10 IP Multicast Commands

About This Chapter

10.1 IGMP Configuration Commands
10.2 MLD Configuration Commands
10.3 PIM (IPv4) Configuration Commands
10.4 PIM (IPv6) Configuration Commands
10.5 MSDP Configuration Commands
10.6 Multicast VPN (IPv4) Configuration Commands in Rosen Mode
10.7 Multicast Route Management (IPv4) Commands
10.8 Multicast Route Management (IPv6) Commands
10.9 IGMP Snooping Configuration Commands
10.10 MLD Snooping Configuration Commands
10.11 Multicast Network Management Commands

10.1 IGMP Configuration Commands

10.1.1 display default-parameter igmp

Function

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

Format

display default-parameter igmp

 Copyright © Huawei Technologies Co., Ltd.

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 10-1 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.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
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.
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	Whether SSM mapping is enabled. SSM mapping is enabled 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.

Copyright © Huawei Technologies Co., Ltd.

Item	Description
Group-policy	Whether a multicast group filtering policy is configured. A multicast group filtering 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.
Other-querier-present-timer-expiry	Status of the other querier present timer. The value **off** indicates that the interface considers itself as a querier and that no other queriers exist.
Prompt-leave	Whether the fast leave function is configured. The fast leave 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. 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	Whether to filter IGMP Report/Leave messages based on host addresses. This function is configured using the **igmp ip-source-policy** command.

Related Topics

10.1.17 igmp group-policy
10.1.18 igmp ip-source-policy
10.1.19 igmp lastmember-queryinterval

Copyright © Huawei Technologies Co., Ltd.

10.1.21 igmp max-response-time
10.1.23 igmp prompt-leave
10.1.28 igmp require-router-alert
10.1.29 igmp robust-count
10.1.30 igmp send-router-alert
10.1.31 igmp ssm-mapping enable
10.1.32 igmp static-group
10.1.33 igmp timer other-querier-present
10.1.34 igmp timer query
10.1.36 igmp version
10.1.37 lastmember-queryinterval (IGMP)
10.1.39 max-response-time (IGMP)
10.1.43 require-router-alert (IGMP)
10.1.48 robust-count (IGMP)
10.1.49 send-router-alert (IGMP)
10.1.51 timer other-querier-present (IGMP)
10.1.52 timer query (IGMP)

10.1.2 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 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-instance	Displays IGMP message statistics in all instances.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
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 GE1/0/0.

```
<Huawei> display igmp control-message counters interface gigabitethernet 1/0/0
Interface message counter information of VPN-Instance: public net
 GigabitEthernet1/0/0(192.168.2.1):
 Message Type              Sent       Valid      Invalid    Ignore
 ----------------------------------------------------------------------
 General Query             280        0          0          0
 Group Query               0          0          0          0
 Source Group Query        0          0          0          0
 ----------------------------------------------------------------------
 IGMPV1V2
 Report ASM                0          279        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
```

 Copyright © Huawei Technologies Co., Ltd.

```
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 10-2 Description of the display igmp control-message counters interface gigabitethernet 1/0/0 command output

Item	Description
Interface message counter information of VPN-Instance: public net	VPN instance to which the interface belongs.
GigabitEthernet1/0/0(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.
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 IGMP Leave messages with multicast group addresses in the ASM group address range.
LEAVE SSM	Number of IGMP Leave messages with multicast group addresses in the SSM group address range.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
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.

Related Topics

10.1.44 reset igmp control-message counters

10.1.3 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 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.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
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

None

Example

Display information about the IGMPv3 hosts that join the specific source/group in INCLUDE mode.

```
<Huawei> display igmp explicit-tracking
Explicit-tracking information of VPN-Instance: public net
 Total 1 host, 2 entries

 GigabitEthernet1/0/0(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
```

 Copyright © Huawei Technologies Co., Ltd.

Table 10-3 Description of the display igmp explicit-tracking command output

Item	Description
Explicit-tracking information of VPN-Instance	VPN instance to which IGMP host information belongs.
Total 1 host, 2 entries	There is one IGMP host and two (S, G) entries.
GigabitEthernet1/0/0(192.168.0.12)	Type, number, and IP address of an interface.
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.
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.

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

10.1.45 reset igmp explicit-tracking

10.1.4 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 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-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.	-
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

Copyright © Huawei Technologies Co., Ltd.

Default Level

1: Monitoring level

Usage Guidelines

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

Example

Display information about dynamic IGMP groups.

```
<Huawei> display igmp group
Interface group report information of VPN-Instance: public net
 GigabitEthernet1/0/0(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 IGMP groups.

```
<Huawei> display igmp group verbose
Interface group report information of VPN-Instance: public net
 Limited entry of this VPN-Instance: -
 GigabitEthernet1/0/0(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 in the public network instance.

```
<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 10-4 Description of the display igmp group verbose command output

Item	Description
Interface group report information of VPN-Instance	VPN instance to which IGMP groups on an interface belong.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Limited entry of this VPN-Instance	Maximum number of IGMP entries that can be created for this instance.
GigabitEthernet1/0/0(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.
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 reporter	Last host that sends a Report message.

Copyright © Huawei Technologies Co., Ltd.

Item	Description
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.
Group mode	Multicast group record type. 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.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
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 is running IGMPv3 and has IGMPv3 receiver hosts attached.
Source	IP address of a multicast source.

Related Topics

10.1.19 igmp lastmember-queryinterval
10.1.21 igmp max-response-time
10.1.29 igmp robust-count
10.1.34 igmp timer query
10.1.46 reset igmp group

10.1.5 display igmp group ssm-mapping

Function

The **display igmp group ssm-mapping** command displays information about multicast group memberships 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**

Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Displays group memberships established with SSM mapping in a specified VPN instance.	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-instance	Displays group memberships established with SSM mapping in all instances.	-
group-address	Displays information about the specified multicast group memberships established with SSM mapping. If this parameter is not specified, the command displays information about all multicast group memberships 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 memberships established with SSM mapping on the specified interface. If this parameter is not specified, the command displays information about multicast group memberships 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 that hosts dynamically join.	-

Views

All views

Default Level

1: Monitoring level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

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

Example

Display summary of all multicast group memberships 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: -
 GigabitEthernet1/0/0(192.167.101.1):
  Total 1 IGMP SSM-Mapping Group reported
   Group Address   Last Reporter   Uptime      Expires
   232.0.0.1       192.167.101.2   00:00:02    00:02:08
```

Display detailed information about all multicast group memberships 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: -
 GigabitEthernet1/0/0(192.167.101.1):
  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: 192.167.101.2
     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 configured with SSM mapping that hosts dynamically join in the public network instance.

```
<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 10-5 Description of the display igmp group ssm-mapping verbose command output

Item	Description
Interface group report information of VPN-Instance	VPN instance to which IGMP SSM mapping information belongs.
Limited entry of this VPN-Instance	Maximum number of entries that can be generated in the VPN instance.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
GigabitEthernet1/0/0(192.167.101.1)	Interface type and interface number (IP address).
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 address received on the interface.
Group	Group address.
Uptime	Amount of time since the last Report message is received.
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	Last host that sends a Report message.
Last-member-query-counter	Number of times Group-Specific Query messages are sent.
Last-member-query-timer-expiry	Length of the last member query timer.
Group mode	Filter mode of a group, which can be include or exclude.
Version1-host-present-timer-expiry	Timeout period of IGMPv1 hosts. The value **off** indicates that the device has not received any Report messages from IGMPv1 hosts.
Version2-host-present-timer-expiry	Timeout period of IGMPv2 hosts. The value **off** indicates that the device has not received any Report messages from IGMPv2 hosts.

Related Topics

10.1.50 ssm-mapping (IGMP)

 Copyright © Huawei Technologies Co., Ltd.

10.1.6 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*] **static interface-number**

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 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 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-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.	-

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
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.	-
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 of VPN-Instance: public net
 Total 2 entries, Total 2 active entries
  Group Address   Source Address  Interface         State     Expires
  225.1.1.1       10.1.1.1        GE0/0/1           UP        never
  225.1.1.2       10.1.1.1        GE0/0/2           UP        never
```

Table 10-6 Description of the display igmp group static command output

Item	Description
Static join group information of VPN-Instance	VPN instance to which static IGMP groups belong.
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.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
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	Scheduled time when a group will be deleted from the IGMP group table. **never** indicates that the group never ages.

Display detailed information about static IGMP entries.

```
<Huawei> display igmp group static verbose
Static join group information of VPN-Instance: public net
 Total 2 entries
 00001.(*, 225.1.1.1)
    Total List of 1 joined interface
    1.GigabitEthernet0/0/1
       State:            UP
       Reference Count:  1
       Multicast Boundary:NO
       Outgoing Interface:YES
 00002.(*, 225.1.1.2)
    Total List of 1 joined interface
    1.GigabitEthernet0/0/2
       State:            UP
       Reference Count:  1
       Multicast Boundary:NO
       Outgoing Interface:YES
```

Table 10-7 Description of the display igmp group static verbose command output

Item	Description
Static join group information of VPN-Instance	VPN instance to which static IGMP groups belong.
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.GigabitEthernet0/0/1	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.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Multicast Boundary	Whether the multicast forwarding boundary is configured.
Outgoing Interface	Whether downstream interfaces exist.

Display lists of Up interfaces in static IGMP entries.

```
<Huawei> display igmp group static up
Static join group information of VPN-Instance: public net
 Total 4 entries
  00001.(*,225.1.1.1)
     Total List of 2 joined interfaces
     Total Matched 2 interfaces
     1.GigabitEthernet0/0/1
     2.GigabitEthernet0/0/2
  00002.(*,225.1.1.2)
     Total List of 2 joined interfaces
     Total Matched 2 interfaces
     1.GigabitEthernet0/0/1
     2.GigabitEthernet0/0/2
```

Table 10-8 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 GE1/0/0.

```
<Huawei> display igmp group interface gigabitethernet 1/0/0 static
Static join group information of VPN-Instance: public net
 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 10-9 Description of the display igmp group interface gigabitethernet 1/0/0 static command output

Item	Description
Static join group information of VPN-Instance	VPN instance to which static IGMP groups belong.
Total 2 entries	Number of static IGMP entries on the interface.
Specified interface state	Status of the specified interface.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Total 2 entries matched	Number of IGMP groups that meet the query conditions.
Group Address	Multicast group address.
Source Address	Multicast source address.
Expires	Scheduled time when a group will be deleted from the IGMP group table. **never** indicates that the group never ages.

Related Topics

10.1.32 igmp static-group

10.1.7 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 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-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.	-

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
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 interfaces of the device.

Example

Display the IGMP configuration and running information on GE1/0/0.

```
<Huawei> display igmp interface gigabitethernet 1/0/0
Interface information of VPN-Instance: public net
 GigabitEthernet1/0/0(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
 GigabitEthernet1/0/0(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
```

 Copyright © Huawei Technologies Co., Ltd.

```
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 10-10 Description of the display igmp interface verbose command output

Item	Description
Interface information of VPN-Instance	VPN instance to which IGMP interface information belongs.
GigabitEthernet1/0/0(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.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
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.
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 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	IGMP querier. In IGMPv1, the querier is selected based on the multicast routing protocol. In IGMPv2, the multicast router with the smallest IP address functions as the querier on the shared network segment.

Copyright © Huawei Technologies Co., Ltd.

Item	Description
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.
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 local device discards 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 local device sends IGMP packets with 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. 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. This function is configured using the **igmp query ip-source-policy** command.
Prompt-leave	Whether fast leave is enabled. The fast leave function is configured using the **igmp prompt-leave** command.
SSM-Mapping	Whether SSM mapping is enabled. SSM mapping is enabled using the **igmp ssm-mapping enable** command.

Copyright © Huawei Technologies Co., Ltd.

Item	Description
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. The value **off** indicates that the interface considers itself as a querier and that no other queriers exist.
TTL-check	Whether the function to check the TTL values in received IGMP Report, Leave, and Query messages is enabled: • enabled • disabled
Total 1 IGMP Group reported	Indicates the number of IGMP groups that the interface dynamically joins.

Related Topics

10.1.15 igmp enable
10.1.17 igmp group-policy
10.1.18 igmp ip-source-policy
10.1.19 igmp lastmember-queryinterval
10.1.21 igmp max-response-time
10.1.23 igmp prompt-leave
10.1.27 igmp query ip-source-policy
10.1.28 igmp require-router-alert
10.1.29 igmp robust-count
10.1.30 igmp send-router-alert
10.1.31 igmp ssm-mapping enable
10.1.34 igmp timer query
10.1.36 igmp version

10.1.8 display igmp invalid-packet

Function

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

 Copyright © Huawei Technologies Co., Ltd.

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 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-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

 Copyright © Huawei Technologies Co., Ltd.

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** [**vpn-instance** *vpn-instance-name* | **all-instance**] **invalid-packet** command to view statistics about invalid IGMP messages received in a specified VPN instance or in all VPN instances.
- 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, details about a maximum of 100 invalid IGMP messages can be displayed.

Example

Display statistics about invalid IGMP messages received by the device.

```
<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 10-11 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.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Unwanted Source List	Number of messages with unwanted source lists.
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          :  GigabitEthernet1/0/0
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 10-12 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.

 Copyright © Huawei Technologies Co., Ltd.

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.

Related Topics

10.7.23 multicast invalid-packet

10.1.9 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**]

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Displays information about IGMP proxy groups in a specific VPN instance.	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.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
all-instance	Displays information about IGMP proxy groups in all VPN instances.	-
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 224.0.0.0 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

Usage Scenario

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 to view information about the IGMP proxy group.

Example

Display information about IGMP proxy groups in a public network instance.

```
<Huawei> display igmp proxy group
Interface group report information of VPN-Instance: public net
    GigabitEthernet1/0/0(10.1.6.2):
     Total 2 IGMP proxy Groups
      Group Address   Filter mode
      225.1.1.1       exclude
      225.1.1.2       include
```

 Copyright © Huawei Technologies Co., Ltd.

Table 10-13 Description of the display igmp proxy group command output

Item	Description
Interface group report information of VPN-Instance	VPN instance to which IGMP group information on an interface belongs.
GigabitEthernet1/0/0(10.1.6.2)	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.

Display details of IGMP proxy groups in a public network instance.

```
<Huawei> display igmp proxy group verbose
Interface group report information of VPN-Instance: public net
    GigabitEthernet1/0/0(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 10-14 Description of the display igmp proxy group verbose command output

Item	Description
Query Response Expiry	Amount of time before the query response time expires.
Source list (total 1 source)	Source list (number of sources in the source list).
Source	Multicast source address.
Group	Multicast group address.

Related Topics

10.1.24 igmp proxy

10.1.25 igmp proxy backup

Copyright © Huawei Technologies Co., Ltd.

10.1.10 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*]

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 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-instance	Displays information about IGMP proxy interfaces in all VPN instances.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

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 to view information about the IGMP proxy interface.

Example

Display information about IGMP proxy interfaces in a public network instance.

```
<Huawei> display igmp proxy interface
Interface information of VPN-Instance: public net
 GigabitEthernet1/0/0(192.168.1.2):
   IGMP proxy is enabled
   Current IGMP proxy version (negotiated) is 3
   Current IGMP proxy version (configured) is 2
```

 Copyright © Huawei Technologies Co., Ltd.

```
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: off
Value of querier present timeout for IGMPv3: 124 s
General query response expiry: off
Querier for IGMP: 192.168.1.1
Robustness (negotiated): 2
Robustness (configured): 2
Require-router-alert: disabled
Send-router-alert: enabled
Ip-source-policy: disabled
Query Ip-source-policy: disabled
TTL-check: disabled
```

Table 10-15 Description of the display igmp proxy interface command output

Item	Description
Interface information of VPN-Instance	VPN instance to which IGMP proxy interface information belongs.
GigabitEthernet1/0/0(192.168.1.2)	Interface number (IP address).
IGMP proxy is enabled	IGMP proxy is enabled on the interface.
Current IGMP proxy version (negotiated) is 3	Negotiated IGMP version on the IGMP proxy interface is IGMPv3.
Current IGMP proxy version (configured) is 2	IGMPv2 is configured 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.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
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 router 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.
Robustness (configured)	Robustness variable configured on the IGMP proxy interface.
Require-router-alert	Whether the device accepts only IGMP messages carrying the Router-Alert option.
Send-router-alert	Whether the device sends IGMP messages carrying the Router-Alert option.
Ip-source-policy	Whether to filter IGMP Report/Leave messages based on host addresses.
Query Ip-source-policy	Whether to filter IGMP Query messages based on source addresses.
TTL-check	Whether the function to check the TTL values in received IGMP Report, Leave, and Query messages is enabled: • enabled • disabled

10.1.11 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*]]

 Copyright © Huawei Technologies Co., Ltd.

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 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-instance	Displays information about IGMP proxy routing tables in all VPN instances.	-
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.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
interface-type interface-number	Specifies the type and number of an interface.	-
none	Displays the routing entries with an empty downstream interface list.	-
incoming-interface	Displays the routing entries with a specified 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

Usage Scenario

If you need to know 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 in a public network instance.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> display igmp proxy routing-table fsm
Routing table of VPN-Instance: public net
 Total 1 (*, G) entry; 1 (S, G) entry

 (*, 225.1.1.1)
     Flag: WC, UpTime: 6d:10h
     Upstream interface: GigabitEthernet1/0/2
     Downstream interface(s) information:
     Total number of downstreams: 1
         1: GigabitEthernet1/0/1
             Protocol: igmp, UpTime: 17:27:13
             IGMP querier: 11.1.1.1(this router)
             IGMP state: EXCLUDE

     FSM information for non-downstream interfaces: None

 (33.3.3.100, 225.1.1.1)
     Flag: JOIN ACT, UpTime: 6d:17h
     Upstream interface: GigabitEthernet1/0/2
     Downstream interface(s) information:
     Total number of downstreams: 1
         1: GigabitEthernet1/0/1
             Protocol: igmp, UpTime: 17:27:13
             IGMP querier: 11.1.1.1(this router)
             IGMP state: NI

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

Table 10-16 Description of the display igmp proxy routing-table fsm command output

Item	Description
Routing table of VPN-Instance	VPN instance to which IGMP proxy routing information belongs.
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.
GigabitEthernet1/0/1	Name of a downstream interface.
Protocol	Protocol of a downstream interface.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
UpTime	Amount of time a downstream interface has been in Up state, expressed in hh:mm:ss format.
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.

10.1.12 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 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-instance	Displays IGMP routing information in all instances.	-

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
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.	It 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.	It 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 for problem location.

 Copyright © Huawei Technologies Co., Ltd.

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 of VPN-Instance: public net
 Total 2 entries

 00001. (10.10.10.10, 232.1.1.3)
      List of 1 downstream interface in include mode
       GigabitEthernet1/0/0 (10.20.20.1),
                Protocol: SSM-MAP

 00002. (*, 225.1.1.1)
      List of 1 downstream interface
       GigabitEthernet1/0/0 (10.20.20.1),
                Protocol: IGMP
```

Table 10-17 Description of the display igmp routing-table command output

Item	Description
Routing table of VPN-Instance: public net	VPN instance to which the IGMP routing table belongs.
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	Downstream interface list in include mode.
GigabitEthernet1/0/0 (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.

