifies the index of a multicast group list. *start-index* specifies the start index of a multicast group list, and *end-index* specifies the end index of a multicast group list.	The value is an integer that ranges from 1 to 128.
preview	Indicates that multicast group lists are added to a multicast profile in preview mode. Users applying this profile can preview all programs in the multicast group lists.	-
watch	Indicates that multicast group lists are added to a multicast profile in watch mode. Users applying this profile can watch all programs in the multicast group lists.	-

Views

Multicast profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A multicast group list is in the middle of the three-level control mechanism for controllable multicast, and is a set of multicast groups. A multicast group list can contain multiple multicast groups. For example, multicast group list l1 contains g1, g2, g3, and g4. A multicast group can be contained in multiple multicast group lists. For example, g3 is contained in l1 and l2. When you configure controllable multicast, you must add the multicast group list to a multicast profile.

Prerequisites

The specified multicast group list has been created.

Example

Reference the multicast group list named **list1** in the multicast profile **profile1**.

```
<HUAWEI> system-view
[HUAWEI] btv
[HUAWEI-btv] multicast-list list1
[HUAWEI-btv-list-list1] quit
[HUAWEI-btv] multicast-profile profile1
[HUAWEI-btv-profile-profile1] add multicast-list name list1 watch
```

Reference the multicast group lists with indexes 1 to 10 in the multicast profile **profile1**.

```
<HUAWEI> system-view
[HUAWEI] btv
[HUAWEI-btv] multicast-profile profile1
[HUAWEI-btv-profile-profile1] add multicast-list index 1 to 10 watch
```

8.15.4 attach multicast-profile

Function

The **attach multicast-profile** command binds a multicast profile to a user.

The **undo attach multicast-profile** command cancels the binding between a multicast profile and a user.

By default, no multicast profile is bound to a user.

Format

attach multicast-profile *profile-name* [**interface** *interface-type interface-number* | **mac-address** *mac-address*] *

undo attach multicast-profile [*profile-name* [**interface** *interface-type interface-number* | **mac-address** *mac-address*] *]

Parameters

Parameter	Description	Value
profile-name	Specifies the name of a multicast profile.	The value is a string of 1 to 31 case-insensitive characters without spaces.
interface *interface-type interface-number*	Specifies a user interface. *interface-type* specifies the type of the user interface. *interface-number* specifies the number of the user interface.	-
mac-address *mac-address*	Specifies the MAC address of a user host.	The MAC address is in the format of H-H-H. Each H stands for four hexadecimal numbers.

Views

VLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Traditional multicast services are uncontrollable. User hosts send IGMP/MLD Report packets to join a specified multicast group. Then they can receive multicast packets of the group. With the development of IPTV services, uncontrollable multicast services cannot meet carriers' requirements. You can configure controllable multicast to authenticate user rights in the VLAN that join a multicast group. The controllable multicast function authenticates users in a VLAN that need to join a multicast group using the multicast group, multicast group list, and multicast profile. After a multicast profile is configured, bind this profile to a VLAN. When a user host sends a request to join a channel, the request is snooped if the channel requested by the user host is not in the multicast profile.

Prerequisites

The specified multicast profile has been created.

Precautions

The switch supports the port+VLAN multicast control mode. To configure the multicast service for multiple user interfaces in the same VLAN, you need to specify a multicast profile for each interface individually by specifying the **interface** *interface-type interface-number* parameter.

Example

Bind **profile1** to the user with the MAC address being 1-2-3 on GE0/0/1 in VLAN 4.

```
<HUAWEI> system-view
[HUAWEI] btv
[HUAWEI-btv] multicast-profile profile1
[HUAWEI-btv-profile-profile1] quit
[HUAWEI-btv] quit
[HUAWEI] vlan 4
[HUAWEI-vlan4] attach multicast-profile profile1 interface gigabitethernet 0/0/1 mac-address 1-2-3
```

8.15.5 btv

Function

The **btv** command enables controllable multicast and displays the BTV view.

The **undo btv** command disables controllable multicast and deletes all configurations in the BTV view.

By default, controllable multicast is disabled.

Format

btv

undo btv

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

The **btv** command allows you to configure controllable multicast in the BTV view.

NOTICE

The **undo btv** deletes all the controllable multicast configurations. Exercise caution when you run this command.

Example

Enter the BTV view.

```
<HUAWEI> system-view
[HUAWEI] btv
[HUAWEI-btv]
```

8.15.6 display multicast-group

Function

The **display multicast-group** command displays the configuration of a multicast group.

Format

display multicast-group [*group-name*]

Parameters

Parameter	Description	Value
group-name	Specifies the name of a multicast group.	The value is a string of 1 to 31 case-insensitive characters without spaces.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Using the **display multicast-group** command, you can view details about a specified multicast group, if *group-name* is specified. Otherwise, you can view brief information about all multicast groups.

Example

Display brief information about all multicast groups.

```
<HUAWEI> display multicast-group
-------------------------------------------------------------------------
Index       Multicast-group-name            Address
-------------------------------------------------------------------------
 1          g1                              232.0.0.1[10.1.1.1]
 2          g2                              232.0.0.2[10.2.1.1]

Total: 2
```


Display details about the multicast group named **g1**.

```
<HUAWEI> display multicast-group g1
 Multicast-group-name        : g1
 Address                     : 232.0.0.1[10.1.1.1]
 Referenced list :
       l1

 Total: 1
```

Table 8-152 Description of the **display multicast-group** command output

Item	Description
Index	Index of a multicast group
Multicast-group-name	Name of a multicast group
Address	Multicast group and source address
Referenced list	Multicast group list that a multicast group is added to
Total	Total number of multicast groups

8.15.7 display multicast-list

Function

The **display multicast-list** command displays the configuration of a multicast group list.

Format

display multicast-list [*list-name*]

Parameters

Parameter	Description	Value
list-name	Specifies the name of a multicast group list.	The value is a string of 1 to 31 case-insensitive characters without spaces.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

If you specify the name of a multicast group list in the **display multicast-list** command, detailed information about the specified multicast group list is displayed. If you do not specify a multicast group list in the command, the summary information about all multicast group lists is displayed.