 Copyright © Huawei Technologies Co., Ltd.

10.1.13 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 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-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

 Copyright © Huawei Technologies Co., Ltd.

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 of VPN-Instance: public net
 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 10-18 Description of the display igmp ssm-mapping group command output

Item	Description
IGMP SSM-Mapping conversion table of VPN-Instance	VPN instance to which the IGMP SSM mapping table belongs.
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 GE1/0/0.

```
<Huawei> display igmp ssm-mapping interface gigabitethernet 1/0/0
IGMP SSM-Mapping is enabled
```

Table 10-19 Description of the display igmp ssm-mapping interface gigabitethernet 1/0/0 command output

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

Related Topics

10.1.31 igmp ssm-mapping enable

10.1.50 ssm-mapping (IGMP)

Copyright © Huawei Technologies Co., Ltd.

10.1.14 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 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

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 in the public network instance or VPN instance.

Example

Enter the IGMP view of the public network instance.

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

Enter the IGMP view of VPN instance mvpn.

```
<Huawei> system-view
[Huawei] ip vpn-instance mvpn
```


Copyright © Huawei Technologies Co., Ltd.

```
[Huawei-vpn-instance-mvpn] ipv4-family
[Huawei-vpn-instance-mvpn-af-ipv4] route-distinguisher 22:1
[Huawei-vpn-instance-mvpn-af-ipv4] quit
[Huawei-vpn-instance-mvpn] multicast routing-enable
[Huawei-vpn-instance-mvpn] quit
[Huawei] igmp vpn-instance mvpn
[Huawei-igmp-mvpn]
```

Related Topics

10.7.28 multicast routing-enable

10.1.15 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

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On a shared network segment, user hosts and Layer 3 multicast devices directly connected to the user network segment 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 in the public network instance or VPN instance.

Precautions

- If PIM and IGMP need to be enabled on the same interface, enable PIM, and then IGMP.

Copyright © Huawei Technologies Co., Ltd.

- If IGMP parameters are configured on an interface, the parameter settings take effect only after IGMP is enabled.

Example

Enable IGMP on GE1/0/0 connected to a user network segment.

```
<Huawei> system-view
[Huawei] multicast routing-enable
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] igmp enable
```

Related Topics

10.7.28 multicast routing-enable

10.1.7 display igmp interface

10.1.16 igmp global limit

Function

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

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

By default, the maximum number of IGMP entries that can be created on the router varies according to device models:

- AR150&200 series: 128
- AR100&AR120&AR160&AR1200 series: 3000
- AR2201-48FE, AR2202-48FE, AR2204-27GE, AR2204-27GE-P, AR2204-51GE-P, AR2204-51GE-R, AR2204E, AR2204E-Dand AR2204: 256
- AR2220, and AR2220E: 20480
- AR2204XE and AR2204XE-DC: 34816
- AR2240C: 33792
- AR2240 series and AR3200 series:
  - Configured with SRU40: 33792
  - Configured with SRU60: 33792
  - Configured with SRU80: 34816
  - Configured with SRU100: 34816
  - Configured with SRU100E: 34816
  - Configured with SRU200: 34816
  - Configured with SRU200E: 34816
  - Configured with SRU400: 34816
- AR3600 series (SRUX5): 34816

Format

igmp global limit *number*

 Copyright © Huawei Technologies Co., Ltd.

undo igmp global limit

Parameters

Parameter	Description	Value
number	Specifies the maximum number of IGMP entries that can be created on the router.	The value is an integer that ranges from: ● 1 to 128 for the AR150&200 series ● 1 to 3000 for the AR100&AR120&AR160&AR1200 series ● 1 to 256 for the AR2201-48FE, AR2202-48FE, AR2204-27GE, AR2204-27GE-P, AR2204-51GE-P, AR2204-51GE-R, AR2204E, AR2204E-D and AR2204 ● 1 to 20480 for the AR2220, and AR2220E ● 1 to 34816 for the AR2204XE and AR2204XE-DC ● AR2240C: 1 to 33792 ● AR2240 series and AR3200 series (depending on the SRU model used on the router): – Configured with SRU40: 1 to 33792 – Configured with SRU60: 1 to 33792 – Configured with SRU80: 1 to 34816 – Configured with SRU100: 1 to 34816 – Configured with SRU100E: 1 to 34816 – Configured with SRU200: 1 to 34816 – Configured with SRU200E: 1 to 34816 – Configured with SRU400: 1 to 34816 ● 1 to 34816 for the AR3600 series (SRUX5)

Views

System view

Default Level

2: Configuration level

Usage Guidelines

When the number of IGMP entries reaches the limit, the system does not create any IGMP entries. To enable the router to create new IGMP entries, 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.

 Copyright © Huawei Technologies Co., Ltd.

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

Example

Set the maximum number of IGMP entries that can be created on the router to 126.

```
<Huawei> system-view
[Huawei] igmp global limit 126
```

Related Topics

10.1.38 limit (IGMP)

10.1.20 igmp limit

10.1.17 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* | **acl-name** *acl-name* } [**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.
acl-name *acl-name*	Specifies the name of a named ACL. **NOTE** **acl-name** *acl-name* can only be the name of a named advanced ACL.	The value is a string of 1 to 32 case-sensitive characters without spaces. The value must start with a letter (case sensitive).
1	Sets the range of multicast groups that IGMPv1 hosts can join.	-

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
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

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 as a filter to specify the range of multicast groups served by the interface. This configuration improves security of the IGMP application. You can also use this command to prevent the router from receiving Join messages for specified groups.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command in the public network instance or VPN instance.

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 router, the router 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.

 Copyright © Huawei Technologies Co., Ltd.

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 GE1/0/0 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 1/0/0
[Huawei-GigabitEthernet1/0/0] igmp group-policy 2005
```

Create an ACL named **myacl**, and configure a rule that allows hosts to receive data of multicast groups in the range of 225.1.0.0/16. Configure an IGMP group policy on GE1/0/0 and reference the ACL to allow hosts connected to the interface to join only the specified multicast groups.

```
<Huawei> system-view
[Huawei] acl name myacl
[Huawei-acl-adv-myacl] rule permit ip destination 225.1.0.0 0.0.255.255
[Huawei-acl-adv-myacl] quit
[Huawei] multicast routing-enable
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] igmp group-policy acl-name myacl
```

Related Topics

10.1.4 display igmp group

10.1.7 display igmp interface

10.7.28 multicast routing-enable

10.1.18 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 router does not filter IGMP Report/Leave messages based on source addresses.

Format

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

undo igmp ip-source-policy

Copyright © Huawei Technologies Co., Ltd.

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.
acl-name *acl-name*	Specifies the name of an ACL. **NOTE** **acl-name** *acl-name* can only be the name of a named advanced ACL.	The value is a string of 1 to 32 case-sensitive characters without spaces. The value must start with a letter (case sensitive).

Views

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. To improve security, 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 in the public network instance or VPN instance.

Precautions

IGMP Report/Leave messages are encapsulated in IP packets. The **igmp ip-source-policy** command configures the router to check the source address in the IP header of each received Report/Leave message. The router 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 router 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 router 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.

 Copyright © Huawei Technologies Co., Ltd.

Example

Enable filtering of IGMP Report/Leave messages based on source addresses on GE1/0/0.

```
<Huawei> system-view
[Huawei] multicast routing-enable
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] igmp ip-source-policy
```

Configure GE1/0/0 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 gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] igmp ip-source-policy 2001
```

Related Topics

10.1.7 display igmp interface
10.7.28 multicast routing-enable

10.1.19 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

Interface view

 Copyright © Huawei Technologies Co., Ltd.

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 Report messages 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 in the public network instance or VPN instance.

Precautions

- The **igmp lastmember-queryinterval** command is valid only when the IGMP querier runs IGMPv2 and 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 is globally valid in the instance, whereas the configuration in the interface view is valid only for the current interface. The system prefers the configuration in the interface view. The configuration in the IGMP view is used only when the configuration in the interface view is incomplete.

Example

Set the interval for sending IGMP Group-Specific Query messages or IGMP Group-and-Source-Specific Query messages to 3 seconds on GE1/0/0.

```
<Huawei> system-view
[Huawei] multicast routing-enable
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] igmp lastmember-queryinterval 3
```

Related Topics

10.1.7 display igmp interface

10.1.29 igmp robust-count

10.1.37 lastmember-queryinterval (IGMP)

10.7.28 multicast routing-enable

10.1.48 robust-count (IGMP)

Copyright © Huawei Technologies Co., Ltd.

10.1.20 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.

By default, the maximum number of IGMP entries that can be created on an interface varies according to device models:

- AR150&AR200 series: 64
- AR2201-48FE, AR2202-48FE, AR2204-27GE, AR2204-27GE-P, AR2204-51GE-P, AR2204-51GE-R, AR2204E, AR2204E-D, and AR2204: 128
- AR100&AR120&AR160&AR1200 series, AR2220E, AR2240C and AR2220: 1000
- AR2204XE and AR2204XE-DC: 2000
- AR2240 and AR3200 series:
  - Configured with SRU40: 1000
  - Configured with SRU60: 1000
  - Configured with SRU80: 2000
  - Configured with SRU100E: 2000
  - Configured with SRU200: 3000
  - Configured with SRU200E: 3000
  - Configured with SRU400: 4000
- AR3600 series (SRUX5): 3000

Format

igmp limit *number* [**except** { *acl-number* | **acl-name** *acl-name* }]

undo igmp limit

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
number	Specifies the maximum number of IGMP entries allowed on an interface.	The value is an integer that ranges from: ● 1 to 64 for the AR150&AR200 series ● 1 to 128 for the AR2201-48FE, AR2202-48FE, AR2204-27GE, AR2204-27GE-P, AR2204-51GE-P, AR2204-51GE-R, AR2204E, AR2204E-D, and AR2204 ● 1 to 1000 for the AR100&AR120&AR160&AR1200 series, AR2220E, AR2240C, AR2220 ● 1 to 2000 for the AR2204XE and AR2204XE-DC ● AR2240 and AR3200 series (depending on the SRU model used on the router): – Configured with SRU40: 1 to 1000 – Configured with SRU60: 1 to 1000 – Configured with SRU80: 1 to 2000 – Configured with SRU100E: 1 to 2000 – Configured with SRU200: 1 to 3000 – Configured with SRU200E: 1 to 3000 – Configured with SRU400: 1 to 4000 ● 1 to 3000 for the AR3600 series (SRUX5)
except	Specifies the range of multicast groups whose IGMP entries are not limited by the IGMP limit.	-
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.
acl-name *acl-name*	Specifies the name of a named ACL. **NOTE** **acl-name** *acl-name* can only be the name of a named advanced ACL.	The value is a string of 1 to 32 case-sensitive characters without spaces. The value must start with a letter (case sensitive).

Copyright © Huawei Technologies Co., Ltd.

Views

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 router 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 in the public network instance or VPN instance view.

Precautions

If **except** is not specified in the command, the configured IGMP limit restricts the maximum number of all dynamic IGMP (*, G) or (S, G) entries. 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 GE1/0/0 to 60.

```
<Huawei> system-view
[Huawei] multicast routing-enable
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] igmp limit 60
```

Create a named ACL **myacl**, and configure a rule that allows hosts to receive messages sent from multicast source 10.1.1.1 to multicast group 232.0.0.0/16. Set the maximum number of IGMP entries that can be created on the GE1/0/0 to 60,

 Copyright © Huawei Technologies Co., Ltd.

and exclude multicast group 232.0.0.0/16 whose IGMP entries do not need to be limited.

```
<Huawei> system-view
[Huawei] multicast routing-enable
[Huawei] acl name myacl
[Huawei-acl-adv-myacl] rule permit ip source 10.1.1.1 0 destination 232.0.0.0 0.0.255.255
[Huawei-acl-adv-myacl] quit
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] igmp limit 60 except acl-name myacl
```

Related Topics

10.1.16 igmp global limit

10.1.38 limit (IGMP)

10.1.21 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

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

 Copyright © Huawei Technologies Co., Ltd.

number of Report messages sent from many hosts at the same time. The network may be congested when this situation occurs.

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 in the public network instance or VPN instance.

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, except for the function range. The configuration in the IGMP view is globally valid, whereas the configuration in the interface view is valid only for the current interface. The system prefers the configuration in the interface view. The configuration in the IGMP view is used only when the configuration in the interface view is not done.

Example

Set the maximum response time for IGMP General Query messages to 8 seconds on GE1/0/0.

```
<Huawei> system-view
[Huawei] multicast routing-enable
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] igmp max-response-time 8
```

Related Topics

10.1.7 display igmp interface

10.1.39 max-response-time (IGMP)

10.7.28 multicast routing-enable

10.1.22 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

 Copyright © Huawei Technologies Co., Ltd.

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

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 multicast membership information based on received Report and Leave messages. Multicast 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 multicast memberships based on requirements of members. The querier does not send Query messages to collect member information, reducing the number of IGMP messages exchanged between the querier and hosts.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command in the public network instance or VPN instance.

Precautions

- IGMP on-demand applies only to IGMPv2 and IGMPv3.
- 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.

 Copyright © Huawei Technologies Co., Ltd.

- 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. The entries 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 GE1/0/0.

```
<Huawei> system-view
[Huawei] multicast routing-enable
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] igmp on-demand
```

Related Topics

10.7.28 multicast routing-enable

10.1.23 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* | **acl-name** *acl-name* }]

undo igmp prompt-leave

Copyright © Huawei Technologies Co., Ltd.

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 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.
acl-name *acl-name*	Specifies the name of a named ACL. **NOTE** **acl-name** *acl-name* can only be the name of a named advanced ACL.	The value is a string of 1 to 32 case-sensitive characters without spaces. The value must start with a letter (case sensitive).

Views

Interface view

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

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 in the public network instance or VPN instance.

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.
- When configuring an ACL 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 ACL, 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 ACL, set **source** to the multicast source address and **destination** to the range of multicast groups that hosts can fast leave.

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 GE1/0/0 so that the entry of group 225.1.0.0/16 will be delete immediately after the interface receives an IGMP Leave message for the group GE1/0/0.

```
<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 1/0/0
[Huawei-GigabitEthernet1/0/0] igmp prompt-leave group-policy 2005
```

Create an ACL named **myacl** 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 GE1/0/0 so that the entry of group 225.1.0.0/16 will be delete immediately after the interface receives an IGMP Leave message for the group GE1/0/0.

```
<Huawei> system-view
[Huawei] acl name myacl
[Huawei-acl-adv-myacl] rule permit ip destination 225.1.0.0 0.0.255.255
[Huawei-acl-adv-myacl] quit
[Huawei] multicast routing-enable
```

 Copyright © Huawei Technologies Co., Ltd.

```
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] igmp prompt-leave group-policy acl-name myacl
```

Related Topics

10.1.7 display igmp interface

10.7.28 multicast routing-enable

10.1.24 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

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-insensitive characters, spaces not supported. **NOTE** When double quotation marks are used around the string, spaces are allowed in the string.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In a simple tree topology, multicast routers 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 routers transparently transmit all IGMP messages from hosts. To reduce loads on the upstream device, configure IGMP proxy on the multicast

Copyright © Huawei Technologies Co., Ltd.

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

IGMP proxy lacks a fault detection mechanism to trigger link switchover quickly. Therefore, multicast services may 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 primary IGMP proxy interface, the device configured with the IGMP proxy backup function can switch multicast traffic to the backup link to minimize the communication interruption time.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command in the public network instance or VPN instance view.

Precautions

A public network or VPN instance supports only one IGMP proxy interface

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.

Example

Enable IGMP proxy on GE 1/0/0 in the public network instance.

```
<Huawei> system-view
[Huawei] multicast routing-enable
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] igmp proxy
```

Enable IGMP proxy on GE1/0/0, and associate GE1/0/0 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 gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] igmp proxy track nqa user test
```

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

10.1.9 display igmp proxy group
10.1.10 display igmp proxy interface
10.1.11 display igmp proxy routing-table

10.1.25 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, IGMP proxy backup is disabled on an interface.

Format

igmp proxy backup

undo igmp proxy backup

Parameters

None

Views

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 in the public network instance or VPN instance view.

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:

 Copyright © Huawei Technologies Co., Ltd.

- 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.

Example

Configure GE1/0/0 as a backup IGMP proxy interface in the public network instance.

```
<Huawei> system-view
[Huawei] multicast routing-enable
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] igmp proxy backup
```

Related Topics

10.1.9 display igmp proxy group

10.1.10 display igmp proxy interface

10.1.11 display igmp proxy routing-table

10.1.26 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.

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 is a string of 1 to 31 case-sensitive characters, spaces not supported. The string can contain spaces if it is enclosed with double quotation marks (").

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
all-instance	Indicates all VPN instances.	-
interface *interface-type interface-number*	Specifies an IGMP proxy interface.	-

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
```

10.1.27 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* | **acl-name** *acl-name* }

undo igmp query ip-source-policy

 Copyright © Huawei Technologies Co., Ltd.

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.
acl-name *acl-name*	Specifies the name of an ACL. **NOTE** **acl-name** *acl-name* can only be the name of a named advanced ACL.	The value is a string of 1 to 32 case-sensitive characters without spaces. The value must start with a letter (case sensitive).

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If an attacker sends forged IGMP Query messages with an IP addresses smaller than the querier IP address, the querier will be replaced by the attacker. As a result, the real querier cannot response 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 device, the device 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 in the public network instance or VPN instance.

Precautions

- IGMP Query messages are encapsulated into IP messages. This command is used to filter IGMP Query messages based on the source addresses in IP headers.
- This command configures a policy to filter IGMP Query messages based on source addresses. The ACL referenced in the policy defines the source addresses allowed. The device accepts only the IGMP Query messages with source addresses in the allowed range.

Example

Configure GE1/0/0 to accept only the IGMP Query messages with the source address 10.10.1.1.

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

 Copyright © Huawei Technologies Co., Ltd.

```
[Huawei] acl number 2001
[Huawei-acl-basic-2001] rule permit source 10.10.1.1 0
[Huawei-acl-basic-2001] quit
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] igmp query ip-source-policy 2001
```

10.1.28 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

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

 Copyright © Huawei Technologies Co., Ltd.

IP multicast routing has been enabled using the **multicast routing-enable** command in the public network instance or VPN instance.

Precautions

This command has the same function as the **require-router-alert** command, except for the function range. The configuration in the IGMP view is globally valid in the instance, whereas the configuration in the interface view is valid only for the current interface. The system prefers the configuration in the interface view. The configuration in the IGMP view is used only when the configuration in the interface view is not done.

Example

Configure GE1/0/0 to discard IGMP messages without the Router-Alert option.

```
<Huawei> system-view
[Huawei] multicast routing-enable
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] igmp require-router-alert
```

Related Topics

10.1.7 display igmp interface

10.1.30 igmp send-router-alert

10.7.28 multicast routing-enable

10.1.43 require-router-alert (IGMP)

10.1.29 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.

Copyright © Huawei Technologies Co., Ltd.

Views

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 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 certain 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 certain 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.

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 in the public network instance or VPN instance.

Precautions

The **igmp robust-count** command has the same function as the **robust-count** command, except for the function range. The configuration in the IGMP view is

 Copyright © Huawei Technologies Co., Ltd.

globally valid in the instance, whereas the configuration in the interface view is valid only for the current interface. The system prefers the configuration in the interface view. The configuration in the IGMP view is used only when the configuration in the interface view is not done.

Example

Set the querier robustness variable on GE1/0/0 to 3.

```
<Huawei> system-view
[Huawei] multicast routing-enable
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] igmp robust-count 3
```

Related Topics

10.1.7 display igmp interface
10.1.19 igmp lastmember-queryinterval
10.1.34 igmp timer query
10.1.37 lastmember-queryinterval (IGMP)
10.7.28 multicast routing-enable
10.1.48 robust-count (IGMP)
10.1.52 timer query (IGMP)

10.1.30 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

Interface view

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

Usage Scenario

By default, the router sends IGMP messages that contain the Router-Alert option in IP headers. If the router 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 router 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 in the public network instance or VPN instance.

Precautions

The **igmp send-router-alert** command has the same function as the **send-router-alert** command, except for the function range. The configuration in the IGMP view is globally valid in the instance, whereas the configuration in the interface view is valid only for the current interface. The system prefers the configuration in the interface view. The configuration in the IGMP view is used only when the configuration in the interface view is not done.

Example

Configure GE1/0/0 to send IGMP messages without the Router-Alert option.

```
<Huawei> system-view
[Huawei] multicast routing-enable
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] undo igmp send-router-alert
```

Related Topics

10.1.7 display igmp interface
10.1.28 igmp require-router-alert
10.7.28 multicast routing-enable
10.1.49 send-router-alert (IGMP)

10.1.31 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

Copyright © Huawei Technologies Co., Ltd.

Parameters

None

Views

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 router. IGMP SSM mapping is implemented based on static SSM mapping entries on the router. The router 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 in the public network instance or VPN instance.

Example

Enable SSM mapping on GE1/0/0.

```
<Huawei> system-view
[Huawei] multicast routing-enable
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] igmp ssm-mapping enable
```

Related Topics

10.1.7 display igmp interface

10.1.50 ssm-mapping (IGMP)

10.7.28 multicast routing-enable

10.1.32 igmp static-group

Function

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

 Copyright © Huawei Technologies Co., Ltd.

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* [**source** *source-address*] **mping-echo**

undo igmp static-group *group-address* [**source** *source-address*] **mping-echo**

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.	-
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.	The address is in dotted decimal notation.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
all	Indicates all multicast groups that an interface statically joins.	-
mping-echo	Configures the device to respond to multicast ping packets received on the interface.	-

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can configure static multicast groups on user-side interfaces of the router in some scenarios, for example:

- There are long-term group members on a shared network segment, and the router 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 router considers that the multicast group always has members on the network segment of the interface. Therefore, the router 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 at a time or configure multiple groups or source-group bindings in a batch.

If **mping-echo** is specified in the **igmp static-group** command, the interface cannot only send and receive multicast data packets but also respond to received multicast ping packets. This keyword enables the device to implement the multicast ping function without the need of a user host that can parse and respond to multicast ping packets. This makes fault location more flexible and convenient.

To add an interface to multiple multicast groups in batches, run the **igmp static-group** *group-address* **inc-step-mask** { *group-mask* | *group-mask-length* } **number** *group-number* command. To convert a *group-mask-length* value to a *group-mask* value, use the following formula: *group-mask* = 1<<(32 – *group-mask-length*). The << symbol represents the left-shift operator, using which the binary format of an

 Copyright © Huawei Technologies Co., Ltd.

integer is shifted left for a specified number of digits. Extra binary digits out of the left boundary are discarded, and 0s are added at the right boundary. For example, 1<<0 represents 0.0.0.1, 1<<1 represents 0.0.0.2, and 1<<3 represents 0.0.0.4.If *group-mask-length* is set to configure the incremental mask of group addresses, when you use the **display current-configuration** command to view related configurations, the format of the displayed incremental mask of group address is converted to *group-mask*.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command in the public network instance or VPN instance.

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 router 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.
- If you perform a second batch configuration by changing only *group-number* in the command and retaining the values of *group-address* and *group-mask* | *group-mask-length* configured in the first batch configuration, the second batch configuration overrides the first one.
- 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.

Example

Configure static multicast group 224.1.1.1 on GE1/0/0.

```
<Huawei> system-view
[Huawei] multicast routing-enable
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] igmp static-group 224.1.1.1
```

Configure the router to forward multicast packets from multicast source 192.168.11.1 to multicast group 232.1.1.1 through GE1/0/0.

```
<Huawei> system-view
[Huawei] multicast routing-enable
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] igmp static-group 232.1.1.1 source 192.168.11.1
```

Configure 10 static multicast groups on GE1/0/0 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 gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] igmp static-group 225.1.1.1 inc-step-mask 32 number 10
```

Configure 10 source-group bindings on GE1/0/0 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.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> system-view
[Huawei] multicast routing-enable
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] igmp static-group 232.1.1.1 inc-step-mask 32 number 10 source 192.168.11.1
```

Configure static group 224.1.1.1 on GE1/0/0 connected to a user host network segment and enable the interface to respond to received multicast ping packets.

```
<Huawei> system-view
[Huawei] multicast routing-enable
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] igmp static-group 224.1.1.1 mping-echo
```

Related Topics

10.1.4 display igmp group

10.7.28 multicast routing-enable

10.1.33 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

Interface view

Copyright © Huawei Technologies Co., Ltd.

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 in the public network instance or VPN instance.

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, except for the function range. The configuration in the IGMP view is globally valid in the instance, whereas the configuration in the interface view is valid only for the current interface. The system prefers the configuration in the interface 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

On GE1/0/0, set the other querier present timer to 200 seconds.

```
<Huawei> system-view
[Huawei] multicast routing-enable
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] igmp timer other-querier-present 200
```

Related Topics

10.1.7 display igmp interface

10.1.34 igmp timer query

10.7.28 multicast routing-enable

10.1.51 timer other-querier-present (IGMP)

 Copyright © Huawei Technologies Co., Ltd.

10.1.34 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

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

An IGMP querier sends IGMP General Query messages at an interval to check whether a local network segment has group members. This interval is the general query interval. You can set the general query interval based on situations on your network. The general query interval affects the following processes:

- When a querier starts, it sends General Query messages certain 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

Copyright © Huawei Technologies Co., Ltd.

IP multicast routing has been enabled using the **multicast routing-enable** command in the public network instance or VPN instance.

Precautions

- The querier is more sensitive when it sends General Query messages at a shorter interval. However, more bandwidth and resources are consumed in this case.
- The function of the **igmp timer query** command is the same as that of the **timer query** command, except for the function range. The configuration in the IGMP view is globally valid in the instance, whereas the configuration in the interface view is valid only for the current interface. The system prefers the configuration in the interface view. The configuration in the IGMP view is used only when the configuration in the interface view is not done.

Example

Set the interval at which GE1/0/0 sends General Query messages to 50 seconds.

```
<Huawei> system-view
[Huawei] multicast routing-enable
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] igmp timer query 50
```

Related Topics

10.1.7 display igmp interface

10.1.29 igmp robust-count

10.1.33 igmp timer other-querier-present

10.7.28 multicast routing-enable

10.1.48 robust-count (IGMP)

10.1.52 timer query (IGMP)

10.1.35 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

Copyright © Huawei Technologies Co., Ltd.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

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

The **igmp ttl-check** command provides the same function as the **ttl-check** command run in the IGMP view, except that the **ttl-check** command configuration takes effect for all interfaces in the instance.

Configuration Impact

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 the device to check the TTL values in received IGMP Report, Leave, and Query messages on a specific interface.

```
<Huawei> system-view
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] igmp ttl-check
```

10.1.36 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

Copyright © Huawei Technologies Co., Ltd.

Parameters

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

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The router can identify IGMP messages of a version earlier than its own IGMP version but cannot identify IGMP messages of a later version. To ensure normal IGMP operation, ensure that the router runs the same IGMP version as member hosts or a later IGMP version.

If multiple routers exist on a shared network segment, configure the same IGMP version on all router 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 in the public network instance or VPN instance.

Example

Configure IGMPv1 on GE1/0/0.

```
<Huawei> system-view
[Huawei] multicast routing-enable
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] igmp version 1
```

Related Topics

10.1.7 display igmp interface

10.7.28 multicast routing-enable

10.1.37 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.

Copyright © Huawei Technologies Co., Ltd.

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 in the public network instance or VPN instance.

Precautions

- The **igmp lastmember-queryinterval** command is valid only when the IGMP querier runs IGMPv2 or IGMPv3.

 Copyright © Huawei Technologies Co., Ltd.

- This command has the same function as the **igmp lastmember-queryinterval** command, except for the function range. The configuration in the IGMP view is globally valid in the instance, whereas the configuration in the interface view is valid only for the current interface. The system prefers the configuration in the interface view. The configuration in the IGMP view is used only when the configuration in the interface view is not done.

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
```

In VPN instance mvpn, 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 vpn-instance mvpn
[Huawei-igmp-mvpn] lastmember-queryinterval 3
```

Related Topics

10.1.7 display igmp interface

10.1.19 igmp lastmember-queryinterval

10.1.29 igmp robust-count

10.7.28 multicast routing-enable

10.1.48 robust-count (IGMP)

10.1.38 limit (IGMP)

Function

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

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

By default, the maximum number of IGMP entries that can be created for an instance varies according to device models:

- AR150&200 series: 128
- AR100&AR120&AR160&AR1200 series: 3000
- AR2201-48FE, AR2202-48FE, AR2204-27GE, AR2204-27GE-P, AR2204-51GE-P, AR2204-51GE-R, AR2204E, AR2204E-Dand AR2204: 256
- AR2220, and AR2220E: 20480
- AR2204XE and AR2204XE-DC: 34816
- AR2240C: 33792
- AR2240 series and AR3200 series:

Copyright © Huawei Technologies Co., Ltd.

  - Configured with SRU40: 33792
  - Configured with SRU60: 33792
  - Configured with SRU80: 34816
  - Configured with SRU100: 34816
  - Configured with SRU100E: 34816
  - Configured with SRU200: 34816
  - Configured with SRU200E: 34816
  - Configured with SRU400: 34816
- AR3600 series (SRUX5): 34816

Format

limit *number*

undo limit

Parameters

Parameter	Description	Value
number	Specifies the maximum number of IGMP entries that can be created for an instance.	The value is an integer that ranges from: • 1 to 128 for the AR150&200 series • 1 to 3000 for the AR100&AR120&AR160&AR1200 series • 1 to 256 for the AR2201-48FE, AR2202-48FE, AR2204-27GE, AR2204-27GE-P, AR2204-51GE-P, AR2204-51GE-R, AR2204E, AR2204E-D and AR2204 • 1 to 20480 for the AR2220, and AR2220E • 1 to 34816 for the AR2204XE and AR2204XE-DC • AR2240C: 1 to 33792 • AR2240 series and AR3200 series (depending on the SRU model used on the router): – Configured with SRU40: 1 to 33792 – Configured with SRU60: 1 to 33792 – Configured with SRU80: 1 to 34816 – Configured with SRU100: 1 to 34816 – Configured with SRU100E: 1 to 34816 – Configured with SRU200: 1 to 34816 – Configured with SRU200E: 1 to 34816 – Configured with SRU400: 1 to 34816 • 1 to 34816 for the AR3600 series (SRUX5)

 Copyright © Huawei Technologies Co., Ltd.

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 for an instance.

When the number of IGMP entries reaches the limit, the system does not create any IGMP entries. To enable the router 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 in the public network instance or VPN instance view.

Example

Set the maximum number of IGMP entries that can be created in the public network instance to 126.

```
<Huawei> system-view
[Huawei] multicast routing-enable
[Huawei] igmp
[Huawei-igmp] limit 126
```

Set the maximum number of IGMP entries that can be created in VPN instance mvpn to 126.

```
<Huawei> system-view
[Huawei] multicast routing-enable
[Huawei] igmp vpn-instance mvpn
[Huawei-igmp-mvpn] limit 126
```

Related Topics

10.1.20 igmp limit

10.1.16 igmp global limit

10.7.28 multicast routing-enable

Copyright © Huawei Technologies Co., Ltd.

10.1.39 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. The network may be congested when this situation occurs.

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.

 Copyright © Huawei Technologies Co., Ltd.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command in the public network instance or VPN instance.

Precautions

- This command applies only to IGMPv2 and IGMPv3.
- A smaller response time allows the router 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
```

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

```
<Huawei> system-view
[Huawei] multicast routing-enable
[Huawei] igmp vpn-instance mvpn
[Huawei-igmp-mvpn] max-response-time 8
```

Related Topics

10.1.7 display igmp interface
10.1.21 igmp max-response-time
10.7.28 multicast routing-enable

10.1.40 proxy source-lifetime

Function

The **proxy source-lifetime** command sets the timeout period for an (S, G) entry that an IGMP proxy-capable router 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 router generates is 210 seconds.

Format

proxy source-lifetime *interval*

Copyright © Huawei Technologies Co., Ltd.

undo proxy source-lifetime

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

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

An IGMP proxy-capable router starts 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 router. An IGMP proxy interface starts a timer when receiving 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 in the public network instance or VPN instance view.

Example

In the public network instance, 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.

```
<Huawei> system-view
[Huawei] multicast routing-enable
[Huawei] igmp vpn-instance mvpn
[Huawei-igmp-mvpn] proxy source-lifetime 200
```

10.1.41 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.

Copyright © Huawei Technologies Co., Ltd.

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* | **acl-name** *acl-name* }

undo proxy source-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 in the range 2000 to 2999. The number of an advanced ACL is an integer in the range 3000 to 3999.
acl-name *acl-name*	Specifies the name of a named ACL. **NOTE** **acl-name** *acl-name* can only be the name of a named advanced ACL.	The value is a string of 1 to 32 case-sensitive characters without spaces. The value must start with a letter (case sensitive).

Views

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

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If an IGMP proxy-capable router needs to restrict multicast data packets sent from some multicast sources, run the **proxy source-policy** command 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 in the public network instance or VPN instance view.

Precautions

The **proxy source-policy** command takes effect on a device only when IGMP proxy is enabled on the device.

 Copyright © Huawei Technologies Co., Ltd.

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

In the public network instance, 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
```

In the public network instance, 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
```

In VPN instance mvpn, configure an IGMP proxy-capable router to accept the multicast data packets from multicast source 10.10.1.2 and discard the multicast data packets from 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 vpn-instance mvpn
[Huawei-igmp-mvpn] proxy source-policy 2001
```

Related Topics

10.1.24 igmp proxy

10.1.42 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.

 Copyright © Huawei Technologies Co., Ltd.

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

Format

proxy ssm-policy { *basic-acl-number* | **acl-name** *acl-name* }

undo proxy ssm-policy

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.
acl-name *acl-name*	Specifies the name of a named ACL. **NOTE** **acl-name** *acl-name* can only be the name of a named advanced ACL.	The value is a string of 1 to 32 case-sensitive characters without spaces. The value must start with a letter (case sensitive).

Views

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

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 group address in this range. Sometimes, the SSM group address range must be narrowed to ensure security of a multicast network, and sometimes, the SSM group address range needs to be expanded because the default SSM group addresses are insufficient. In these cases, configure an SSM group address range on IGMP proxy devices. 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 in the public network instance or VPN instance view.

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.

 Copyright © Huawei Technologies Co., Ltd.

- 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

In the public network instance, 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
```

In VPN instance mvpn, 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 vpn-instance mvpn
[Huawei-igmp-mvpn] proxy ssm-policy 2000
```

10.1.43 require-router-alert (IGMP)

Function

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

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

By default, the router 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

 Copyright © Huawei Technologies Co., Ltd.

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 router 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 in the public network instance or VPN instance.

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 router to discard IGMP messages without the Router-Alert option.

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

In VPN instance mvpn, configure the router to discard IGMP messages without the Router-Alert option.

```
<Huawei> system-view
[Huawei] multicast routing-enable
[Huawei] igmp vpn-instance mvpn
[Huawei-igmp-mvpn] require-router-alert
```

Related Topics

10.1.7 display igmp interface
10.1.28 igmp require-router-alert
10.7.28 multicast routing-enable

 Copyright © Huawei Technologies Co., Ltd.

10.1.44 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 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-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

 Copyright © Huawei Technologies Co., Ltd.

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 GE1/0/0.

```
<Huawei> reset igmp control-message counters interface gigabitethernet 1/0/0
```

Related Topics

10.1.2 display igmp control-message counters

10.1.45 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 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-instance	Deletes information about the hosts with IGMP-attached group memberships on interfaces in all instances.	-
all	Deletes information about all the hosts.	-

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
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 through IGMP on interfaces.

Example

Delete information about IGMP host 192.168.0.12 in group 232.1.1.1 on GE1/0/0.

```
<Huawei> reset igmp explicit-tracking interface gigabitethernet 1/0/0 host 192.168.0.12 group 232.1.1.1
```

Related Topics

10.1.3 display igmp explicit-tracking

10.1.46 reset igmp group

Function

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

Copyright © Huawei Technologies Co., Ltd.

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 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-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.
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.

 Copyright © Huawei Technologies Co., Ltd.

Views

User view

Default Level

3: Management level

Usage Guidelines

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

After IGMP entries on an interface are deleted, the interface can join the involved groups again.

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 dynamic IGMP entries on all interfaces.

```
<Huawei> reset igmp group all
```

Delete all dynamic IGMP entries on GE1/0/0.

```
<Huawei> reset igmp group interface gigabitethernet 1/0/0 all
```

Delete the IGMP entries of group 225.0.0.1 on GE1/0/0.

```
<Huawei> reset igmp group interface gigabitethernet 1/0/0 225.0.0.1
```

Delete IGMP entries of groups 225.1.1.0 to 225.1.1.255 on GE1/0/0.

```
<Huawei> reset igmp group interface gigabitethernet 1/0/0 225.1.1.0 mask 255.255.255.0
```

Related Topics

10.1.4 display igmp group

10.1.47 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* }] } }

Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Deletes group memberships established with SSM mapping in a specified VPN instance.	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-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

 Copyright © Huawei Technologies Co., Ltd.