Example

Display brief information about all multicast group lists.

```
<HUAWEI> display multicast-list
--------------------------------------------------------------------------
Index       Multicast-list-name           Multicast-group
--------------------------------------------------------------------------
 1          l1                            2

Total: 1
```

Display details about the multicast group list named **l1**.

```
<HUAWEI> display multicast-list l1
 Multicast-list-name : l1

 Referenced multicast-group (Total: 2)
      g1                        232.0.0.1[10.1.1.1]
      g2                        232.0.0.2[10.2.1.1]

 Referenced multicast-profile (Total: 2)
      p1                        [w]
      p2                        [w]
```

Table 8-153 Description of the **display multicast-list** command output

Item	Description
Index	Index of a multicast group list.
Multicast-list-name	Name of a multicast group list.
Multicast-group	Number of multicast groups contained in a multicast group list.
Referenced multicast-group	Multicast groups contained in a multicast group list. For example, g1 and 232.0.0.1 are the name and address of the multicast group, while 10.1.1.1 is a multicast source address.
Referenced multicast-profile	Profile that a multicast group list is added to. p1 is the name of the multicast profile. [w] means that the profile is in watching state, and [p] indicates that the profile is in preview state.

Item	Description
Total	• The first **Total** field indicates the total number of multicast group lists. • The second **Total** field indicates the number of multicast groups in the specified multicast group list. • The third **Total** field indicates the number of multicast profiles that references the multicast group list.

8.15.8 display multicast-profile

Function

The **display multicast-profile** command displays information about multicast profile.

Format

display multicast-profile [*profile-name* [**verbose**]]

Parameters

Parameter	Description	Value
profile-name	Specifies the name of a multicast profile.	The value is a string of 1 to 31 case-insensitive characters without spaces.
verbose	Indicates detailed information.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

If you specify *profile-name*, this command displays information about a specified multicast profile. If you do not specify *profile-name*, this command displays brief information about all multicast profiles.

Example

Display brief information about all multicast profiles.

```
<HUAWEI> display multicast-profile
--------------------------------------------------------------------------------
Index       Profile-Name                 Multicast-list  Attach-User
--------------------------------------------------------------------------------
 1          p1                           1               2
 2          p2                           2               2

Total: 2
```

Display detailed information about the multicast profile **p1**.

```
<HUAWEI> display multicast-profile p1 verbose
 Profile-name : p1
 Referenced multicast-group  (Total: 2)
      g1                          225.0.0.1       [w]
      g2                          225.0.0.2       [w]
```

Table 8-154 Description of the **display multicast-profile** command output

Item	Description
Index	Index of a multicast profile.
Profile-Name	Name of the multicast profile.
Multicast-list	Number of multicast group lists contained in the multicast profile.
Attach-User	Number of user VLANs that the multicast profile is bound to.
Referenced multicast-group	Number of multicast groups in the multicast profile. In this example, g1 is the multicast group name, 225.0.0.1 is the group address. [w] means that the profile is in watching state, and [p] indicates that the profile is in preview state.
Total	• The first **Total** field indicates the total number of multicast profiles. • The second **Total** field indicates the number of multicast groups in the specified multicast profile.

8.15.9 display multicast-profile-apply

Function

The **display multicast-profile-apply** command displays bindings between multicast profiles and VLANs.

Format

display multicast-profile-apply

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can use this command to check the multicast profiles applied to different VLANs.

Example

Display bindings between multicast profiles and VLANs on the switch.

```
<HUAWEI> display multicast-profile-apply
--------------------------------------------------------------------------------
 Vlan-id  Port                SMAC                    Max-Users
                Index           Profile-name
--------------------------------------------------------------------------------
 Vlan1    --                  --                      8
                1               p1
 Vlan2    --                  --                      8
                1               p1
 Vlan3    --                  --                      8
                2               p2
 Vlan4    --                  --                      8
                2               p2

Total: 4
```

Table 8-155 Description of the **display multicast-profile-apply** command output

Item	Description
Vlan-id	ID of a VLAN bound to a multicast profile.
Port	Interface in the VLAN. -- indicates that no interfaces are bound to the multicast profile in this VLAN.
Index	Index of a multicast profile.
SMAC	MAC address of a user. -- indicates that no user hosts are bound to the multicast profile in this VLAN.
Profile-name	Name of a multicast profile.

Item	Description
Max-Users	Maximum number of programs that users can watch and preview at the same time. If the value is set in a VLAN and the multicast profile bound to the VLAN, only the configuration in the VLAN takes effect. If the value is not set in a VLAN: • The configuration in the multicast profile takes effect if the VLAN is bound to only one multicast profile. • The default value 8 is used if the VLAN is bound to multiple multicast profiles.
Total	Total number of binding entries between VLANs and multicast profiles.

8.15.10 max-program-num (multicast profile view)

Function

The **max-program-num** command sets the maximum number of programs that users can receive simultaneously.

The **undo max-program-num** command restores the maximum number of programs for a user to the default value.

By default, users can receive a maximum of 8 programs simultaneously.

Format

max-program-num *max-value*

undo max-program-num [*max-value*]

Parameters

Item	Description	Value
max-value	Indicates the maximum number of programs that users can receive simultaneously.	The value ranges from 1 to 8.

Views

Multicast profile view

Default Level

2: Configuration level

Usage Guidelines

Run the **max-program-num (VLAN view)** command in the VLAN view to set the maximum number of multicast groups that users can simultaneously join. If the value is set in a VLAN and the multicast profile bound to the VLAN, only the configuration in the VLAN takes effect. If the value is not set in a VLAN:

- The configuration in the multicast profile takes effect if the VLAN is bound to only one multicast profile.
- The default value 8 is used if the VLAN is bound to multiple multicast profiles.

Example

Set the maximum number of programs that multicast profile **p1** allows users to receive simultaneously to 4.

```
<HUAWEI> system-view
[HUAWEI] btv
[HUAWEI-btv] multicast-profile p1
[HUAWEI-btv-profile-p1] max-program-num 4
```

8.15.11 max-program-num (VLAN view)

Function

The **max-program-num** command sets the maximum number of programs that users can receive simultaneously.

The **undo max-program-num** command restores the maximum number of programs for a user to the default value.

By default, users can receive a maximum of 8 programs simultaneously.