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
```

Related Topics

10.1.13 display igmp ssm-mapping

10.1.48 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

Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

Usage Scenario

The IGMP querier robustness variable specifies the retransmission count of IGMP packets to minimize 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 queries sends General Query messages at startup

  When the querier starts, it sends General Query messages certain 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 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 certain 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 in the public network instance or VPN instance.

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.

 Copyright © Huawei Technologies Co., Ltd.

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

In VPN instance mvpn, set the robustness variable of an IGMP querier to 3.

```
<Huawei> system-view
[Huawei] multicast routing-enable
[Huawei] igmp vpn-instance mvpn
[Huawei-igmp-mvpn] robust-count 3
```

Related Topics

10.1.7 display igmp interface

10.1.29 igmp robust-count

10.7.28 multicast routing-enable

10.1.49 send-router-alert (IGMP)

Function

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

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

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

Copyright © Huawei Technologies Co., Ltd.

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 in the public network instance or VPN instance.

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 router to send IGMP messages without the Router-Alert option.

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

In VPN instance mvpn, configure the router to send IGMP messages without the Router-Alert option.

```
<Huawei> system-view
[Huawei] multicast routing-enable
[Huawei] igmp vpn-instance mvpn
[Huawei-igmp-mvpn] undo send-router-alert
```

Related Topics

10.1.7 display igmp interface

10.1.30 igmp send-router-alert

10.7.28 multicast routing-enable

10.1.43 require-router-alert (IGMP)

10.1.50 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*

Copyright © Huawei Technologies Co., Ltd.

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 in the public network instance or VPN instance.

Precautions

 Copyright © Huawei Technologies Co., Ltd.

- You can run this command several times to configure multiple static SSM mapping entries.
- 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
```

In VPN instance mvpn, 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 vpn-instance mvpn
[Huawei-igmp-mvpn] ssm-mapping 225.5.5.5 32 10.8.8.8
```

Related Topics

10.1.13 display igmp ssm-mapping
10.1.31 igmp ssm-mapping enable
10.7.28 multicast routing-enable
10.3.79 ssm-policy (IPv4)

10.1.51 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

 Copyright © Huawei Technologies Co., Ltd.

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 in the public network instance or VPN instance.

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.

 Copyright © Huawei Technologies Co., Ltd.

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

In VPN instance mvpn, set the other querier present timer to 200 seconds.

```
<Huawei> system-view
[Huawei] multicast routing-enable
[Huawei] igmp vpn-instance mvpn
[Huawei-igmp-mvpn] timer other-querier-present 200
```

Related Topics

10.1.7 display igmp interface

10.1.33 igmp timer other-querier-present

10.7.28 multicast routing-enable

10.1.52 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

Copyright © Huawei Technologies Co., Ltd.

An IGMP querier sends IGMP General Query messages at an interval to check whether a local network segment has group members. This interval is the general query interval. You can set the general query interval based on situations on your network. The general query interval affects the following processes:

- When the querier starts, it sends General Query messages certain 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 in the public network instance or VPN instance.

Precautions

- The querier is more sensitive when it sends General Query messages at a shorter interval. However, more bandwidth and router 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 public network instance, 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
```

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

```
<Huawei> system-view
[Huawei] multicast routing-enable
[Huawei] igmp vpn-instance mvpn
[Huawei-igmp-mvpn] timer query 125
```

Related Topics

10.1.7 display igmp interface

10.1.34 igmp timer query

10.7.28 multicast routing-enable

 Copyright © Huawei Technologies Co., Ltd.

10.1.53 ttl-check (IPv4)

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 the device to check the TTL values in received IGMP Report, Leave, and Query messages on all interfaces.

```
<Huawei> system-view
[Huawei] igmp
[Huawei-igmp] ttl-check
```

10.2 MLD Configuration Commands

NOTE

AR120 series do not support this function.

 Copyright © Huawei Technologies Co., Ltd.

10.2.1 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
```

 Copyright © Huawei Technologies Co., Ltd.

```
Timer query: 125 s
Version: 2
```

Table 10-20 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. To set the interval for sending Multicast Address Specific Query messages or Multicast Address and Source Specific Query messages, run 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. To set the maximum response time for MLD Query messages, run 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 device checks the Router-Alert option in the received MLD message. To set whether the device checks the Router-Alert option in the received MLD message, run 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. To set the robustness variable of an MLD querier, run 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 device carry the Router-Alert option. To set whether the MLD messages sent from the device carry the Router-Alert option, run the **send-router-alert (MLD view)** command in the MLD view or the **mld send-router-alert** command in the interface view.

Copyright © Huawei Technologies Co., Ltd.

Item	Description
Ssm-mapping	Whether SSM mapping is enabled. To enable SSM mapping, run the **mld ssm-mapping enable** command in the interface view.
Timer query	Interval for sending MLD General Query messages. To set the interval for sending MLD General Query messages, run 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 filtering policy is configured. To configure a multicast group filtering policy, run 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. To configure the fast leave function, run 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.
Static-group	Whether static multicast groups are configured. To configure a static multicast group on an interface, run the **mld static-group** command.
Version	MLD version number. MLD has two versions: MLDv1 and MLDv2. To set the MLD version, run the **mld version** command.

Copyright © Huawei Technologies Co., Ltd.

10.2.2 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 GE1/0/0.

```
<Huawei> display mld control-message counters interface gigabitethernet 1/0/0
Interface message counter information
 GigabitEthernet1/0/0(FE80::219:74FF:FE59:3302):
 Message Type             Sent       Valid      Invalid    Ignore
 ----------------------------------------------------------------
 General Query            45         0          0          0
```

 Copyright © Huawei Technologies Co., Ltd.

```
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 10-21 Description of the display mld control-message counters interface gigabitethernet 1/0/0 command output

Item	Description
Interface message counter information	Statistics about MLD messages on an interface.
GigabitEthernet1/0/0(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.
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.

 Copyright © Huawei Technologies Co., Ltd.

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

Related Topics

10.2.36 reset mld control-message counters

10.2.3 display mld explicit-tracking

Function

The **display mld explicit-tracking** command displays information about the MLDv2 hosts that join the specific source and 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*]]

 Copyright © Huawei Technologies Co., Ltd.

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.
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

None

Example

Display information about the MLDv2 hosts that join the specific source and group in INCLUDE mode.

```
<Huawei> display mld explicit-tracking
Explicit-tracking information
```

 Copyright © Huawei Technologies Co., Ltd.

```
Total 2 hosts, 4 entries

GigabitEthernet1/0/0(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 10-22 Description of the display mld explicit-tracking command output

Item	Description
Explicit-tracking information	Host information.
Total 2 hosts, 4 entries	Two hosts and four (S, G) entries in total.
GigabitEthernet1/0/0(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.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
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.

Related Topics

10.2.37 reset mld explicit-tracking

10.2.4 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**

Copyright © Huawei Technologies Co., Ltd.

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
```

 Copyright © Huawei Technologies Co., Ltd.

```
Limited entry of this VPN-Instance: -
GigabitEthernet1/0/0(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 in the public network instance.

```
<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 10-23 Description of the display mld group verbose command output

Item	Description
Total entry on this router	Total number of dynamic MLD multicast groups on the router.
Interface group report information of VPN-Instance	VPN instance to which the group carried in the Multicast Listener Report message received on the interface belongs.
Limited entry of this VPN-Instance	Maximum number of MLD entries that can be created for this instance.
GigabitEthernet1/0/0(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.
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.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
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 multicast group.
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 multicast groups, that is, exclude or include.
Version1-host-present-timer-expiry	Timeout period of an MLDv1 host.

Related Topics

10.2.38 reset mld group

10.2.5 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**]

Copyright © Huawei Technologies Co., Ltd.

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.	-

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

 Copyright © Huawei Technologies Co., Ltd.

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: -
 GigabitEthernet1/0/0(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 the multicast groups configured with SSM mapping that hosts dynamically join in the public network instance.

```
<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 10-24 Description of the display mld group ssm-mapping verbose command output

Item	Description
Total entry on this router	Number of multicast group entries established with SSM mapping on the router.
Interface group report information of VPN-Instance	VPN instance to which the multicast group on the interface belongs.
Limited entry of this VPN-Instance	Maximum number of multicast group entries that can be generated in the VPN instance.
GigabitEthernet1/0/0(FE80::DD:84)	Interface type and interface number (IPv6 link-local address).
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.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
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	Scheduled time after which a group is deleted from the MLD group list.
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 Last Listener Query messagesMulticast 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.

Related Topics

10.2.42 ssm-mapping (MLD view)
10.2.39 reset mld group ssm-mapping

10.2.6 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**]

Copyright © Huawei Technologies Co., Ltd.

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.	-
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.	-

 Copyright © Huawei Technologies Co., Ltd.

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:GE1/0/0
  State:UP
  Expires:Never

  (*, FF25:100::1)
  Interface:GE1/0/0
  State:UP
  Expires:Never
```

Table 10-25 Description of the display mld group static command output

Item	Description
Static join group information	Information about the MLD multicast groups that a router statically joins.
Total 2 entries, Total 2 active entries	Total number of static multicast groups and active entries set on the router.
(*, FF25::1)	(*, G) entry.
Interface:GE1/0/0	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
```

 Copyright © Huawei Technologies Co., Ltd.

```
00001.(*, FF25::1)
    Total List of 2 joined interfaces
    1.GigabitEthernet0/0/1
        State:            UP
        Reference Count:  1
        Multicast Boundary:YES
        Outgoing Interface:YES
    2.GigabitEthernet0/0/2
        State:            UP
        Reference Count:  1
        Multicast Boundary:YES
        Outgoing Interface:YES
```

Table 10-26 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.GigabitEthernet0/0/1	Type and number of the interface.
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.
Outgoing Interface	Whether the downstream interfaces exist.

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.GigabitEthernet0/0/1
     2.GigabitEthernet0/0/2
 00002.(FC00:0:0:1::1,FF25::1)
     Total List of 2 joined interfaces
     Total Matched 2 interfaces
```

 Copyright © Huawei Technologies Co., Ltd.

```
  1.GigabitEthernet0/0/1
  2.GigabitEthernet0/0/2
```

Table 10-27 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 10-28 Description of the display mld group static interface-number command output

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

Related Topics

10.2.30 mld static-group

10.2.7 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**]

Copyright © Huawei Technologies Co., Ltd.

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 GE1/0/0.

```
<Huawei> display mld interface gigabitethernet 1/0/0 verbose
Interface information
 GigabitEthernet1/0/0(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
```

 Copyright © Huawei Technologies Co., Ltd.

```
 SSM-Mapping: enabled
 Startup-query-timer-expiry: off
 Other-querier-present-timer-expiry: off
 TTL-check: disabled
Total 2 MLD Groups reported
```

Table 10-29 Description of the display mld interface verbose command output

Item	Description
GigabitEthernet1/0/0(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.
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.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
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 messages (Last listener query), in seconds. To set the interval for sending Last listener query, run the **mld lastlistener-queryinterval** command.
Value of startup query interval	Interval for sending Query messages when a querier starts, in seconds. The interval is one-fourth 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.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Require-router-alert	Whether the MLD packet without the Router-Alert option is discarded. To configure whether the MLD packet without the Router-Alert option is discarded, run the **mld require-router-alert** command.
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. To configure whether to filter Multicast Listener Report/Done messages based on host addresses, run 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. To enable fast leave, run the **mld prompt-leave** command.
SSM-Mapping	Whether SSM mapping is enabled. To enable SSM mapping, run the **mld ssm-mapping enable** command.
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.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
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 IGMP Report, Leave, and Query messages is enabled: • enabled • disabled
Total 2 MLD Groups reported	Two Multicast Listener Report messages are received on the interface.

Related Topics

10.2.16 mld enable
10.2.34 mld version
10.2.18 mld group-policy
10.2.21 mld limit
10.2.32 mld timer query
10.2.31 mld timer other-querier-present
10.2.22 mld max-response-time
10.2.20 mld lastlistener-queryinterval
10.2.27 mld robust-count
10.2.26 mld require-router-alert
10.2.28 mld send-router-alert
10.2.19 mld ip-source-policy
10.2.24 mld prompt-leave
10.2.29 mld ssm-mapping enable

10.2.8 display mld invalid-packet

Function

The **display mld invalid-packet** command displays statistics and details about invalid MLD packets received by a device.

 Copyright © Huawei Technologies Co., Ltd.

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.

 Copyright © Huawei Technologies Co., Ltd.

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 10-30 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.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
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          :  GigabitEthernet1/0/0
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 10-31 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.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
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.

Related Topics

10.8.12 multicast ipv6 invalid-packet

10.2.9 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.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
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 outgoing interfaces in MLD routing entries.	-
number	Specifies the number of outgoing interfaces. After this parameter is specified, the command displays information about the specified number of outgoing 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
```

 Copyright © Huawei Technologies Co., Ltd.

```
Total 2 entries

00001. (FC00:0:0:1::3, FF44::)
     List of 1 downstream interface in include mode
      GigabitEthernet1/0/0 (FE80::EE:53),
               Protocol: STATIC

00002. (*, FF55::)
     List of 1 downstream interface
      GigabitEthernet1/0/0 (FE80::EE:53),
               Protocol: MLD
```

Table 10-32 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.
GigabitEthernet1/0/0(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.

10.2.10 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*] }

 Copyright © Huawei Technologies Co., Ltd.

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.
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 of VPN-Instance: public net
GigabitEthernet1/0/0(FE80::1)
```

Table 10-33 Description of the display mld ssm-mapping interface command output

Item	Description
Interface information of VPN-Instance: public net	VPN instance to which the interface enabled with SSM mapping belongs. Currently, only the public network instance is supported.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
GigabitEthernet1/0/0(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 10-34 Description of the display mld ssm-mapping group command output

Item	Description
MLD SSM-Mapping conversion table	MLD SSM mapping switching table.
Group	Address of a multicast group.
Number of Source(s)	Number of multicast sources configured with SSM mapping.
FC00:0:0:1::1::1	Multicast source address.

Check whether MLD SSM mapping is enabled on GE1/0/0.

```
<Huawei> display mld ssm-mapping interface GigabitEthernet 1/0/0
MLD SSM-Mapping is enabled
```

Table 10-35 Description of the display mld ssm-mapping interface GigabitEthernet 1/0/0 command output

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

Related Topics

10.2.29 mld ssm-mapping enable

10.2.42 ssm-mapping (MLD view)

10.2.11 display mld ssm-mapping interface

Function

The **display mld ssm-mapping interface** command displays information about interfaces enabled with SSM mapping.

Copyright © Huawei Technologies Co., Ltd.

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.	-
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 of VPN-Instance: public net
 GigabitEthernet1/0/0(FE80::1)
```

Table 10-36 Description of the display mld ssm-mapping interface command output

Item	Description
Interface information of VPN-Instance: public net	VPN instance to which the interface enabled with SSM mapping belongs. Currently, only the public network instance is supported.
GigabitEthernet1/0/0(FE80::1)	Interface type and interface number (IPv6 link-local address).

 Copyright © Huawei Technologies Co., Ltd.

10.2.12 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.

Copyright © Huawei Technologies Co., Ltd.

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. If the querier receives no Multicast Listener Report message within the maximum response time, 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
```

Related Topics

10.2.20 mld lastlistener-queryinterval

10.2.27 mld robust-count

10.2.40 robust-count (MLD view)

10.2.13 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.

By default, the maximum number of MLD entries that can be created on the entire router varies according to device models:

- AR100&AR120&AR150&AR160&AR200 series: 64
- AR1200 series, AR2201, AR2202, and AR2204: 128
- AR2220, AR2240C, and AR2220E: 256
- AR2204XE and AR2204XE-DC: 512
- AR2240 and AR3200 series:
  - Configured with SRU40: 256

Copyright © Huawei Technologies Co., Ltd.

  - Configured with SRU60: 256
  - Configured with SRU80: 512
  - Configured with SRU100: 512
  - Configured with SRU100E: 512
  - Configured with SRU200: 4000
  - Configured with SRU200E: 4000
  - Configured with SRU400: 4000
- AR3600 series (SRUX5): 4000

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 64 for the AR100&AR120&AR150&AR160&AR200 series. • 1 to 128 for the AR1200 series, AR2201, AR2202, and AR2204. • 1 to 256 for the AR2220, AR2240C, and AR2220E. • 1 to 512 for the AR2204XE and AR2204XE-DC • AR2240 and AR3200 series (depending on the SRU model used on the router): – Configured with SRU40: 1 to 256 – Configured with SRU60: 1 to 256 – Configured with SRU80: 1 to 512 – Configured with SRU100: 1 to 512 – Configured with SRU100E: 1 to 512 – Configured with SRU200: 1 to 4000 – Configured with SRU200E: 1 to 4000 – Configured with SRU400: 1 to 4000 • 1 to 4000 for the AR3600 series (SRUX5)

Views

MLD view

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

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 does not create any more. To enable the router 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 **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 60 globally.

```
<Huawei> system-view
[Huawei] multicast ipv6 routing-enable
[Huawei] mld
[Huawei-mld] limit 60
```

Related Topics

10.2.21 mld limit
10.2.17 mld global limit

10.2.14 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*

Copyright © Huawei Technologies Co., Ltd.

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. The network is congested.

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 value of the timer ranges from 0 to 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.

 Copyright © Huawei Technologies Co., Ltd.

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
```

Related Topics

10.2.22 mld max-response-time

10.2.15 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.

Example

Enter the MLD view.

```
<Huawei> system-view
[Huawei] multicast ipv6 routing-enable
```

 Copyright © Huawei Technologies Co., Ltd.

```
[Huawei] mld
[Huawei-mld]
```

Related Topics

10.8.16 multicast ipv6 routing-enable

10.2.16 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

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.

Copyright © Huawei Technologies Co., Ltd.

Example

Enable MLD on GE1/0/0 connected to a user network segment.

```
<Huawei> system-view
[Huawei] multicast ipv6 routing-enable
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] mld enable
```

Related Topics

10.8.16 multicast ipv6 routing-enable

10.2.17 mld global limit

Function

The **mld global limit** command sets the maximum number of MLD entries that can be created on the entire router.

The **undo mld global limit** command deletes the configured maximum number of MLD entries.

By default, the maximum number of MLD entries that can be created on the entire router varies according to device models:

- AR100&AR120&AR150&AR160&AR200 series: 64
- AR1200 series, AR2201, AR2202, and AR2204: 128
- AR2220, AR2240C, and AR2220E: 256
- AR2204XE and AR2204XE-DC: 512
- AR2240 and AR3200 series:
  - Configured with SRU40: 256
  - Configured with SRU60: 256
  - Configured with SRU80: 512
  - Configured with SRU100: 512
  - Configured with SRU100E: 512
  - Configured with SRU200: 4000
  - Configured with SRU200E: 4000
  - Configured with SRU400: 4000
- AR3600 series (SRUX5): 4000

Format

mld global limit *number*

undo mld global limit

Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
number	Specifies the maximum number of MLD entries that can be created on the entire router.	The value is a decimal integer that ranges from: • 1 to 64 for the AR100&AR120&AR150&AR160&AR200 series. • 1 to 128 for the AR1200 series, AR2201, AR2202, and AR2204. • 1 to 256 for the AR2220, AR2240C, and AR2220E. • 1 to 512 for the AR2204XE and AR2204XE-DC • AR2240 and AR3200 series (depending on the SRU model used on the router): – Configured with SRU40: 1 to 256 – Configured with SRU60: 1 to 256 – Configured with SRU80: 1 to 512 – Configured with SRU100: 1 to 512 – Configured with SRU100E: 1 to 512 – Configured with SRU200: 1 to 4000 – Configured with SRU200E: 1 to 4000 – Configured with SRU400: 1 to 4000 • 1 to 4000 for the AR3600 series (SRUX5)

Views

System 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 more. To enable the router 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

 Copyright © Huawei Technologies Co., Ltd.

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 **igmp 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 router to 60.