Format

max-program-num *max-value* [**interface** *interface-type interface-number* | **mac-address** *mac-address*] *

undo max-program-num [**interface** *interface-type interface-number* | **mac-address** *mac-address*] *

Parameters

Item	Description	Value
max-value	Indicates the maximum number of programs that users can receive simultaneously.	The value ranges from 1 to 8.

Item	Description	Value
interface *interface-type interface-number*	Indicates the maximum number of programs that users on a specified interface can watch simultaneously.	-
mac-address *mac-address*	Indicates the maximum number of programs that users with specified MAC addresses can watch simultaneously.	The value is in H-H-H format, in which H is a 4-digit hexadecimal number.

Views

VLAN view

Default Level

2: Configuration level

Usage Guidelines

Run the **max-program-num (multicast profile view)** command in the multicast profile view to set the maximum number of multicast groups that users can simultaneously join. If the value is set in a VLAN and the multicast profile bound to the VLAN, only the configuration in the VLAN takes effect. If the value is not set in a VLAN:

- The configuration in the multicast profile takes effect if the VLAN is bound to only one multicast profile.
- The default value 8 is used if the VLAN is bound to multiple multicast profiles.

The **interface** *interface-type interface-number* and **mac-address** *mac-address* parameters specified in the command must be the same as those specified in the **attach multicast-profile** command.

Example

Allow users in VLAN 10 to watch four programs simultaneously.

```
<HUAWEI> system-view
[HUAWEI] vlan 10
[HUAWEI-vlan10] max-program-num 4
```

8.15.12 multicast-group

Function

The **multicast-group** command creates a controllable multicast group.

The **undo multicast-group** command deletes a controllable multicast group.

By default, no multicast group is created.

Format

multicast-group *group-name* { **ip-address** *ipv4-group-address* [**source** *ipv4-source-address*] | **ipv6-address** *ipv6-group-address* [**source** *ipv6-source-address*] }

undo multicast-group { **all** | *group-name* | **index** *start-index* **to** *end-index* }

Parameters

Parameter	Description	Value
group-name	Specifies the name of a multicast group.	The value is a string of 1 to 31 case-insensitive characters without spaces.
ip-address *ipv4-group-address*	Specifies the address of a multicast group.	The value ranges from 224.0.1.0 to 239.255.255.255 in dotted decimal notation.
source *ipv4-source-address*	Specifies an IPv4 source address.	It is in dotted decimal notation.
ipv6-address *ipv6-group-address*	Specifies an IPv6 multicast group address.	The address is a 32-digit hexadecimal number, in the format X:X:X:X:X:X:X:X. The value ranges from FF00:: to FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF, excluding the multicast addresses reserved for protocols.
source *ipv6-source-address*	Specifies an IPv6 source address.	The address is a 32-digit hexadecimal number, in the format X:X:X:X:X:X:X:X.
all	Deletes all multicast groups.	-
index *start-index* **to** *end-index*	Specifies the index of a multicast group. *start-index* specifies the start index of a multicast group, and *end-index* specifies the end index of a multicast group.	The value is an integer that ranges from 1 to 1024.

Views

Broadband TV (BTV) view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A multicast group is at the lowest level of the three-level control mechanism for controllable multicast. A multicast group corresponds to a multicast address such as 224.1.1.1. A multicast group can be regarded as a channel or program of IPTV.

Precautions

If two programs have the same multicast IP address but different source addresses, the two programs are considered different.

Example

Configure the IP address of a multicast group to 225.0.0.1 and name the multicast program **tv-1**.

```
<HUAWEI> system-view
[HUAWEI] btv
[HUAWEI-btv] multicast-group tv-1 ip-address 225.0.0.1
```

Configure the IP address of a multicast group to ff1e::1234 and name the multicast program **tv-2**.

```
<HUAWEI> system-view
[HUAWEI] btv
[HUAWEI-btv] multicast-group tv-2 ipv6-address ff1e::1234
```

Configure the IP address of a multicast group to 232.0.0.1, specify the source IP address to 192.168.1.1, and name the multicast program **tv-3**.

```
<HUAWEI> system-view
[HUAWEI] btv
[HUAWEI-btv] multicast-group tv-3 ip-address 232.0.0.1 source 192.168.1.1
```

8.15.13 multicast-list

Function

The **multicast-list** command creates a multicast group list.

The **undo multicast-list** command deletes a multicast group list.

By default, no multicast group list is configured.

Format

multicast-list *list-name*

undo multicast-list { *list-name* | **index** *start-index* **to** *end-index* | **all** }

Parameters

Parameter	Description	Value
list-name	Specifies the name of a multicast group list.	The value is a string of 1 to 31 case-insensitive characters without spaces.
index *start-index* **to** *end-index*	Specifies the index of a multicast group list. *start-index* specifies the start index of a multicast group, and *end-index* specifies the end index of a multicast group.	The value is an integer that ranges from 1 to 128.
all	Deletes all multicast group lists.	-

Views

BTV view

Default Level

2: Configuration level

Usage Guidelines

A multicast group list is in the middle of the three-level control mechanism for controllable multicast, and is a set of multicast groups. A multicast group list can contain multiple multicast groups. For example, multicast group list L1 contains G1, G2, G3, and G4. A multicast group can be contained in multiple multicast group lists. For example, G3 is contained in L1 and L2. When you configure controllable multicast, you must add the multicast group list to a multicast profile.

Using the **multicast-list** command, you can create a multicast group list and enter the multicast group list view. If a multicast group list is already created, you can directly enter the multicast group list view.

Example

Create the multicast group list named **list1**.

```
<HUAWEI> system-view
[HUAWEI] btv
[HUAWEI-btv] multicast-list list1
[HUAWEI-btv-list-list1]
```


8.15.14 multicast-preview interval

Function

The **multicast-preview interval** command sets the interval between the first and second previews on a multicast group.

The **undo multicast-preview interval** command restores the default interval between the first and second previews on a multicast group.

By default, the interval between the first and second previews on a multicast group is 5 minutes.

Format

multicast-preview interval *interval*

undo multicast-preview interval [*interval*]

Parameters

Parameter	Description	Value
interval	Specifies the interval between the first and second previews on a multicast group.	The value is an integer that ranges from 1 to 30, in minutes.