```
<Huawei> system-view
[Huawei] multicast ipv6 routing-enable
[Huawei] mld global limit 60
```

Related Topics

10.2.13 limit (MLD view)

10.2.21 mld limit

10.2.18 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* | **acl6-name** *acl6-name* } [**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.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
acl6-name *acl6-name*	Specifies the name of a named ACL6. **NOTE** **acl6-name** *acl6-name* can only be the name of a named advanced ACL.	The value is a string of 1 to 32 case-sensitive characters without spaces. The value must start with a letter (case sensitive).
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

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 ACL6 in the **mld group-policy** command as a filter to specify the range of multicast groups served by the interface. This configuration improves security of the MLD application. You can also run this command to prevent router from receiving Multicast Listener Report messages for specified groups.

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.

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.

 Copyright © Huawei Technologies Co., Ltd.

- 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 router, the router 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 GE1/0/0 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 1/0/0
[Huawei-GigabitEthernet1/0/0] mld group-policy 2005
```

Create an ACL6 named **myacl6**, and configure a rule that allows hosts to receive data of multicast groups in the range of FF13::101. Configure an MLD group policy on GE1/0/0 and reference the ACL6 to allow hosts connected to the interface to join only the specified multicast groups.

```
<Huawei> system-view
[Huawei] acl ipv6 name myacl6
[Huawei-acl6-adv-myacl6] rule permit ipv6 destination ff13::101 128
[Huawei-acl6-adv-myacl6] quit
[Huawei] multicast ipv6 routing-enable
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] mld group-policy acl6-name myacl6
```

10.2.19 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* | **acl6-name** *acl6-name* }

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.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
acl6-name *acl6-name*	Specifies the name of a named ACL6. **NOTE** **acl6-name** *acl6-name* can only be the name of a named advanced ACL.	The value is a string of 1 to 32 case-sensitive characters without spaces. The value must start with a letter (case sensitive).

Views

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. To improve security, 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.

Example

Configure GE1/0/0 to receive 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 1/0/0
[Huawei-GigabitEthernet1/0/0] mld ip-source-policy 2001
```

Related Topics

10.2.7 display mld interface

10.8.16 multicast ipv6 routing-enable

10.2.20 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.

Copyright © Huawei Technologies Co., Ltd.

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

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. If the querier receives no Multicast Listener Report message within the maximum response time, 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

 Copyright © Huawei Technologies Co., Ltd.

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 GE1/0/0.

```
<Huawei> system-view
[Huawei] multicast ipv6 routing-enable
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] mld lastlistener-queryinterval 3
```

Related Topics

10.2.12 lastlistener-queryinterval (MLD view)
10.2.27 mld robust-count
10.2.40 robust-count (MLD view)

10.2.21 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.

By default, the maximum number of MLD entries that can be created on the current interface varies according to device models:

- AR100&AR120&AR150&AR160&AR200 series: 64
- AR1200 series, AR2201, AR2202, and AR2204: 128
- AR2220, AR2240C, and AR2220E: 256
- AR2204XE and AR2204XE-DC: 512
- AR2240 and AR3200 series:
  - Configured with SRU40: 256
  - Configured with SRU60: 256
  - Configured with SRU80: 512
  - Configured with SRU100E: 512
  - Configured with SRU200: 1024
  - Configured with SRU200E: 1024
  - Configured with SRU400: 2048
- AR3600 series (SRUX5): 1024

Copyright © Huawei Technologies Co., Ltd.

Format

mld limit *number* [**except** { *acl6-number* | **acl6-name** *acl6-name* }]

undo mld limit

Parameters

Parameter	Description	Value
number	Specifies the maximum number of MLD entries that the current interface can create.	The value is an integer that ranges from: ● 1 to 64 for the AR100&AR120&AR150&AR160&AR200 series. ● 1 to 128 for the AR1200 series, AR2201, AR2202, and AR2204. ● 1 to 256 for the AR2220, AR2240C, and AR2220E. ● 1 to 512 for the AR2204XE and AR2204XE-DC ● AR2240 and AR3200 series (depending on the SRU model used on the router): – Configured with SRU40: 1 to 256 – Configured with SRU60: 1 to 256 – Configured with SRU80: 1 to 512 – Configured with SRU100E: 1 to 512 – Configured with SRU200: 1 to 1024 – Configured with SRU200E: 1 to 1024 – Configured with SRU400: 1 to 2048 ● 1 to 1024 for the AR3600 series (SRUX5)
except	Specifies the range of multicast groups that are not limited by the set 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.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
acl6-name *acl6-name*	Specifies the name of a named ACL6. **NOTE** **acl6-name** *acl6-name* can only be the name of a named advanced ACL.	The value is a string of 1 to 32 case-sensitive characters without spaces. The value must start with a letter (case sensitive).

Views

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 make the router allow more new join requests, delete some 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

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

 Copyright © Huawei Technologies Co., Ltd.

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.

Example

Set the maximum number of MLD entries that can be created on the GE1/0/0 to 60.

```
<Huawei> system-view
[Huawei] multicast ipv6 routing-enable
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] mld limit 60
```

Create the advanced ACL6 with the number being 3100; set the maximum number of MLD entries that can be created on GE1/0/0 to 60; 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 gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] mld limit 60 except 3100
```

Related Topics

10.2.17 mld global limit
10.2.13 limit (MLD view)

10.2.22 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

Copyright © Huawei Technologies Co., Ltd.

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

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. The network is congested.

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 value of the timer ranges from 0 to 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.

 Copyright © Huawei Technologies Co., Ltd.

Example

Set the maximum response time for MLD General Query messages to 8 seconds on GE1/0/0.

```
<Huawei> system-view
[Huawei] multicast ipv6 routing-enable
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] mld max-response-time 8
```

Related Topics

10.2.14 max-response-time (MLD view)

10.2.23 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

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. After MLD on-demand is configured on the querier,

 Copyright © Huawei Technologies Co., Ltd.

the querier does not send Query messages, 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. The querier does not send Query messages to collect membership information, 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.

IPv6 function has been enabled using the **ipv6 enable (interface view)** command in the interface view.

Precautions

- 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. The entries will never age out.
  - When the interface receives a Multicast Listener Done message, it deletes the corresponding MLD group entry.

Example

Enable the MLD on-demand function on GE1/0/0.

```
<Huawei> system-view
[Huawei] ipv6
[Huawei] multicast ipv6 routing-enable
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] ipv6 enable
[Huawei-GigabitEthernet1/0/0] mld on-demand
```

10.2.24 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.

Copyright © Huawei Technologies Co., Ltd.

Format

mld prompt-leave [**group-policy** { *acl6-number* | **acl6-name** *acl6-name* }]

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.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
acl6-name *acl6-name*	Specifies the name of a named ACL6. **NOTE** **acl6-name** *acl6-name* can only be the name of a named advanced ACL.	The value is a string of 1 to 32 case-sensitive characters without spaces. The value must start with a letter (case sensitive).

Views

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.

 Copyright © Huawei Technologies Co., Ltd.

Example

Configure fast leave on GE1/0/0.

```
<Huawei> system-view
[Huawei] multicast ipv6 routing-enable
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] mld prompt-leave
```

Create an ACL6 named **myacl6**. Configure fast leave on GE1/0/0 and apply the **myacl6** to allow the interface to immediately leave multicast group FF13::101 defined in the **myacl6**.

```
<Huawei> system-view
[Huawei] acl ipv6 name myacl6
[Huawei-acl6-adv-myacl6] rule permit ipv6 destination ff13::101 128
[Huawei-acl6-adv-myacl6] quit
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] mld prompt-leave group-policy acl6-name myacl6
```

10.2.25 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* | **acl6-name** *acl6-name* }

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.
acl6-name *acl6-name*	Specifies the name of an ACL6. **NOTE** **acl6-name** *acl6-name* can only be the name of a named advanced ACL.	The value is a string of 1 to 32 case-sensitive characters without spaces. The value must start with a letter (case sensitive).

Views

Interface view

Copyright © Huawei Technologies Co., Ltd.

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 response 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. After this function is configured on a device, the device 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 GE1/0/0 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 1/0/0
[Huawei-GigabitEthernet1/0/0] mld query ip-source-policy 2001
```

10.2.26 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.

Copyright © Huawei Technologies Co., Ltd.

Format

mld require-router-alert

undo mld require-router-alert

Parameters

None

Views

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 GE1/0/0 to discard MLD messages without the Router-Alert option.

```
<Huawei> system-view
[Huawei] multicast ipv6 routing-enable
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] mld require-router-alert
```

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

10.2.28 mld send-router-alert
10.2.35 require-router-alert (MLD view)

10.2.27 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

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 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

 Copyright © Huawei Technologies Co., Ltd.

When a querier starts, it sends General Query messages certain 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 certain 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 certain 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 GE1/0/0 to 3.

```
<Huawei> system-view
[Huawei] multicast ipv6 routing-enable
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] mld robust-count 3
```

Related Topics

10.2.12 lastlistener-queryinterval (MLD view)

10.2.20 mld lastlistener-queryinterval

10.2.32 mld timer query

10.2.40 robust-count (MLD view)

10.2.44 timer query (MLD view)

Copyright © Huawei Technologies Co., Ltd.

10.2.28 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

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

By default, the router sends MLD messages that contain the Router-Alert option in IPv6 headers. If the router 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 router 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.

 Copyright © Huawei Technologies Co., Ltd.

Example

Configure GE1/0/0 to send MLD messages with the Router-Alert option.

```
<Huawei> system-view
[Huawei] multicast ipv6 routing-enable
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] mld send-router-alert
```

Related Topics

10.2.26 mld require-router-alert
10.2.41 send-router-alert (MLD view)

10.2.29 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

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 router. MLD SSM mapping is implemented based on static SSM mapping entries on the router. The router 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.

 Copyright © Huawei Technologies Co., Ltd.

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.

Example

Enable MLD SSM mapping on GE1/0/0.

```
<Huawei> system-view
[Huawei] multicast ipv6 routing-enable
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] mld ssm-mapping enable
```

Related Topics

10.2.5 display mld group ssm-mapping

10.2.42 ssm-mapping (MLD view)

10.2.30 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*] }

Copyright © Huawei Technologies Co., Ltd.

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.
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

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can configure static multicast groups on user-side interfaces of the router in some scenarios, for example:

- There are long-term group members on a shared network segment, and the router needs to forward multicast data to these group members quickly and steadily.

 Copyright © Huawei Technologies Co., Ltd.

- 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 router considers that the multicast group always has members on the network segment of the interface. Therefore, the router 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 at a time 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 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 router 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.

Example

Configure static multicast group FF13::101 on GE1/0/0.

```
<Huawei> system-view
[Huawei] multicast ipv6 routing-enable
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] mld static-group ff13::101
```

Configure the router to forward multicast packets from multicast source FC00::101 to multicast group FF14::202 through GE1/0/0.

```
<Huawei> system-view
[Huawei] multicast ipv6 routing-enable
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] mld static-group ff14::202 source fc00::101
```

Add GE1/0/0 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 gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] mld static-group ff25::1 inc-step-mask 24 number 2
```

 Copyright © Huawei Technologies Co., Ltd.

Add GE1/0/0 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 gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] mld static-group ff33::1 inc-step-mask 24 number 2 source fc00::101
```

10.2.31 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

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

 Copyright © Huawei Technologies Co., Ltd.

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 GE1/0/0, set the other querier present timer to 200 seconds.

```
<Huawei> system-view
[Huawei] multicast ipv6 routing-enable
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] mld timer other-querier-present 200
```

Related Topics

10.2.7 display mld interface

10.2.43 timer other-querier-present (MLD view)

10.2.32 mld timer query

10.2.32 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.

Copyright © Huawei Technologies Co., Ltd.

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

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

An MLD querier sends MLD General Query messages at an interval to check whether a local network segment has multicast group members. This interval is the general query interval. You can set the general query interval based on the network situation. The general query interval affects the following processes:

- When a querier starts, it sends General Query messages certain 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 one-fourth 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 router 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

 Copyright © Huawei Technologies Co., Ltd.

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 GE1/0/0 sends General Query messages to 200 seconds.

```
<Huawei> system-view
[Huawei] multicast ipv6 routing-enable
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] mld timer query 200
```

Related Topics

10.2.27 mld robust-count

10.2.40 robust-count (MLD view)

10.2.44 timer query (MLD view)

10.2.33 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

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To protect a device against MLD message attacks, run the **mld ttl-check** command to enable the device to check the TTL values in received MLD Report,

 Copyright © Huawei Technologies Co., Ltd.

Done, and Query messages on a specific interface and discard such a message if its TTL value is not 1.

The **mld ttl-check** command provides the same function as the **ttl-check** command run in the MLD view, except that the **ttl-check** command configuration takes effect for all interfaces.

Configuration Impact

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 the device to check the TTL values in received MLD Report, Done, and Query messages on a specific interface.

```
<Huawei> system-view
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] mld ttl-check
```

10.2.34 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

Interface view

Default Level

2: Configuration level

Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

Usage Scenario

A multicast router can identify MLD messages of a version earlier than its own MLD version but cannot identify MLD messages of a later version. To ensure normal MLD operation, ensure that the router runs the same MLD version as receiver hosts or a later MLD version.

If many routers exist on a shared network segment, configure the same MLD version on all router 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 GE1/0/0.

```
<Huawei> system-view
[Huawei] multicast ipv6 routing-enable
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] mld version 2
```

10.2.35 require-router-alert (MLD view)

Function

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

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

By default, the router 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

Copyright © Huawei Technologies Co., Ltd.

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 router 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
```

Related Topics

10.2.26 mld require-router-alert

10.2.36 reset mld control-message counters

Function

The **reset mld control-message counters** command deletes statistics of MLD messages.

Copyright © Huawei Technologies Co., Ltd.

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.	-
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 GE1/0/0.

```
<Huawei> reset mld control-message counters interface gigabitethernet 1/0/0
```

Related Topics

10.2.2 display mld control-message counters

10.2.37 reset mld explicit-tracking

Function

The **reset mld explicit-tracking** command deletes hosts that dynamically join a multicast group using MLD from an interface.

Copyright © Huawei Technologies Co., Ltd.

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 FF80:: to FF80: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.

 Copyright © Huawei Technologies Co., Ltd.

Example

Delete the host FE80::101 that joins multicast group FF23::101 through MLD on GE1/0/0.

```
<Huawei> reset mld explicit-tracking interface gigabitethernet 1/0/0 host fe80::101 group ff23::101
```

Delete the host FE80::101 that joins the (FC00:0:0:1::12, FF23::101) forwarding entry from GE1/0/0.

```
<Huawei> reset mld explicit-tracking interface gigabitethernet 1/0/0 host fe80::101 group ff23::101 source fc00:0:0:1::12
```

Related Topics

10.2.3 display mld explicit-tracking

10.2.38 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.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
ipv6-group-mask-length	Specifies the mask length of the 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 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 GE1/0/0.

```
<Huawei> reset mld group interface gigabitethernet 1/0/0 ff03::101:0 112
```

Related Topics

10.2.4 display mld group

10.2.39 reset mld group ssm-mapping

Copyright © Huawei Technologies Co., Ltd.

10.2.39 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 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.

Views

User view

Copyright © Huawei Technologies Co., Ltd.

Default Level

3: Management level

Usage Guidelines

This command is valid on the multicast groups that the interface dynamically joins only, and only the MLDv1 multicast group entries within the range of SSM group addresses are deleted.

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 GE1/0/0.

```
<Huawei> reset mld group ssm-mapping interface gigabitethernet 1/0/0 ff13::101:0 112
```

Related Topics

10.2.5 display mld group ssm-mapping

10.2.40 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.

Copyright © Huawei Technologies Co., Ltd.

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 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 certain 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 certain 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 certain 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

 Copyright © Huawei Technologies Co., Ltd.

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
```

Related Topics

10.2.12 lastlistener-queryinterval (MLD view)

10.2.20 mld lastlistener-queryinterval

10.2.27 mld robust-count

10.2.32 mld timer query

10.2.44 timer query (MLD view)

10.2.41 send-router-alert (MLD view)

Function

The **send-router-alert** command configures the router to send MLD messages containing the Router-Alert option in IPv6 headers.

The **undo send-router-alert** command disables the router from sending MLD messages containing the Router-Alert option in IPv6 headers.

By default, MLD messages sent by the router contain the Router-Alert option.

Format

send-router-alert

undo send-router-alert

Parameters

None

Views

MLD view

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

Usage Scenario

By default, MLD messages sent by the router contain the Router-Alert option in their IPv6 headers. If the router needs to communicate with a device that does not support the Router-Alert option, run the **undo send-router-alert** command to configure the router 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 router 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
```

Related Topics

10.2.28 mld send-router-alert

10.2.35 require-router-alert (MLD view)

10.2.42 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*] }

Copyright © Huawei Technologies Co., Ltd.

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 repeatedly run the **ssm-mapping** command to configure multiple static SSM mapping entries.
- 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.

Copyright © Huawei Technologies Co., Ltd.

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
```

10.2.43 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

 Copyright © Huawei Technologies Co., Ltd.

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
```

Related Topics

10.2.31 mld timer other-querier-present

10.2.44 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

Copyright © Huawei Technologies Co., Ltd.

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 sends MLD General Query messages at an interval to check whether a local network segment has multicast group members. This interval is the general query interval. You can set the general query interval based on the network situation. The general query interval affects the following processes:

- When a querier starts, it sends General Query messages certain 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 one-fourth 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 router 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.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> system-view
[Huawei] multicast ipv6 routing-enable
[Huawei] mld
[Huawei-mld] timer query 200
```

Related Topics

10.2.32 mld timer query

10.2.27 mld robust-count

10.2.40 robust-count (MLD view)

10.2.45 ttl-check (IPv6)

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] mld
[Huawei-mld] ttl-check
```

 Copyright © Huawei Technologies Co., Ltd.

10.3 PIM (IPv4) Configuration Commands

NOTE

AR120 series do not support this function.

10.3.1 anycast-rp (IPv4)

Function

The **anycast-rp** command configures an Anycast RP and displays the Anycast-RP view or directly displays the existing Anycast-RP view.

The **undo anycast-rp** command deletes the configurations of an Anycast RP.

By default, no Anycast RP is configured.

Format

anycast-rp *rp-address*

undo anycast-rp *rp-address*

Parameters

Parameter	Description	Value
rp-address	Indicates the Anycast RP address.	The value is in dotted decimal notation. This address must be a valid unicast IP address and cannot be an address on the network segment 127.0.0.0/8.

Views

PIM view of public network instance or PIM view of VPN instance

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In a traditional PIM-SM domain, all multicast groups map to one RP. When the network is overloaded or traffic concentrates on an RP, the RP may be overburdened. If the RP fails, routes are converged slowly or multicast packets are forwarded over non-optimal paths.

Configuring the Anycast RP in the PIM-SM domain can address this problem. IP routing will automatically select the topologically closest RP for each source and receiver. This releases burdens on RPs, implements RP backup, and optimizes the forwarding paths.

 Copyright © Huawei Technologies Co., Ltd.

Currently, the Anycast RP can be implemented in a PIM domain by using the following schemes:

- MSDP Anycast RP, which is applicable to IPv4 networks
- PIM Anycast RP, which is applicable to IPv4 networks

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command in the public network instance or VPN instance.

Configuration Impact

If PIM Anycast RP is configured, after an RP receives a Register message, it checks the source address of the Register message. If the Register message is sent by the source's DR, the RP forwards the Register message to Anycast RP peers. If the Register message is sent by an Anycast RP peer, it does not forward the Register message. In such a manner, Anycast RP peers can learn source/group information from each other.

Precautions

- In IPv4 network deployment, you can choose either of the two schemes. Mixed use of the two schemes is not recommended.
- The Anycast RP address must be the same as that of the elected RP on the current network.
- In a single instance, you can configure a maximum of four Anycast RP addresses on each device.
- Either static or dynamic RPs can be used on the network. Configuring RPs on loopback interfaces is recommended. You need to configure the same RP address on the devices to be deployed with the Anycast RP. If the dynamic RP is used on the network, before configuring an Anycast RP address, run the **display pim rp-info** command to check the address of the RP on the current network.

Example

Set the Anycast RP address to 10.10.10.10 in the public network instance and enter the Anycast-RP view.

```
<Huawei> system-view
[Huawei] multicast routing-enable
[Huawei] pim
[Huawei-pim] anycast-rp 10.10.10.10
[Huawei-pim-anycast-rp-10.10.10.10]
```

Related Topics

10.3.43 local-address (IPv4)

10.3.45 peer (IPv4)

10.3.30 display pim rp-info

Copyright © Huawei Technologies Co., Ltd.

10.3.2 auto-rp listening enable

Function

The **auto-rp listening enable** command enables the auto-RP listening function. A device receives auto-RP announcement and discovery messages and learns RP information from the messages.

The **undo auto-rp listening enable** command restores the default configuration.

By default, auto-RP listening is disabled.

Format

auto-rp listening enable

undo auto-rp listening enable

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 auto-RP listening function enables the device to receive auto-RP announcement and discovery messages and learn RP information from the messages. After receiving an Auto-RP Advertisement or Discovery message, the device obtains the source address of the message, and then performs reverse path forwarding (RPF) check based on the source address. If the RPF check fails, the device discards the packet. If the RPF check succeeds, the device forwards the packet to other PIM neighbors.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command in the public network instance or VPN instance.

Example

In the public network instance, enable auto-RP listening on a router.

```
<Huawei> system-view
[Huawei] multicast routing-enable
[Huawei] pim
[Huawei-pim] auto-rp listening enable
```

 Copyright © Huawei Technologies Co., Ltd.

10.3.3 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 in the public network instance or VPN instance.

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

 Copyright © Huawei Technologies Co., Ltd.

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 it can solve the problem faced by IP fragmentation that all fragments become unavailable due to loss of fragment information.

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.

```
<Huawei> system-view
[Huawei] multicast routing-enable
[Huawei] pim
[Huawei-pim] bsm semantic fragmentation
```

10.3.4 bsr-policy (IPv4)

Function

The **bsr-policy** command specifies the range of valid bootstrap router (BSR) addresses. Then the router 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* | **acl-name** *acl-name* }

undo bsr-policy

 Copyright © Huawei Technologies Co., Ltd.

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.
acl-name *acl-name*	Specifies the name of a named ACL. **NOTE** **acl-name** *acl-name* can only be the name of a named advanced ACL.	The value is a string of 1 to 32 case-sensitive characters without spaces. The value must start with a letter (case sensitive).

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 router as a C-BSR to elect the BSR. Once being elected as the BSR, the router is responsible for advertising RP information in the network. To prevent the valid BSR from being maliciously replaced, use the following measures:

- Certain hosts try changing the RP mapping to spoof the router by forging BSR packets.

  Solution: The attack often occurs on edge routers because the BSR packet is a multicast packet and the TTL value of the BSR packet is 1. The BSR is inside the network, and hosts are outside the network. The routers can perform neighbor check and RPF check on the received BSR packets to prevent the attack.
- Certain attackers control the router on the network, or the router accesses the network. The attackers configure the router as a C-BSR, and help the router win the BSR election. The attackers obtain the right of advertising RP information in the network.

  Solution: After the router is configured as a C-BSR, the router spreads BSR packets in the network. The BSR packets are multicast packets. The TTL value of BSR packets is 1. The BSR packets are forwarded hop by hop. As long as the neighboring router cannot receive the packets, the packets are not spread in the entire network. The solution is to use the **bsr-policy** command on every router in the network to limit the valid BSR range. For example, only routers 10.1.1.1/32 and 10.1.1.2/32 are elected as BSRs; therefore, the routers do not receive or forward other BSR packets. This type of attack is prevented.

 Copyright © Huawei Technologies Co., Ltd.

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

IP multicast routing has been enabled using the **multicast routing-enable** command in the public network instance or VPN instance.

Configuration Impact

After the **bsr-policy** command is run, the router 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.

When you use the **rule** command to configure a filtering rule for the Named ACL, the rule is effective only within the source address range specified by the **source** parameter and within the time period specified by the **time-range** parameter.

Example

In the public network instance, 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
```

In the public network instance, use a Named ACL to configure address 10.1.1.0/24 as the valid BSR address range.

```
<Huawei> system-view
[Huawei] acl name myacl
[Huawei-acl-adv-myacl] rule permit ip source 10.1.1.0 0.0.0.255
[Huawei-acl-adv-myacl] quit
[Huawei] pim
[Huawei-pim] bsr-policy acl-name myacl
```

10.3.5 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

 Copyright © Huawei Technologies Co., Ltd.

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. The BSR 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 better than the current BSR, the C-BSR replaces its BSR address with the address of the BSR carried in the received Bootstrap message.

 Copyright © Huawei Technologies Co., Ltd.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command in the public network instance or VPN instance.

Before configuring an interface as a C-BSR, enable PIM-SM on the interface.

Example

In the public network instance, configure a C-BSR on GE1/0/0.

```
<Huawei> system-view
[Huawei] multicast routing-enable
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] pim sm
[Huawei-GigabitEthernet1/0/0] quit
[Huawei] pim
[Huawei-pim] c-bsr gigabitethernet 1/0/0
```

Related Topics

10.3.13 c-rp (IPv4)

10.3.62 pim sm

10.3.6 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

Copyright © Huawei Technologies Co., Ltd.

By default, each PIM-SM domain has only one 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. 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, serving all the remained 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 equals 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 equals 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 router.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command in the public network instance or VPN instance.

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, 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
```

Related Topics

10.3.5 c-bsr (IPv4)

10.3.7 c-bsr global

Function

The **c-bsr global** command configures the router as a C-BSR in the global domain.

The **undo c-bsr global** command restores the default configuration.

Copyright © Huawei Technologies Co., Ltd.

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

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 router as a C-BSR in the global domain. The BSR in the global domain is generated through election.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command in the public network instance or VPN instance.

Precautions

The **c-bsr global** command takes effect only in a BSR administrative domain. This means that the **c-bsr global** command can enable a device in a BSR administrative domain to accept multicast data of group out of the BSR administrative domain.

The **c-bsr global** command needs to be used together with the **c-bsr admin-scope** command.

 Copyright © Huawei Technologies Co., Ltd.

Example

In the public network instance, configure the router 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
```

Related Topics

10.3.6 c-bsr admin-scope
10.3.8 c-bsr group
10.3.12 c-bsr priority (IPv4)

10.3.8 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.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
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 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.

Example

In the public network instance, 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
```

Related Topics

10.3.6 c-bsr admin-scope

10.3.7 c-bsr global

10.3.12 c-bsr priority (IPv4)

 Copyright © Huawei Technologies Co., Ltd.

10.3.9 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 router 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 in the public network instance or VPN instance.

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

Copyright © Huawei Technologies Co., Ltd.

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, 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
```

Related Topics

10.3.5 c-bsr (IPv4)

10.3.7 c-bsr global

10.3.8 c-bsr group

10.3.10 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

Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

Usage Scenario

After a C-BSR is elected as the BSR, the C-BSR periodically sends Bootstrap messages carrying the IP address of the C-BSR 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 hold time. 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 fail the previous election elect a new BSR. Services are not interrupted.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command in the public network instance or VPN instance.

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 60 seconds and the default holdtime is 130s.

Example

In the 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
```

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

10.3.5 c-bsr (IPv4)

10.3.11 c-bsr interval (IPv4)

10.3.11 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, the C-BSR periodically sends Bootstrap messages carrying the IP address of the C-BSR 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.

Copyright © Huawei Technologies Co., Ltd.

- If the timer times out, the BSR is considered to be faulty. The C-BSRs that fail in the election triggers a new BSR election. Services are not interrupted.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command in the public network instance or VPN instance.

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 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 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
```

Related Topics

10.3.5 c-bsr (IPv4)

10.3.10 c-bsr holdtime (IPv4)

10.3.12 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*

 Copyright © Huawei Technologies Co., Ltd.

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 router with the highest priority wins in the BSR election.
- In the case of the same priority, the router 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 in the public network instance or VPN instance.

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 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
```

Related Topics

10.3.5 c-bsr (IPv4)

Copyright © Huawei Technologies Co., Ltd.

10.3.8 c-bsr group
10.3.7 c-bsr global

10.3.13 c-rp (IPv4)

Function

The **c-rp** command configures the router 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* | **acl-name** *acl-name* } | **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.
acl-name *acl-name*	Specifies the name of a named ACL. **NOTE** **acl-name** *acl-name* can only be the name of a named advanced ACL.	The value is a string of 1 to 32 case-sensitive characters without spaces. The value must start with a letter (case sensitive).

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
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 the public network instance or PIM view of the VPN instance

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

An RP is the core of a PIM-SM or Bidir-PIM domain, and therefore a C-RP must be able to communicate with the other devices in the PIM-SM or Bidir-PIM domain. You are advised to configure a C-RP on the core router and reserve enough bandwidth between the router and each of the other devices in the PIM-SM or Bidir-PIM domain.

An RP is elected from multiple C-RPs following these rules:

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. If multiple C-RPs have the same priority, the C-RP with the largest hash value wins.
4. If all the preceding factors are the same, the C-RP with the largest address wins.

Prerequisites

- IP multicast routing has been enabled using the **multicast routing-enable** command in the public network instance or VPN instance.
- PIM-SM has been enabled on the interface that acts as the C-RP.

Configuration Impact

 Copyright © Huawei Technologies Co., Ltd.

An interface is specified in the command; therefore, the settings of **group-policy** { *basic-acl-number* | **acl-name** *acl-name* }, **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.

Example

In the 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
```

In the public network instance, use named ACL **myacl** to specify Loopback 0 as the C-RP of PIM-SM multicast 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 name myacl
[Huawei-acl-adv-myacl] rule permit ip destination 225.1.0.0 0.0.255.255
[Huawei-acl-adv-myacl] rule permit ip destination 226.2.0.0 0.0.255.255
[Huawei-acl-adv-myacl] 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 acl-name myacl priority 10
```

Related Topics

10.3.5 c-bsr (IPv4)

 Copyright © Huawei Technologies Co., Ltd.

10.3.14 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 in the public network instance or VPN instance.

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.

Copyright © Huawei Technologies Co., Ltd.

Example

In the 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
```

Related Topics

10.3.13 c-rp (IPv4)

10.3.15 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

Copyright © Huawei Technologies Co., Ltd.

IP multicast routing has been enabled using the **multicast routing-enable** command in the public network instance or VPN instance.

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 hold time 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 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
```

Related Topics

10.3.13 c-rp (IPv4)

10.3.16 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

Copyright © Huawei Technologies Co., Ltd.

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The following rules are used to elect an RP from multiple C-RPs:

- The C-RP with the interface address that has the longest mask wins.
- The C-RP with highest priority wins.
- In case of the same priority, hash functions are operated. The C-RP with the greatest calculated value wins.
- If all the preceding factors are the same, 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 in the public network instance or VPN instance.

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 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
```

Related Topics

10.3.13 c-rp (IPv4)

10.3.17 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.

 Copyright © Huawei Technologies Co., Ltd.

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* | **acl-name** *acl-name* }

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.
acl-name *acl-name*	Specifies the name of a named ACL. **NOTE** **acl-name** *acl-name* can only be the name of a named advanced ACL.	The value is a string of 1 to 32 case-sensitive characters without spaces. The value must start with a letter (case sensitive).

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 router 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 as the RP-set, and floods it through BSR messages on the entire network. The local router then works out the RP serving a specific multicast group address range according to the RP-set.

To protect valid C-RP from being spoofed, configure **crp-policy** on BSR routers 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 in the public network instance or VPN instance.

Configuration Impact

 Copyright © Huawei Technologies Co., Ltd.

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.

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
```

Use a named ACL to configure a C-RP policy on the C-BSR : only 10.1.1.1/32 can function as the C-RP, and the C-RP is allowed to service only the multicast groups in the range of 225.1.0.0/16.

```
<Huawei> system-view
[Huawei] acl name myacl
[Huawei-acl-adv-myacl] rule permit ip source 10.1.1.1 0 destination 225.1.0.0 0.0.255.255
[Huawei-acl-adv-myacl] quit
[Huawei] multicast routing-enable
[Huawei] pim
[Huawei-pim] crp-policy acl-name myacl
```

10.3.18 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

 Copyright © Huawei Technologies Co., Ltd.

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 neighbor-policy: disabled
```

Table 10-37 Description of the **display default-parameter pim-dm** command output

Item	Description
PIM View Default Configurations	Indicates default configurations in the PIM view.
Hello-option dr-priority	Indicates the priority for DR election. This parameter is configured by the **hello-option dr-priority (IPv4)** command.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Hello-option holdtime	Indicates the 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	Indicates the 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	Indicates whether neighbor tracking is enabled. This parameter is configured by the **hello-option neighbor-tracking (IPv4)** command.
Hello-option override-interval	Indicates the interval for sending Prune Override messages. This parameter is configured by the **hello-option override-interval (IPv4)** command.
Holdtime assert	Indicates the time period for holding the Assert state. This parameter is configured by the **holdtime assert (IPv4)** command.
Holdtime join-prune	Indicates the time period for holding the Join or Prune state. This parameter is configured by the **holdtime join-prune (IPv4)** command.
Source-lifetime	Indicates the timeout period of an (S, G) entry. This parameter is configured by the **source-lifetime (IPv4)** command.
State-refresh-interval	Indicates the interval for sending State-Refresh messages. This parameter is configured by the **state-refresh-interval (IPv4)** command.
State-refresh-rate-limit	Indicates the 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	Indicates the TTL value of the State-Refresh message. This parameter is configured by the **state-refresh-ttl (IPv4)** command.

Copyright © Huawei Technologies Co., Ltd.

Item	Description
Hello periodic interval	Indicates the interval for sending Hello messages. This parameter is configured by the **timer hello (IPv4)** command.
Join-prune periodic interval	Indicates the interval for sending Join/Prune messages. This parameter is configured by the **timer join-prune (IPv4)** command.
Interface View Default Configurations	Indicates the default configurations in the interface view.
Pim bfd	Indicates the PIM BFD on an interface. This parameter is configured by the**pim bfd enable** command.
Pim hello-option dr-priority	Indicates the priority for DR election on the interface. This parameter is configured by the **pim hello-option dr-priority** command.
Pim hello-option holdtime	Indicates the 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	Indicates the 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	Indicates 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	Indicates the interval for the interface to send Prune Override messages. This parameter is configured by the **pim hello-option override-interval** command.
Pim holdtime assert	Indicates the time period for the interface to hold the Assert state. This parameter is configured by the **pim holdtime assert** command.
Pim holdtime join-prune	Indicates the time period for the interface to hold the Join or Prune state. This parameter is configured by the **pim holdtime join-prune** command.

Copyright © Huawei Technologies Co., Ltd.

Item	Description
Pim require-genid	Indicates whether the received Hello message is required to carry the Generation ID. This parameter is configured by the **pim require-genid** command.
Pim silent	Indicates whether PIM Silent is enabled on the interface. This parameter is configured by the **pim silent** command.
Pim state-refresh-capable	Indicates whether State-Refresh is enabled on the interface. This parameter is configured by the **pim state-refresh-capable** command.
Pim timer dr-switch-delay	Indicates whether the DR switch delay is set on the interface. This parameter is configured by the **pim timer dr-switch-delay** command.
Pim timer graft-retry	Indicates the interval for the interface to retransmit Graft messages. This parameter is configured by the **pim timer graft-retry** command.
Pim hello periodic interval	Indicates the interval for the interface to send Hello messages. This parameter is configured by the **pim timer hello** command.
Pim join-prune periodic interval	Indicates the interval for the interface to send Join/Prune messages. This parameter is configured by the **pim timer join-prune** command.
Pim triggered-hello-delay	Indicates the maximum delay for the interface to send Hello messages. This parameter is configured by the **pim triggered-hello-delay** command.
Pim version	Indicates the version of PIM enabled on the interface.
Pim neighbor-policy	Indicates whether the neighbor-policy is set on the interface. This parameter is configured by the **pim neighbor-policy** command.

Copyright © Huawei Technologies Co., Ltd.

10.3.19 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
```

 Copyright © Huawei Technologies Co., Ltd.

```
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 join-policy: disabled
Pim neighbor-policy: disabled
```

Table 10-38 Description of the **display default-parameter pim-sm** command output

Item	Description
PIM View Default Configurations	Default configurations in the PIM view.
Auto-rp listening enable	Whether auto-RP listening is enabled. This parameter is configured by the **auto-rp listening enable** command.
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.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
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.
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.

Copyright © Huawei Technologies Co., Ltd.

Item	Description
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.
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.