Views

Multicast profile view

Default Level

2: Configuration level

Usage Guidelines

Controllable multicast allows users to preview programs. The **multicast-preview interval** command sets the interval between the first and second previews. Users can preview the same program after this interval.

Example

Set the interval between the first and second previews on a multicast profile named **profile1** to 15 minutes.

```
<HUAWEI> system-view
[HUAWEI] btv
[HUAWEI-btv] multicast-profile profile1
[HUAWEI-btv-profile-profile1] multicast-preview interval 15
```


8.15.15 multicast-preview minutes

Function

The **multicast-preview minutes** command sets the period for a user to preview a multicast group each time.

The **undo multicast-preview minutes** command restores the default preview period.

By default, the period for a user to preview a multicast group each time is 5 minutes.

Format

multicast-preview minutes *minutes*

undo multicast-preview minutes [*minutes*]

Parameters

Parameter	Description	Value
minutes	Specifies the period for a user to preview a multicast group each time.	The value is an integer that ranges from 1 to 10, in minutes.

Views

Multicast profile view

Default Level

2: Configuration level

Usage Guidelines

Controllable multicast allows users to preview programs. The **multicast-preview minutes** command sets the period for a user to preview a multicast group. Users are not allowed to preview the program after the configured period is reached.

Example

Set the period for previewing the multicast profile named **profile1** each day to 9 minutes.

```
<HUAWEI> system-view
[HUAWEI] btv
[HUAWEI-btv] multicast-profile profile1
[HUAWEI-btv-profile-profile1] multicast-preview minutes 9
```


8.15.16 multicast-preview times

Function

The **multicast-preview times** command sets the number of times for a user to preview a multicast group each day.

The **undo multicast-preview times** command restores the default number of previews each day.

By default, the number of times a user can preview a multicast group each day is 10.

Format

multicast-preview times *times*

undo multicast-preview times [*times*]

Parameters

Parameter	Description	Value
times	Specifies the number of times for a user to preview a multicast group each day.	The value is an integer that ranges from 1 to 10.

Views

Multicast profile view

Default Level

2: Configuration level

Usage Guidelines

Controllable multicast allows users to preview programs. The **multicast-preview times** command sets the number of times for a user to preview a multicast group each day.

Example

Set the number of times for a user to preview the multicast profile named **profile1** each day to 8.

```
<HUAWEI> system-view
[HUAWEI] btv
[HUAWEI-btv] multicast-profile profile1
[HUAWEI-btv-profile-profile1] multicast-preview times 8
```


8.15.17 multicast-profile

Function

The **multicast-profile** command creates a multicast profile and enters the multicast profile view. If a multicast profile is already created, you can directly enter the multicast profile view.

The **undo multicast-profile** command deletes a multicast profile.

By default, no multicast profile is configured.

Format

multicast-profile *profile-name*

undo multicast-profile { *profile-name* | **index** *start-index* **to** *end-index* | **all** }

Parameters

Parameter	Description	Value
profile-name	Specifies the name of a multicast profile.	The value is a string of 1 to 31 case-insensitive characters without spaces.
index *start-index* **to** *end-index*	Specifies the index of a multicast profile. *start-index* specifies the start index of a multicast profile, and *end-index* specifies the end index of a multicast profile.	The value is an integer that ranges from 1 to 64.
all	Deletes all multicast profiles.	-

Views

BTV view

Default Level

2: Configuration level

Usage Guidelines

A multicast profile is a set of multicast group lists, and it defines user rights to join related multicast groups. A multicast profile can contain multiple multicast group lists. For example, multicast profile P1 contains L1, L2, and L3. A multicast group list can be contained in several multicast profiles. For example, L2 is contained in

P1 and P2. Multicast group lists that are added to a profile have their attributes, that is, preview or watch. If a multicast group list is added to a multicast profile in watch mode, users bound to the multicast profile can watch all multicast groups in the list. If a multicast group list is added to a multicast profile in preview mode, users bound to the multicast profile can only preview all multicast groups in the list.

Example

Create the multicast profile named **profile1** and enter the multicast profile view.

```
<HUAWEI> system-view
[HUAWEI] btv
[HUAWEI-btv] multicast-profile profile1
[HUAWEI-btv-profile-profile1]
```

8.16 Multicast Network Management Commands

8.16.1 Command Support

Commands provided in this section and all the parameters in the commands are supported by all switch models (except the S5731-L and S5731S-L), unless otherwise specified. For details, see specific commands.

8.16.2 display multicast threshold-alarm

Function

The **display multicast threshold-alarm** command displays the alarm thresholds for multicast entry resource usage.

Format

display multicast threshold-alarm

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can use this command to check the alarm thresholds for multicast entry resource usage.

Example

Display the alarm thresholds for multicast entry resource usage.

```
<HUAWEI> display multicast threshold-alarm
Multicast table trap threshold value
Upperlimit value: 86%
Lowerlimit value: 78%
```

Table 8-156 Description of the **display multicast threshold-alarm** command output

Item	Description
Multicast table trap threshold value	Alarm thresholds for multicast entry resource usage.
Upperlimit value	Upper threshold value. This parameter is configured using the **multicast threshold-alarm upper-limit** *upper-limit* **lower-limit** *lower-limit* command.
Lowerlimit value	Lower threshold value. This parameter is configured using the **multicast threshold-alarm upper-limit** *upper-limit* **lower-limit** *lower-limit* command.

8.16.3 display pim mib-control-message

Function

The **display pim mib-control-message** command displays PIM-related statistics and counts of various messages received the last time.

Format

display pim mib-control-message { **counters** | **join-prune** | **assert** | **register** }

NOTE

Only the S5720I-SI, S5720-LI, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5720S-LI, S5735-S, S500, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6720S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Parameters

Parameter	Description	Value
counters	Indicates related PIM counters.	-

Parameter	Description	Value
join-prune	Indicates the number of invalid Join/Prune messages that are received at the last time.	-
assert	Indicates the number of Assert messages that are received or sent at the last time.	-
register	Indicates the number of invalid Register messages that are received at the last time.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The **display pim mib-control-message counters** command displays the number of neighbor loss events, the number of DR elections, the number of invalid Join/Prune messages, the number of invalid Register messages, the number of RP-mapping changes, and the number of received and sent Assert messages.