Copyright © Huawei Technologies Co., Ltd.

Item	Description
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.
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.

Copyright © Huawei Technologies Co., Ltd.

Item	Description
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.
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 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.

 Copyright © Huawei Technologies Co., Ltd.

10.3.20 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
```

 Copyright © Huawei Technologies Co., Ltd.

```
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 join-policy: disabled
Pim neighbor-policy: disabled
```

Table 10-39 Description of the **display default-parameter pim-ssm** 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, 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.
Source-lifetime	Timeout period of an (S, G) entry, in seconds. This parameter is configured by the **source-lifetime (IPv4)** command.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
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.
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.

Copyright © Huawei Technologies Co., Ltd.

Item	Description
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.
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.
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.

Copyright © Huawei Technologies Co., Ltd.

Item	Description
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.

10.3.21 display pim bfd session

Function

The **display pim bfd session** command displays the information about PIM BFD sessions.

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 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-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.

Copyright © Huawei Technologies Co., Ltd.

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 GE 0/0/1 in the public network instance.

```
<Huawei> display pim bfd session interface gigabitethernet 0/0/1
 VPN-Instance: public net

 GigabitEthernet0/0/1 (12.1.1.2): Total 1 BFD session Created

 Neighbor        ActTx(ms) ActRx(ms) ActMulti Local/Remote State
 12.1.1.1        1000      1000      3         8192/8192   Up
```

Display PIM BFD sessions on GE 0/0/1 in the public network instance when the router is not enabled with global BFD.

```
<Huawei> display pim bfd session interface gigabitethernet 0/0/1
 VPN-Instance: public net

 GigabitEthernet0/0/1 (12.1.1.2): Total 1 BFD session Created

 Neighbor        ActTx(ms) ActRx(ms) ActMulti Local/Remote State
 12.1.1.1        --        --        --          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 public network instance neighbor 10.1.2.3.

```
<Huawei> display pim bfd session neighbor 10.1.2.3
 VPN-Instance: public net

 GigabitEthernet0/0/1 (12.1.1.2)

 Neighbor        ActTx(ms) ActRx(ms) ActMulti Local/Remote State
 12.1.1.1        1000      1000      3         8192/8192   Up
```

Table 10-40 Description of the **display pim bfd session** command output

Item	Description
VPN-Instance	Indicates the VPN instance to which PIM BFD session information belongs.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
GigabitEthernet0/0/1 (12.1.1.2)	Indicates the PIM interface name (the IP address).
Neighbor	Indicates the IP address of a PIM neighbor.
ActTx (ms)	Indicates the actual minimum transmission interval, in milliseconds.
ActRx (ms)	Indicates the actual minimum receiving interval, in milliseconds.
ActMulti	Indicates the actual local detection multiple.
Local/Remote	Indicates the local and remote discriminators.
State	Indicates the 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	Indicates the total number of PIM BFD sessions in a public network instance or a VPN instance.
Total 1 PIM BFD session up	Indicates the number of PIM BFD sessions in the Up state in a public network instance or a VPN instance.
Total 0 PIM BFD session down	Indicates the 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.

10.3.22 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**

 Copyright © Huawei Technologies Co., Ltd.

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 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-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 router in the domain to view the BSR information.

- If the current router is configured with the C-BSR, the command output includes information about the elected BSR and locally configured C-BSR.
- If the current router 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 of the current public network instance. If the router 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
```

 Copyright © Huawei Technologies Co., Ltd.

```
    Uptime: 00:01:46
    Expires: 00:02:02
    C-RP Count: 1
```

Display information about BSR in the current PIM-SM of the current public network instance.

If the router 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 10-41 Description of the **display pim bsr-info** command output

Item	Description
VPN-Instance	Indicates the VPN instance to which BSR information belongs.
Elected AdminScoped BSR Count	Indicates the number of elected AdminScoped BSRs.
Elected BSR Address	Indicates the address of the elected BSR. **NOTE** If stably running devices in the same BSR domain display different values in the **Elected BSR Address** field, the elected BSR is incorrect. Contact technical support personnel to troubleshoot faults.
Priority	Indicates the priority of the BSR. By default, the value is 0.
Hash mask length	Indicates the mask length in the RP hash calculation.
State	Indicates the status of the BSR.
Scope	Indicates the 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.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Uptime	Indicates the period during which the BSR exists.
Expires	Indicates the remaining time of the BSR.
C-RP Count	Indicates the number of RPs learned through the BSR.
Next BSR message scheduled at	Indicates the period after which the next BSR message is sent. BSR messages are sent only when the timer maintained by the elected BSR times out.
Candidate AdminScoped BSR Count	Indicates the number of AdminScoped C-BSRs.
Candidate BSR Address	Indicates the address of the C-BSR.
Wait to be BSR	Indicates 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 router exceeds the threshold, the value is 1.

Related Topics

10.3.5 c-bsr (IPv4)
10.3.13 c-rp (IPv4)

10.3.23 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*]

Copyright © Huawei Technologies Co., Ltd.

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 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-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 unicast routes used by PIM, such as 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: GigabitEthernet2/0/0, 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)
```

 Copyright © Huawei Technologies Co., Ltd.

Table 10-42 Description of the **display pim claimed-route** command output

Item	Description
VPN-Instance	Indicates the VPN instance to which the unicast routing information corresponds.
multicast load-splitting rule	Indicates the way 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 This parameter is configured by the **multicast load-splitting** command.
RPF information about: 10.1.0.0 in PIM-SM routing table	Indicates the RPF routing information with the source address of 10.1.0.0 in the PIM-SM routing table
RPF interface	Indicates the RPF interface.
RPF neighbor	Indicates the RPF neighbor.
Referenced route/mask	Indicates the referenced route/mask.
Referenced route type	Indicates the type of route.
RPF-route selecting rule	Indicates the preferred rule for selecting the RPF-route.
The (S,G) or (*,G) list dependent on this route entry	Indicates the list of multicast entries based on RPF routes.

Related Topics

10.7.13 display multicast rpf-info

10.3.24 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** }

Copyright © Huawei Technologies Co., Ltd.

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 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-instance	Indicates all the instances.	-
message-type	Indicates a PIM control message type.	-
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

 Copyright © Huawei Technologies Co., Ltd.

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 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 router.

Example

Display the statistics about sent, received, and invalid PIM control messages in the public network instance.

```
<Huawei> display pim control-message counters
 VPN-Instance: public net
 Register* - Register Anycast-RP, Probe* - Probe Anycast-RP
 ------------------------------------------------------------------------------
 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
 Register*        0                0                0                0
 Probe*           0                0                0                0

 PIM control-message counters for interface: GigabitEthernet1/0/1
 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: GigabitEthernet1/0/2
 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 statistics about sent, received, invalid PIM control messages on GE1/0/0 in the public network instance.

```
<Huawei> display pim control-message counters interface GigabitEthernet 1/0/0
 VPN-Instance: public net
 PIM control-message counters for interface: GigabitEthernet1/0/0
 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
```

 Copyright © Huawei Technologies Co., Ltd.

```
State-Refresh    0              0              0          0
BSR              9778           0              0          0
```

Table 10-43 Description of the **display pim control-message counters** command output

Item	Description
VPN-Instance	VPN instance to which the statistics of PIM messages belong.
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	Statistics about Register messages.
Register-Stop	Statistics about Register-Stop messages.
Probe	Statistics about Probe messages.
C-RP	Statistics about CRP messages.
Register*	Statistics about Register messages for anycast RP.
Probe*	Statistics about Probe messages for anycast RP.
Assert	Statistics about Assert messages.
Graft	Statistics about Graft messages.
Graft-Ack	Statistics about Graft-Ack messages.
Hello	Statistics about Hello messages.
Join-prune	Statistics about Join/Prune messages.
State-Refresh	Statistics about State-Refresh messages.
BSR	Statistics about Bootstrap messages.

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

10.3.74 reset pim control-message counters

10.3.25 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 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-instance	Specifies all the instances.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

In PIM-DM, after sending the Graft message, the router 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 in the public network instance.

```
<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
```

 Copyright © Huawei Technologies Co., Ltd.

Table 10-44 Description of the **display pim grafts** command output

Item	Description
VPN-Instance	Indicates the VPN instance to which the Graft messages belong.
Source	Indicates the multicast source address.
Group	Indicates the multicast group address.
Expire	Indicates the timeout period of an (S, G) entry.
RetransmitIn	Indicates the waiting period before the next Graft message is received.

10.3.26 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 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-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.	-
verbose	Displays detailed information about a PIM interface.	-

 Copyright © Huawei Technologies Co., Ltd.

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, the following situations occur:

- If *interface-type interface-number* is specified, the information about various PIM state parameters on the interface is displayed.
- If *interface-type interface-number* is not specified, the information about the state parameters of all the PIM interfaces is displayed.
- If **up** is set in the command, the information about the parameters of the PIM interfaces in the Up state is displayed.
- If **down** is set in the command, the information about the parameters of the PIM interfaces in the Down state is displayed.

Example

Display information about all the PIM interfaces in the public network instance.

```
<Huawei> display pim interface
 VPN-Instance: public net
 Interface      State   NbrCnt   HelloInt   DR-Pri     DR-Address
 GE1/0/0         up      1         30          1          10.1.1.2
 GE2/0/0         up      0         30          1          10.1.2.2    (local)
 Loopback0        up       0          30           1           10.1.3.2    (local)
```

Table 10-45 Description of the **display pim interface** command output

Item	Description
VPN-Instance	VPN instance to which the PIM interface belongs.
Interface	Name of the PIM interface.
State	Status of the PIM interface, Up or Down.
NbrCnt	Number of PIM neighbors on the interface.
HelloInt	Interval for sending Hello messages, in seconds.
DR-Pri	DR priority.
DR-Address	DR address.

Copyright © Huawei Technologies Co., Ltd.

Display detailed information about PIM on GE1/0/0 of the public network instance.

```
<Huawei> display pim interface gigabitethernet 1/0/0 verbose
 VPN-Instance: public net
 Interface: GigabitEthernet1/0/0, 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 BFD min-tx-interval: 1000 ms
    PIM BFD min-rx-interval: 1000 ms
    PIM BFD detect-multiplier: 3
    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: -
```

Table 10-46 Description of the **display pim interface verbose** command output

Item	Description
VPN-Instance	VPN instance to which the PIM interface belongs.
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.
PIM DR Priority (configured)	DR priority configured on the interface.
PIM neighbor count	Number of PIM neighbors on the interface.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
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 PIM Silent function is enabled on the interface.
PIM neighbor tracking (negotiated)	Whether the PIM neighbor tracking function is enabled on the interface after negotiation.
PIM neighbor tracking (configured)	Whether the PIM neighbor tracking function is configured on the interface.
PIM generation ID	Generation ID option on the interface.
PIM require-GenID	Whether the function that rejects the Hello messages without the Generation ID option is enabled.
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 domain boundary is configured on the interface.
PIM BFD	Whether PIM BFD is enabled.
PIM BFD min-tx-interval	Minimum interval for sending BFD packets.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
PIM BFD min-rx-interval	Minimum interval for receiving BFD packets.
PIM BFD detect-multiplier	PIM BFD detection multiplier.
PIM dr-switch-delay timer	DR switching delay.
Number of routers on link not using DR priority	Number of routers 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 routers 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 router 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.

10.3.27 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**

 Copyright © Huawei Technologies Co., Ltd.

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 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-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 router.	-
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.	-
register-stop	Displays statistics about invalid Register-Stop messages.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
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 device fails to create PIM entries, you can run the **display pim invalid-packet** command first to check whether the device 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 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 in the public network instance.

```
<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

AnycastRP Register invalid packet:
Invalid Multicast Source: 0           Invalid Multicast Group : 0
```

 Copyright © Huawei Technologies Co., Ltd.

```
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 10-47 Description of the **display pim invalid-packet** command output

Item	Description
Statistics of invalid packets for public net	VPN instance in which statistics about invalid PIM messages need to be displayed.
PIM General invalid packet	General invalid PIM messages.
Invalid PIM Version	Messages with invalid PIM versions.
Invalid PIM Type	Messages with invalid PIM message types.
Fault Length	Messages of invalid lengths.
Bad Checksum	Messages with invalid checksum.
PIM Register invalid packet	Invalid PIM Register messages.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Invalid Multicast Source	Messages with invalid multicast source addresses.
Invalid Multicast Group	Messages with invalid multicast group addresses.
Invalid Dest Addr	Messages with invalid destination addresses.
AnycastRP Register invalid packet	Statistics about invalid Register messages in the anycast-RP scenario.
PIM Register-Stop invalid packet	Invalid PIM Register-Stop messages.
IP Source not RP	Messages whose source addresses are not the RP address.
PIM CRP invalid packet	Invalid PIM C-RP messages.
Invalid CRP Addr	Messages with invalid C-RP addresses.
CRP Adv Fault Length	Messages whose CRP Adv fields are of invalid lengths.
PIM Assert invalid packet	Invalid PIM Assert messages.
Invalid IP Source Addr	Indicates messages with invalid source addresses.
PIM BSR invalid packet	Invalid PIM BSR messages.
Bad Payload	Messages with invalid payloads.
Bad Scope Mask	Messages with invalid scope masks.
Not CBSR But BSR	BSR messages received on interfaces that do not act as a C-BSR.
Invalid BSR Addr	Messages with invalid BSR addresses.
Fault Hash Length	Messages with hash mask fields of invalid lengths.
PIM Hello invalid packet	Indicates invalid PIM Hello messages.
Invalid Addr List	Indicates messages with invalid address lists.
Bad Holdtime Length	Messages with Holdtime fields of invalid lengths.
Bad LanPruneDelay Length	Messages with LanPruneDelay fields of invalid lengths.
Bad DrPriority Length	Messages with DrPriority fields of invalid lengths.
Bad GenID Length	Messages with GenerationID fields of invalid lengths.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
PIM Join/Prune invalid packet	Invalid PIM Join/Prune messages.
Invalid Up Neighbor	Messages with invalid upstream neighbors.
PIM Graft invalid packet	Invalid PIM Graft messages.
PIM Graft-Ack invalid packet	Invalid PIM Graft-Ack messages.
PIM State Refresh invalid packet	Invalid PIM State-Refresh messages.
Invalid Originator Addr	Messages with invalid Originator address.

Display details of one invalid PIM message recently received in the public network instance.

```
<Huawei> display pim invalid-packet 1 verbose
      Detailed information of invalid packets
----------------------------------------------------------
Packet information (Index 1):
----------------------------------------------------------
Interface          :  GigabitEthernet1/0/0
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 10-48 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.

 Copyright © Huawei Technologies Co., Ltd.

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.

Related Topics

10.7.23 multicast invalid-packet

10.3.28 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**] *

Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Specifies the name of a VPN instance.	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-instance	Specifies all the instances.	-
interface *interface-type interface-number*	Specifies the type and number of an interface.	-
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 router.

Example

Display information about all PIM neighbors in the public network instance.

```
<Huawei> display pim neighbor
 VPN-Instance: public net
 Total Number of Neighbors = 2

 Neighbor        Interface     Uptime      Expires     Dr-Priority  BFD-Session
```

 Copyright © Huawei Technologies Co., Ltd.

```
10.1.1.2        GE1/0/0         02:50:49    00:01:31    1           Y
10.1.2.2        GE2/0/0         02:49:39    00:01:42    1           Y
```

Table 10-49 Description of the **display pim neighbor** command output

Item	Description
VPN-Instance	VPN instance to which PIM neighbors belong.
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.
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.

Display detailed information about the PIM neighbor with IP address 10.1.1.2 in the public network instance.

```
<Huawei> display pim neighbor 192.168.11.1 verbose
 VPN-Instance: public net
 Neighbor: 192.168.11.1
    Interface: Vlanif11
    Uptime: 04:56:41
    Expiry time: 00:01:44
    DR Priority: 1
    Generation ID: 0XD287B917
    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 10-50 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.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
LAN delay	Delay in transmitting Prune messages.
Override interval	Override interval for a prune action.
Neighbor tracking	Whether the neighbor tracking function is enabled.
PIM BFD-Session	Whether the BFD session is 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-multipler	PIM BFD detection multiplier.

10.3.29 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* | **mcast-extranet** | **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* }] | **extranet** { **source-vpn-instance** { *vpn-instance-name* | **all** | **public** } | **receive-vpn-instance** { *vpn-instance-name* | **all** } } | **incoming-interface** { *interface-type interface-number* | **register** | **mcast-extranet** } | **outgoing-interface** { **include** | **exclude** | **match** } { *interface-type interface-number* | **register** | **none** } | **vpn-instance** *vpn-instance-name* | **mode** { **dm** | **sm** | **ssm** } | **flags** *flag-value* | **fsm**] * [**outgoing-interface-number** [*number*]] [**rpf-vector** [*vector-address*]]

NOTE

If you specify the **register** keyword before **mode**, the value of **mode** can only be **sm**.

After the PIM mode is set to **dm** or **ssm**, the **register** keyword cannot be specified in the command.

Copyright © Huawei Technologies Co., Ltd.

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 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-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.
extranet	Displays multicast extranet routing entries.	-
source-vpn-instance *vpn-instance-name*	Indicates the source VPN instance. *vpn-instance-name* specifies the name of the source VPN instance.	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	Indicates all instances.	-
public	Indicates the public network instance.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
receive-vpn-instance *vpn-instance-name*	Indicates the receiver VPN instance. *vpn-instance-name* specifies the name of the receiver VPN instance.	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.
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.	-
mcast-extranet	Indicates that the upstream interface is an extranet 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.	-
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.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
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.
rpf-vector *vector-address*	Displays detailed information about Reverse Path Forwarding (RPF) vectors. *vector-address* specifies the vector address.	The address mask is in dotted decimal notation.
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 10-51 lists the values of the **flags** *flag-value* parameter.

 Copyright © Huawei Technologies Co., Ltd.

Table 10-51 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 the router 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 router has receivers of the source specified in the (S, G) entry, and PIM is the owner of the downstream interfaces.
sgjoin	The router has receivers of the source specified in the (S, G) entry, but PIM is not the owner of the downstream interfaces.
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 waiting for data received from a new interface.
wc	(*, G) entry.

Example

Display the PIM routing table of the public network instance.

```
<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)
```

 Copyright © Huawei Technologies Co., Ltd.

```
RP: 10.2.2.2
Protocol: pim-sm, Flag: SPT LOC ACT
UpTime: 02:54:43
Upstream interface: GigabitEthernet1/0/0
    Upstream neighbor: NULL
    RPF prime neighbor: NULL
Downstream interface(s) information:
Total number of downstreams: 1
    1: GigabitEthernet2/0/0
        Protocol: pim-sm, UpTime: 02:54:43, Expires: 00:02:47
```

Table 10-52 Description of the **display pim routing-table** command output

Item	Description
VPN-Instance	VPN instance to which PIM routing information belongs.
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.
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.
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.