The **display pim mib-control-message join-prune** command displays the source address, group address, and RP address carried in the last received invalid Join/Prune message.

The **display pim mib-control-message assert** command displays the source address and group address carried in the last received or sent Assert message.

The **display pim mib-control-message register** command displays the source address, group address, and RP address carried in the last received invalid Register message.

Example

Display the number of neighbor loss events, the number of times for DR election, the number of invalid Join/Prune messages, the number of invalid Register messages, the number of RP-Mapping, the number of received and sent Assert messages.

```
<HUAWEI> display pim mib-control-message counters
 pim mib-control-message counters
 Neighbor-loss (times)        : 0
 DR-Election(times)           : 0
 Invalid-join-prune (times)   : 0
 RP-Mapping (times)           : 0
 Invalid-register (times)     : 0
 Assert-received(times)       : 0
 Assert-send(times)           : 0
```

Display the invalid Join/Prune message that is received at the last time.


```
<HUAWEI> display pim mib-control-message join-prune
The last invalid join-prune message received information:
Group address  : 225.1.1.1
Source address : 0.0.0.0
RP address     : 10.0.5.5
```

Display the Assert message that is sent or received at the last time. If the interface that receives or sends the Assert message is pulled out when this command is used, the prompt that "The last assert message was received or sent on lost interface" is displayed.

```
<HUAWEI> display pim mib-control-message assert
The last assert message received or sent on Vlanif100
Group address   : 226.3.3.3
Source address  : 10.0.5.55
```

Display the invalid Register message that is received at the last time.

```
<HUAWEI> display pim mib-control-message register
The last invalid register message received information:
Group address  : 225.1.1.1
Source address : 10.0.5.100
RP address     : 10.0.3.1
```

Table 8-157 Description of the **display pim mib-control-message** command output

Item	Description
pim mib-control-message counters	Numbers of neighbor loss events, DR election events, invalid Join/Prune messages, invalid Register messages, RP-mapping changes, and received and sent Assert messages.
The last invalid join-prune message received information	Invalid Join/Prune message received the last time.
The last assert message received or sent on Vlanif100	Assert message sent or received the last time.
The last invalid register message received information	Invalid Register message received the last time.
Neighbor-loss(times)	Number of neighbor loss events.
DR-Election (times)	Number of DR election events.
Invalid-join-prune(times)	Number of invalid Join/Prune messages.
RP-Mapping(times)	Number of RP-Mapping changes.
Invalid-register(times)	Number of invalid Register messages.
Assert-received(times)	Number of received Assert messages.
Assert-send(times)	Number of sent Assert messages.
Group address	Multicast group address.
Source address	Multicast source address

Item	Description
RP address	IP address of the RP.

8.16.4 display pim mib-notification interval

Function

The **display pim mib-notification interval** command displays the interval for sending PIM notification messages.

Format

display pim mib-notification interval

NOTE

Only the S5720I-SI, S5720-LI, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5720S-LI, S5735-S, S500, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6720S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After the interval for sending PIM notification messages is set or modified by using the **pim mib-notification interval** command, you can run the **display pim mib-notification interval** command to view the configured interval.

Example

Display the interval for sending PIM notification messages.

```
<HUAWEI> display pim mib-notification interval
Neighbor-loss notification interval      : 0 s
Invalid-join-prune notification interval : 50 s
RP-mapping-change notification interval  : 100 s
Interface-election notification interval : 2000 s
Invalid-register notification interval   : 60000 s
New-neighbor notification interval       : 0 s
Mrt-limit notification interval          : never
```


Table 8-158 Description of the **display pim mib-notification interval** command output

Item	Description
Neighbor-loss notification interval	Interval for sending the notification messages about the neighbor loss
Invalid-join-prune notification interval	Interval for sending the notification messages about invalid Join/Prune messages
RP-mapping-change notification interval	Interval for sending the notification messages about RP-mapping changes
Interface-election notification interval	Interval for sending the notification messages about interface election
Invalid-register notification interval	Interval for sending the notification messages about invalid Register messages
New-neighbor notification interval	Interval for sending trap messages about neighbor addition.
Mrt-limit notification interval	Interval for sending trap messages about the failure in joining multicast groups because the number of PIM entries reaches the upper limit.

8.16.5 igmp trap-interval limit

Function

The **igmp trap-interval limit** command configures the interval for sending trap messages on failures to join IGMP groups because the number of the IGMP entries exceeds the limit.

The **undo igmp trap-interval limit** command deletes the interval for sending trap messages on failures to join IGMP groups because the number of the IGMP entries exceeds the limit. When a group joining failure occurs, a trap message is sent immediately.

By default, a trap message is sent immediately when an IGMP group joining failure occurs because the number of the IGMP entries exceeds the limit.

Format

igmp trap-interval limit *min-interval*

undo igmp trap-interval limit

NOTE

Only the S5720I-SI, S5720-LI, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5720S-LI, S5735-S, S500, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6720S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Parameters

Parameter	Description	Value
min-interval	Specifies the interval for sending trap messages of the failure of IGMP joining because the number of the IGMP entries exceeds the limit.	The value is an integer that ranges from 0 to 65535, in seconds. The default value is 0 seconds.

Views

Multicast MIB view

Default Level

2: Configuration level

Usage Guidelines

If the interval is set to 0, a trap message will be sent immediately when an IGMP group joining failure occurs because the number of the IGMP entries exceeds the limit; otherwise, the interval for sending such trap messages should be equal to or longer than the configured one.

Example

Set the interval for sending trap messages on failures to join IGMP groups because the number of the IGMP entries exceeds the limit to 50 seconds.

```
<HUAWEI> system-view
[HUAWEI] multicast-mib
[HUAWEI-mcast-mib] igmp trap-interval limit 50
```

8.16.6 mgmd total-number threshold-alarm

Function

The **mgmd total-number threshold-alarm** command sets the upper and lower alarm thresholds for IGMP/MLD entries.

The **undo mgmd total-number threshold-alarm** command restores the default alarm thresholds for IGMP/MLD entries.

By default, the upper and lower alarm thresholds are 80% and 75% respectively.

Format

mgmd total-number threshold-alarm upper-limit *upper-limit-value* **lower-limit** *lower-limit-value*

undo mgmd total-number threshold-alarm

NOTE

Only the S5720I-SI, S5720-LI, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5720S-LI, S5735-S, S500, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6720S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Parameters

Parameter	Description	Value
upper-limit *upper-limit-value*	Specifies the upper alarm threshold for IGMP/MLD entries, in percentage.	The value is an integer ranging from 1 to 100.
lower-limit *lower-limit-value*	Specifies the lower alarm threshold for IGMP/MLD entries, in percentage.	The value is an integer ranging from 1 to 100. *lower-limit-value* must be smaller than *upper-limit-value*.

Views

Multicast MIB view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A device supports a limited number of IGMP/MLD entries. After the number of IGMP/MLD entries reaches the maximum value, no more IGMP/MLD entries can be created. As a result, some multicast traffic cannot be forwarded. To facilitate network operation and maintenance, configure the upper and lower alarm thresholds for IGMP/MLD entries. IGMP/MLD entry alarms and clear alarms quickly notify you of IGMP/MLD entry usage. The **mgmd total-number threshold-alarm** command allows you to flexibly adjust the alarm thresholds for IGMP/MLD entries based on service requirements. Note that:

- If the proportion of existing IGMP/MLD entries to the maximum number reaches *upper-limit-value*, an IGMP/MLD entry alarm is reported for all VPN instances. This alarm is informational only and does not affect creation of new IGMP/MLD entries.

- If the proportion of existing IGMP/MLD entries to the maximum number falls below *lower-limit-value*, an IGMP/MLD entry clear alarm is reported for all VPN instances.

Prerequisites

This command only configures the alarm thresholds for IGMP/MLD entries. To enable the configured alarm thresholds to take effect, run the **snmp-agent trap enable feature-name igmp trap-name** { **hwmgmdtotallimitthresholdexceed** | **hwmgmdtotallimitthresholdexceedclear** } command twice to enable the device to report IGMP/MLD entry alarms and clear alarms.

Precautions

If the **mgmd total-number threshold-alarm** command is executed multiple times, only the latest configuration takes effect.

Example

Configure the upper and lower alarm thresholds for IGMP/MLD entries.

```
<HUAWEI> system-view
[HUAWEI] multicast-mib
[HUAWEI-mcast-mib] mgmd total-number threshold-alarm upper-limit 88 lower-limit 77
```

8.16.7 mgmd host threshold-alarm

Function

The **mgmd host threshold-alarm** command configures the upper and lower alarm thresholds for the multicast entry usage of all instances on a user-side IGMP/MLD device.

The **undo mgmd host threshold-alarm** command restores the default upper and lower alarm thresholds.

By default, the upper and lower alarm thresholds are 80% and 75%, respectively.

Format

mgmd host { **star-group-number** | **source-group-number** } **threshold-alarm upper-limit** *upper-limit-value* **lower-limit** *lower-limit-value*

undo mgmd host { **star-group-number** | **source-group-number** } **threshold-alarm**

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Parameters

Parameter	Description	Value
star-group-number	Enables you to configure the upper and lower alarm thresholds for the (*, G) entry usage of all instances.	-
source-group-number	Enables you to configure the upper and lower alarm thresholds for the (S, G) entry usage of all instances.	-
upper-limit *upper-limit-value*	Configures an upper alarm threshold for the multicast entry usage of all instances, in percentage.	The value is an integer ranging from 1 to 100.
lower-limit *lower-limit-value*	Configures a lower alarm threshold for the multicast entry usage of all instances, in percentage.	The value is an integer ranging from 1 to 100. *lower-limit-value* must be smaller than *upper-limit-value*.

Views

Multicast MIB view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A user-side IGMP/MLD device has an upper limit for the number of multicast entries. When this upper limit is reached, the device cannot create new entries, so it will reject new multicast service requests. To resolve this issue and improve device maintenance, run the **mgmd host threshold-alarm** command to configure the upper and lower alarm thresholds for the multicast entry usage on a user-side IGMP/MLD device, enabling you to learn the multicast entry usage status. After the **mgmd host threshold-alarm** command is executed:

- When the value of *upper-limit-value* is reached, the device triggers a multicast entry usage alarm. Such an alarm is a notification only, and the device can still create new multicast entries before the multicast entry usage reaches 100%.
- When the multicast entry usage falls below the value specified by *lower-limit-value*, the device triggers a clear alarm for the multicast entry usage alarm.

Prerequisites

The **mgmd host threshold-alarm** command works with the **snmp-agent trap enable feature-name igmp trap-name** { **hwmgmdhoststargthresholdexceed** | **hwmgmdhoststargthresholdexceedclear** | **hwmgmdhostsgthresholdexceed** | **hwmgmdhostsgthresholdexceedclear** } command. The former configures the upper and lower alarm thresholds, while the latter enables or disables the function to report alarms.

Precautions

If the **mgmd host threshold-alarm** command is run more than once, the latest configuration overrides the previous one.

Example

Configure the upper and lower alarm thresholds for the (*, G) entry usage of all instances.

```
<HUAWEI> system-view
[HUAWEI] multicast-mib
[HUAWEI-mcast-mib] mgmd host star-group-number threshold-alarm upper-limit 88 lower-limit 77
```

Configure the upper and lower alarm thresholds for the (S, G) entry usage of all instances.

```
<HUAWEI> system-view
[HUAWEI] multicast-mib
[HUAWEI-mcast-mib] mgmd host source-group-number threshold-alarm upper-limit 88 lower-limit 77
```

8.16.8 multicast forwarding-table source-group-number threshold-alarm

Function

The **multicast forwarding-table source-group-number threshold-alarm** command configures the upper and lower alarm thresholds for multicast forwarding entries.

The **undo multicast forwarding-table source-group-number threshold-alarm** command restores the default alarm thresholds for multicast forwarding entries.

By default, the upper and lower alarm thresholds are 80% and 75% respectively.

Format

multicast forwarding-table source-group-number threshold-alarm upper-limit *upper-limit-value* **lower-limit** *lower-limit-value*

undo multicast forwarding-table source-group-number threshold-alarm

NOTE

Only the S5720I-SI, S5720-LI, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5720S-LI, S5735-S, S500, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6720S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Parameters

Parameter	Description	Value
upper-limit *upper-limit-value*	Specifies the upper alarm threshold for multicast forwarding entries, in percentage.	The value is an integer ranging from 1 to 100.
lower-limit *lower-limit-value*	Specifies the lower alarm threshold for multicast forwarding entries, in percentage.	The value is an integer ranging from 1 to 100. *lower-limit-value* must be smaller than *upper-limit-value*.

Views

Multicast MIB view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A device supports a limited number of multicast forwarding entries. After the number of multicast forwarding entries reaches the maximum value, no more multicast forwarding entries can be created. As a result, some multicast traffic cannot be forwarded. To facilitate network operations and maintenance, configure the upper and lower alarm thresholds for multicast forwarding entries. Multicast forwarding entry alarms and clear alarms quickly notify you of IGMP/MLD entry usage. The **multicast forwarding-table source-group-number threshold-alarm** command allows you to flexibly adjust the alarm thresholds for multicast forwarding entries based on service requirements. Note that:

- If the proportion of existing multicast forwarding entries to the maximum number reaches *upper-limit-value*, a multicast forwarding entry alarm is reported. This alarm is informational only and does not affect creation of new multicast forwarding entries.
- If the proportion of existing multicast forwarding entries to the maximum number falls below *lower-limit-value*, a multicast forwarding entry clear alarm is reported.

Prerequisites

This command only configures the alarm thresholds for multicast forwarding entries. To enable the configured alarm thresholds to take effect, run the **snmp-agent trap enable feature-name mrm trap-name** { **hwipmcastsgthresholdexceed** | **hwipmcastsgthresholdexceedclear** } command twice to enable the device to report multicast forwarding entry alarms and clear alarms.

Precautions

If the **multicast forwarding-table source-group-number threshold-alarm** command is executed multiple times, only the latest configuration takes effect.

Example

Configure the upper and lower alarm thresholds for multicast forwarding entries.

```
<HUAWEI> system-view
[HUAWEI] multicast-mib
[HUAWEI-mcast-mib] multicast forwarding-table source-group-number threshold-alarm upper-limit 88 lower-limit 77
```

8.16.9 multicast mib-notification join-leave frequency

Function

The **multicast mib-notification join-leave frequency** command sets the maximum number of trap messages sent by the system per second when IGMP/MLD joining or leaving events occur.

The **undo multicast mib-notification join-leave frequency** command restores the default number of trap messages sent by the system per second when IGMP/MLD joining or leaving events occur.

By default, the system does not send any trap message when IGMP/MLD joining or leaving events occur.

Format

multicast mib-notification join-leave frequency *count*

undo multicast mib-notification join-leave frequency

NOTE

Only the S5720I-SI, S5720-LI, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5720S-LI, S5735-S, S500, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6720S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Parameters

Parameter	Description	Value
count	Specifies the maximum number of trap messages sent by the system per second when IGMP/MLD joining or leaving events occur.	The value is an integer that ranges from 0 to 240. The unit is in packets per second. The default value is 0.

Views

Multicast MIB view

Default Level

2: Configuration level

Usage Guidelines

If network administrators need to know which receivers join or leave multicast groups in real time, run this command. The switch will send trap messages after receivers join or leave multicast groups.

Example

Set the maximum number of trap messages sent by the system per second to 30 when IGMP/MLD joining or leaving events occur.

```
<HUAWEI> system-view
[HUAWEI] multicast-mib
[HUAWEI-mcast-mib] multicast mib-notification join-leave frequency 30
```

8.16.10 multicast-mib

Function

The **multicast-mib** command enables the multicast MIB and displays the multicast MIB view.

The **undo multicast-mib** command deletes all configurations in the multicast MIB view.

By default, the multicast MIB is not enabled.

Format

multicast-mib

undo multicast-mib

NOTE

Only the S5720I-SI, S5720-LI, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5720S-LI, S5735-S, S500, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6720S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Run the **undo multicast-mib** command to delete all configurations in the multicast MIB view.

NOTICE

When using the **undo multicast-mib** command, you need to enter Y or N to confirm the action. This command will clear global multicast MIB configurations. So, use this command with caution.

Example

Enable multicast MIB and enter the multicast MIB view.

```
<HUAWEI> system-view
[HUAWEI] multicast-mib
[HUAWEI-mcast-mib]
```

8.16.11 multicast threshold-alarm

Function

The **multicast threshold-alarm** command configures an alarm threshold for the usage of multicast entry resources.

The **undo multicast threshold-alarm** command restores the default alarm threshold for the usage of multicast entry resources.

By default, the upper and lower alarm thresholds are 85% and 75% respectively.

Format

multicast threshold-alarm upper-limit *upper-limit* **lower-limit** *lower-limit*

undo multicast threshold-alarm

Parameters

Parameter	Description	Value
upper-limit *upper-limit*	Indicates the upper threshold for the usage of multicast entry resources.	The value is an integer that ranges from 2 to 100, in percentage.
lower-limit *lower-limit*	Indicates the lower threshold for the usage of multicast entry resources.	The value is an integer that ranges from (*upper-limit* - 10) to (*upper-limit* - 1), in percentage.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Multicast packets are forwarded based on multicast forwarding entries no matter whether the Layer 2 or Layer 3 multicast mode is used. A high entries resource usage indicates that the switch has forwarded too many multicast packets and there is a heavy load on it. If the resources for multicast forwarding entries are used up, multicast packets cannot be forwarded.

After the alarm threshold is set, the switch sends a trap when entries resource usage reaches the threshold. You can monitor multicast entries resource usage. When entries resource usage reaches the upper threshold, the alarm 1.3.6.1.4.1.2011.5.25.227.2.1.8, 1.3.6.1.4.1.2011.5.25.227.2.1.10, or 1.3.6.1.4.1.2011.5.25.227.2.1.62 is generated, indicating that the entries resources will be used up. When entries resource usage falls below the lower threshold, the alarm 1.3.6.1.4.1.2011.5.25.227.2.1.9, 1.3.6.1.4.1.2011.5.25.227.2.1.11, or 1.3.6.1.4.1.2011.5.25.227.2.1.63 is generated, indicating that entries resource usage is restored to an acceptable range.

Example

Set the upper threshold to 80% and lower threshold to 70%.

```
<HUAWEI> system-view
[HUAWEI] multicast threshold-alarm upper-limit 80 lower-limit 70
```

8.16.12 pim mib-notification interval

Function

The **pim mib-notification interval** command sets the interval for sending trap messages about various PIM events.

The **undo pim mib-notification interval** command restores the default interval for sending trap messages about various PIM events.

By default, an alarm is generated only when a neighbor loss event or a neighbor addition event occurs. No alarm is generated when the other events occur.

Format

pim mib-notification interval { **interface-election-dr** *election-value* | **invalid-join-prune** *jp-value* | **invalid-register** *register-value* | **neighbor-loss** *loss-value* | **new-neighbor** *new-value* | **rp-mapping-change** *change-value* | **mrt-limit** *mrt-value* }

undo pim mib-notification interval { **all** | **interface-election-dr** | **invalid-join-prune** | **invalid-register** | **neighbor-loss** | **new-neighbor** | **rp-mapping-change** | **mrt-limit** }

NOTE

Only the S5720I-SI, S5720-LI, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5720S-LI, S5735-S, S500, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6720S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Parameters

Parameter	Description	Value
interface-election-dr *election-value*	Specifies the minimum interval for sending trap messages about DR election.	The value is an integer that ranges from 0 to 65535, in seconds. The default value is 65535 seconds.
invalid-join-prune *jp-value*	Specifies the minimum interval for sending trap messages about invalid Join/Prune messages.	The value is an integer that ranges from 10 to 65535, in seconds. The default value is 65535 seconds.
invalid-register *register-value*	Specifies the minimum interval for sending trap messages about invalid Register messages.	The value is an integer that ranges from 10 to 65535, in seconds. The default value is 65535 seconds.
neighbor-loss *loss-value*	Specifies the minimum interval for sending trap messages about neighbor loss.	The value is an integer that ranges from 0 to 65535, in seconds. The default value is 0 seconds.
new-neighbor *new-value*	Specifies the minimum interval for sending trap messages about neighbor addition.	The value is an integer that ranges from 0 to 65535, in seconds. The default value is 0 seconds.
rp-mapping-change *change-value*	Specifies the minimum interval for sending trap messages about the RP-mapping change.	The value is an integer that ranges from 0 to 65535, in seconds. The default value is 65535 seconds.
mrt-limit *mrt-value*	Specifies the minimum interval for sending trap messages about the failure in joining multicast groups because the number of PIM entries reaches the upper limit.	The value is an integer that ranges from 10 to 65535, in seconds. By default, the value is 65535 seconds.

Parameter	Description	Value
all	Restore the default interval for PIM to send all trap messages.	-

Views

Multicast MIB view

Default Level

2: Configuration level

Usage Guidelines

The **pim mib-notification interval** command sets the interval for sending trap messages. When an event occurs but the period from when the last trap message was sent to the current time is shorter than the configured interval, the system does not send any trap message.

- If the default interval is 0, a trap message is sent immediately after an event occurs.
- If the default interval is 65535, no trap message is sent after an event occurs. In this case, run this command to adjust the interval to a smaller value so that a trap message can be sent after an event occurs.

Example

Set the interval for PIM to send trap messages about invalid Join/Prune messages.

```
<HUAWEI> system-view
[HUAWEI] multicast-mib
[HUAWEI-mcast-mib] pim mib-notification interval invalid-join-prune 50
```

8.16.13 pim threshold-alarm

Function

The **pim threshold-alarm** command configures the upper and lower alarm thresholds for PIM entries.

The **undo pim threshold-alarm** command restores the default alarm thresholds for PIM entries.

By default, the upper and lower alarm thresholds are 80% and 75% respectively.

Format

pim { **star-group-number** | **source-group-number** } **threshold-alarm upper-limit** *upper-limit-value* **lower-limit** *lower-limit-value*

undo pim { **star-group-number** | **source-group-number** } **threshold-alarm**

NOTE

Only the S5720I-SI, S5720-LI, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5720S-LI, S5735-S, S500, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6720S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Parameters

Parameter	Description	Value
star-group-number	Sets the alarm thresholds for PIM (*, G) entries.	-
source-group-number	Sets the alarm thresholds for PIM (S, G) entries.	-
upper-limit *upper-limit-value*	Specifies the upper alarm threshold value for PIM entries, in percentage.	The value is an integer ranging from 1 to 100.
lower-limit *lower-limit-value*	Specifies the lower alarm threshold value for PIM entries, in percentage.	The value is an integer ranging from 1 to 100. *lower-limit-value* must be smaller than *upper-limit-value*.

Views

Multicast MIB view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A device supports a limited number of PIM entries. After the number of PIM entries reaches the maximum value, no more PIM entries can be created. As a result, some multicast traffic cannot be forwarded. To facilitate network operations and maintenance, configure the upper and lower alarm thresholds for PIM entries. PIM entry alarms and clear alarms quickly notify you of PIM entry usage. The **pim threshold-alarm** command allows you to adjust the alarm thresholds for PIM entries based on service requirements. Note that:

- If the proportion of existing PIM entries to the maximum number reaches *upper-limit-value*, a PIM entry alarm is reported. This alarm is informational only and does not affect creation of new PIM entries.
- If the proportion of existing PIM entries to the maximum number falls below *lower-limit-value*, a PIM entry clear alarm is reported.

Prerequisites

This command only configures the alarm thresholds for PIM entries. To enable the configured alarm thresholds to take effect, run the **snmp-agent trap enable feature-name pim trap-name** { **hwpimsgthresholdexceed** | **hwpimsgthresholdexceedclear** | **hwpimstargthresholdexceed** | **hwpimstargthresholdexceedclear** } command twice to enable the device to report PIM entry alarms and clear alarms.

Precautions

If the **pim threshold-alarm** command is executed multiple times, only the latest configuration takes effect.

Example

Configure the upper and lower alarm thresholds for PIM (*, G) entries.

```
<HUAWEI> system-view
[HUAWEI] multicast-mib
[HUAWEI-mcast-mib] pim star-group-number threshold-alarm upper-limit 88 lower-limit 77
```

Configure the upper and lower alarm thresholds for PIM (S, G) entries.

```
<HUAWEI> system-view
[HUAWEI] multicast-mib
[HUAWEI-mcast-mib] pim source-group-number threshold-alarm upper-limit 88 lower-limit 77
```