 Copyright © Huawei Technologies Co., Ltd.

Display the number of the downstream interfaces of PIM routing entries in the public network instance.

```
<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 10-53 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.

Display brief information about the PIM routing entries in the public network instance.

```
<Huawei> display pim routing-table brief
  VPN-Instance: public net
 Total 0 (*, G) entry; 6 (S, G) entries

 00001.(10.0.4.100, 225.0.0.1)
      Upstream interface:GigabitEthernet1/0/0
      Number of downstream:1
      Number of receive vrf:0
 00002.(10.0.4.100, 225.0.0.2)
      Upstream interface:GigabitEthernet1/0/0
      Number of downstream:1
      Number of receive vrf:0
 00003.(10.0.4.100, 225.0.0.3)
      Upstream interface:GigabitEthernet1/0/0
      Number of downstream:1
      Number of receive vrf:0
 00004.(10.0.4.100, 225.0.0.4)
      Upstream interface:GigabitEthernet1/0/0
      Number of downstream:1
      Number of receive vrf:0
 00005.(10.0.4.100, 225.0.0.5)
      Upstream interface:GigabitEthernet1/0/0
      Number of downstream:1
      Number of receive vrf:0
```

 Copyright © Huawei Technologies Co., Ltd.

```
00006.(10.0.4.100, 225.0.0.6)
    Upstream interface:GigabitEthernet1/0/0
    Number of downstream:1
    Number of receive vrf:0
```

Table 10-54 Description of the **display pim routing-table brief** command output

Item	Description
Total 0 (*, G) entry; 6 (S, G) entries	Total number of the (S, G) entries and (*, G) entries in the PIM routing table.
Upstream interface	Upstream interface in an (S, G) or (*, G) entry.
Number of downstream	Number of downstream interfaces.
Number of receive vrf	Number of receiving VRFs.

Related Topics

10.7.11 display multicast routing-table

10.3.30 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 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-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.

Copyright © Huawei Technologies Co., Ltd.

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, static RP, and auto-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.

```
<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 10-55 Description of the display pim rp-info command output

Item	Description
VPN-Instance	VPN instance to which RP information belongs.
PIM-SM BSR RP Number	Number of PIM-SM BSR RPs.
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.

Copyright © Huawei Technologies Co., Ltd.

Item	Description
Static RP	IP address of a static RP.

10.3.31 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.

NOTE

Only the AR3200 series routers support PIM GR.

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

On the PIM-SM network, after an active/standby switchover is performed on the router equipped with two MPUs, the new active MPU deletes original PIM forwarding entries. Because the active MPU on the router cannot create new PIM forwarding entries in a short time, multicast data transmission is interrupted.

PIM GR enables the router to back up join and prune information in PIM routing entries to the new MPU when an active/standby switchover is performed on the router. This ensures normal multicast data forwarding during restoration of the multicast distribution tree.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command in the public network instance or VPN instance.

 Copyright © Huawei Technologies Co., Ltd.

Precautions

At least one router interface is enabled with PIM-SM so that the **graceful-restart** command takes effect.

Example

Enable PIM GR in the public network instance.

```
<Huawei> system-view
[Huawei] multicast routing-enable
[Huawei] pim
[Huawei-pim] graceful-restart
```

Related Topics

10.3.32 graceful-restart period (IPv4)

10.3.32 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.

NOTE

Only the AR3200 series routers support PIM GR.

Format

graceful-restart period *period*

undo graceful-restart period

Parameters

Parameter	Description	Value
period	Specifies the minimum PIM GR period.	It 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

Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

Usage Scenario

The **graceful-restart period** command ensures the minimal time for maintaining forwarding entries.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command in the public network instance or VPN instance.

Configuration Impact

If you run the **graceful-restart period** command multiple times, only the latest configuration takes effect.

Precautions

PIM GR is on the basis of unicast GR; therefore, the minimum PIM GR period should be longer than the corresponding unicast GR period.

The PIM GR period also depends on the complexity of the network topology and increases as the expansion of unicast route capacity and multicast route capacity.

Example

Set the minimum PIM GR period in the 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
```

Related Topics

10.3.31 graceful-restart (IPv4)

10.3.33 hello-option dr-priority (IPv4)

Function

The **hello-option dr-priority** command configures the priority of the router that candidates for the Designated Router (DR).

The **undo hello-option dr-priority** command restores the default priority.

By default, the priority of the router that candidates for the DR is 1.

Format

hello-option dr-priority *priority*

undo hello-option dr-priority

Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
priority	Specifies the priority of the router 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

In PIM, routers on the shared network segment candidates for the DR. The DR is responsible for the registering of the local multicast source and the joining of the receivers.

The DR election is based on the priority and the IP address. To elect the DR, the routers send the Hello message that contains the priority to each other. The router with the highest priority functions as the DR. If the routers have the same priority, the router with the largest IP address functions as the DR.

If there is at least one router that does not support Hello packets that contain the priority in the network, the DR election is based on the IP address of each router. The router with the largest IP address functions as the DR.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command in the public network instance or VPN instance.

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 public network instance, configure the DR priority of a router to 3.

```
<Huawei> system-view
[Huawei] multicast routing-enable
[Huawei] pim
[Huawei-pim] hello-option dr-priority 3
```

Related Topics

10.3.51 pim hello-option dr-priority

 Copyright © Huawei Technologies Co., Ltd.

10.3.34 hello-option holdtime (IPv4)

Function

The **hello-option holdtime** command sets the timeout period for a router 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 router 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 router 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 the PIM network, after the device receives a Hello message from its PIM neighbor, the device starts the timer. The timer value is the value of Holdtime in the Hello message. If the device does not receive any Hello message from its PIM neighbor after the timeout, the device considers the neighbor invalid or unreachable.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command in the public network instance or VPN instance.

Precautions

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.

Copyright © Huawei Technologies Co., Ltd.

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 public network instance, set the timeout interval to 120 seconds. The timeout interval is the period during which a router 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
```

Related Topics

10.3.52 pim hello-option holdtime

10.3.35 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

Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

Usage Scenario

Hello messages sent by routers carry **lan-delay** and **override-interval**. The **lan-delay** parameter indicates the delay in transmitting messages in the LAN. When the values of **lan-delay** on all routers on the same link are different, the maximum value of these values is used.

When a router sends a Prune message to the upstream router in the same network segment, if other router still requests the multicast data, it needs to send a Join message to the upstream router in the override-interval period.

The value of the Prune-Pending Timer (PPT) is obtained by the value of **lan-delay** plus the value of **override-interval**. PPT refers to the delay during which the current router receives a Prune message from the downstream interface and performs the prune action. If the router receives a Join message from the downstream interface in PPT, the router cancels the prune action.

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 PIM-SM and PIM-DM.

If the delay in transmitting Prune message is too short, the upstream router will stop forwarding multicast packets before the downstream router 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 public network instance.

```
<Huawei> system-view
[Huawei] multicast routing-enable
[Huawei] pim
[Huawei-pim] hello-option lan-delay 200
```

Related Topics

10.3.37 hello-option override-interval (IPv4)

10.3.55 pim hello-option override-interval

10.3.53 pim hello-option lan-delay

Copyright © Huawei Technologies Co., Ltd.

10.3.36 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 device generates a Generation ID and encapsulates it into the message. The Generation ID changes only when the device status changes. After receiving the Hello message, the neighboring device detects Generation ID change and immediately sends a Join message to the device to update the neighbor relationship. If multiple devices on the shared network segment 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. The upstream neighbor cannot update neighbor relationships with downstream devices because of 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 in the public network instance or VPN instance.

Precautions

 Copyright © Huawei Technologies Co., Ltd.

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 public network instance, enable the downstream neighbor tracking function.

```
<Huawei> system-view
[Huawei] multicast routing-enable
[Huawei] pim
[Huawei-pim] hello-option neighbor-tracking
```

Related Topics

10.3.54 pim hello-option neighbor-tracking

10.3.37 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

Copyright © Huawei Technologies Co., Ltd.

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Hello messages sent by routers carry **lan-delay** and **override-interval**. The **override-interval** parameter refers to the period during which a downstream router overrides the prune action.

When a router sends a Prune message to the upstream router in the same network segment, if other router still requests the multicast data, it needs to send a Join message to the upstream router in the override-interval period.

When the values of **override-interval** on all routers in the same network segment are different, the maximum value of these values is used.

The value of PPT is obtained by the value of **lan-delay** plus the value of **override-interval**. When receiving a Prune message from a downstream interface, the router does not perform the prune action until the PPT times out. If the router 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 in the public network instance or VPN instance.

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 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
```

Related Topics

10.3.35 hello-option lan-delay (IPv4)

10.3.53 pim hello-option lan-delay

10.3.55 pim hello-option override-interval

Copyright © Huawei Technologies Co., Ltd.

10.3.38 holdtime assert (IPv4)

Function

The **holdtime assert** command sets the timeout period for all PIM interfaces to keep the Assert state on the local router.

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 router 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 retains 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 in the public network instance or VPN instance.

Precautions

 Copyright © Huawei Technologies Co., Ltd.

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 public network instance, set the interval during which a router keeps the Assert state to 100s.

```
<Huawei> system-view
[Huawei] multicast routing-enable
[Huawei] pim
[Huawei-pim] holdtime assert 100
```

Related Topics

10.3.39 holdtime join-prune (IPv4)
10.3.57 pim holdtime join-prune
10.3.56 pim holdtime assert

10.3.39 holdtime join-prune (IPv4)

Function

The **holdtime join-prune** command sets the holdtime value in Join/Prune messages sent by all PIM interfaces. routers 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 router.	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

Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

Usage Scenario

After receiving a Join/Prune message from the downstream device, the router starts the holdtime timer. After the timeout interval, if the router does not receive subsequent Join/Prune messages from the downstream device, the downstream interface of a multicast group is suppressed from forwarding Join/Prune messages with information about multicast group joining. If Join/Prune messages carry information about multicast group prune, the downstream interface of the multicast group is restored.

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 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 public network instance, set the time during which the downstream interface of a router keeps the Join or Prune state to 280 seconds.

```
<Huawei> system-view
[Huawei] multicast routing-enable
[Huawei] pim
[Huawei-pim] holdtime join-prune 280
```

Related Topics

10.3.57 pim holdtime join-prune

10.3.40 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.

Copyright © Huawei Technologies Co., Ltd.

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 single Join/Prune message carrying a lot of (S, G) entries, the maximum size of each Join/Prune message can be set to a small value to limit the number of (S, G) entries in each message, relieving the burden on the peer device.

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 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
```

 Copyright © Huawei Technologies Co., Ltd.

10.3.41 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, change the length of a queue for periodically sending messages to a small value 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 in the public network instance or VPN instance.

Precautions

This command is valid for PIM-SM and PIM-DM.

 Copyright © Huawei Technologies Co., Ltd.

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
```

10.3.42 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 to send a cacheage of PIM Join/Prune messages than to send a large number of individual PIM Join/Prune messages. A device sends PIM Join/Prune messages in cacheages. To disable the cacheage function, run the **join-prune triggered-message-cache disable** command.

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 PIM-SM and PIM-DM.

 Copyright © Huawei Technologies Co., Ltd.

Example

Disable the Join/Prune message cacheage function.

```
<Huawei> system-view
[Huawei] multicast routing-enable
[Huawei] pim
[Huawei-pim] join-prune triggered-message-cache disable
```

10.3.43 local-address (IPv4)

Function

The **local-address** command sets a local address for an Anycast RP.

The **undo local-address** command deletes the local address set for an Anycast RP.

By default, no local address is set for an Anycast RP.

Format

local-address *local-address*

undo local-address

Parameters

Parameter	Description	Value
local-address	Specifies the local address of Anycast RP.	The value is in dotted decimal notation. This address must be a valid unicast IP address and cannot be an address on the network segment 127.0.0.0/8.

Views

Anycast RP view of public network instance or Anycast RP view of VPN instance

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If PIM Anycast RP is configured, after an RP receives a Register message, it checks the source address of the Register message. If the Register message is sent by the source's DR, the RP forwards the Register message to Anycast RP peers. If the Register message is sent by an Anycast RP peer, it does not forward the Register message.

When forwarding a PIM Register message to other Anycast RP peers, the local RP needs to use its own IP address (called the local address) as the source address of the Register message and use the addresses of Anycast RP peers as the

 Copyright © Huawei Technologies Co., Ltd.

destination addresses of the Register message. In such a manner, Anycast RP peers can learn source/group information from each other. This command is used to set a local address for an Anycast RP.

Prerequisites

The local address specified for Anycast RP must be an existing interface IP address.

Precautions

The local address must be different from the Anycast RP address.

NOTE

Setting a Loopback interface address as the local address of the Anycast RP is recommended.

Example

In the public network instance, set the Anycast RP address to 10.10.10.10 and local address of Anycast RP to 10.1.1.1.

```
<Huawei> system-view
[Huawei] multicast routing-enable
[Huawei] pim
[Huawei-pim] anycast-rp 10.10.10.10
[Huawei-pim-anycast-rp-10.10.10.10] local-address 10.1.1.1
```

Related Topics

10.3.1 anycast-rp (IPv4)

10.3.45 peer (IPv4)

10.3.44 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.	-

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
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 neighbor 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 in the public network instance or VPN instance.

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 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
```

10.3.45 peer (IPv4)

Function

The **peer** command configures Anycast RP peers.

The **undo peer** command removes the configurations of Anycast RPs.

By default, no Anycast RP peer is configured.

Copyright © Huawei Technologies Co., Ltd.

Format

peer *peer-address* [**fwd-msdp-sa** [*acl-number* | **acl-name** *acl-name*]]

undo peer *peer-address*

Parameters

Parameter	Description	Value
peer-address	Specifies the address of an Anycast RP peer.	The value is in dotted decimal notation.
fwd-msdp-sa	Enables a local RP to extract source/group information from the received MSDP SA message, encapsulates the information into a Register message, and sends the Register message to Anycast RP peers.	-
acl-number	Specifies the range of multicast groups to which an MSDP SA message can be forwarded. *acl-number* specifies an ACL number.	The value is an integer ranging from 2000 to 3999.
acl-name *acl-name*	Specifies the range of multicast groups to which an MSDP SA message can be forwarded. *acl-name* specifies an ACL name. **NOTE** **acl-name** *acl-name* can only be the name of a named advanced ACL.	The value is a string of 1 to 32 case-sensitive characters without spaces. The value must start with a letter (case sensitive).

Views

Anycast RP view of public network instance or Anycast RP view of VPN instance

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If PIM Anycast RP is configured, after an RP receives a Register message, it checks the source address of the Register message. If the Register message is sent by the source's DR, the RP forwards the Register message to Anycast RP peers. If the Register message is sent by an Anycast RP peer, it does not forward the Register message.

When forwarding a PIM Register message to other Anycast RP peers, the local RP needs to use its own IP address (called the local address) as the source address of the Register message and use the addresses of Anycast RP peers as the destination addresses of the Register message. In such a manner, Anycast RP peers

 Copyright © Huawei Technologies Co., Ltd.

can learn source/group information from each other. This command is used to configure an address for an Anycast RP peer. This address is used as the destination address of the Register message to be sent by the local RP.

To enable an RP to obtain information about the multicast source in another PIM-SM domain, you can adopt either of the following schemes:

- Set up MSDP peer relationships between every Anycast RP member in a PIM-SM domain and the RP in another PIM-SM domain.
- Set up MSDP peer relationships between some Anycast RP members with the RP in another PIM-SM domain. After the members who have set up MSDP peer relationships receive SA messages, they extract source/group information from SA messages, encapsulate the information into Register messages, and forward the Register messages to the members who do not set up MSDP peer relationships with the RP.

Precautions

You can specify a maximum of 16 Anycast RP peers for each Anycast RP.

In a PIM-SM domain, all the devices deployed with Anycast RP must be fully connected logically. Anycast RP peer relationships need to be configured between every two devices deployed with the Anycast RP.

Example

In the public network instance, set the Anycast RP address to 10.3.3.3 and the peer address to 10.2.2.2, and enable the local RP to forward MSDP SA messages to its peers.

```
<Huawei> system-view
[Huawei] multicast routing-enable
[Huawei] pim
[Huawei-pim] anycast-rp 10.3.3.3
[Huawei-pim-anycast-rp-10.3.3.3] peer 10.2.2.2 fwd-msdp-sa
```

Related Topics

10.3.43 local-address (IPv4)

10.3.1 anycast-rp (IPv4)

10.3.46 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*]

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Specifies the name of a VPN instance.	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

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 in the public network instance or VPN instance.

Precautions

NOTICE

In using the **undo pim** command, enter Y or N to confirm the action. This command clears global IPv4 PIM configurations in the current instance. Use this command with caution.

Example

Enter the PIM view of the public network instance.

```
<Huawei> system-view
[Huawei] multicast routing-enable
[Huawei] pim
[Huawei-pim]
```

Enter the PIM view of VPN instance **mytest**.

```
<Huawei> system-view
[Huawei] ip vpn-instance mytest
[Huawei-vpn-instance-mytest] ipv4-family
[Huawei-vpn-instance-mytest-af-ipv4] route-distinguisher 100:1
[Huawei-vpn-instance-mytest-af-ipv4] multicast routing-enable
[Huawei-vpn-instance-mytest-af-ipv4] quit
[Huawei-vpn-instance-mytest] quit
```

 Copyright © Huawei Technologies Co., Ltd.

```
[Huawei] pim vpn-instance mytest
[Huawei-pim-mytest]
```

Related Topics

10.3.50 pim dm

10.3.62 pim sm

10.3.47 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.

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 10 to 2000, in milliseconds. The default value is 1000 milliseconds.
min-rx-interval *rx-value*	Specifies the minimum interval for receiving BFD packets.	The value is an integer that ranges from 10 to 2000, in milliseconds. The default value is 1000 milliseconds.
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

Interface view

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

Usage Scenario

After PIM BFD is enabled, sometimes you need to run the **pim bfd** command to adjust PIM BFD parameters to adapt to the link. You can use this command to set the minimum interval for sending BFD packets, minimum interval for receiving PIM BFD packets, and local detection multiplier.

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 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. You are recommended to set the two values to be equal to or greater than 100. Otherwise, the BFD session flapping may occur.

Example

Adjust the minimum interval for transmitting BFD packets on GE 0/0/1.

```
<Huawei> system-view
[Huawei] bfd
[Huawei-bfd] quit
[Huawei] multicast routing-enable
[Huawei] interface gigabitethernet 0/0/1
[Huawei-GigabitEthernet0/0/1] pim sm
[Huawei-GigabitEthernet0/0/1] pim bfd enable
[Huawei-GigabitEthernet0/0/1] pim bfd min-tx-interval 100
```

Related Topics

10.3.26 display pim interface

10.3.21 display pim bfd session

10.3.48 pim bfd enable

10.3.48 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.

Format

pim bfd enable

undo pim bfd enable

Copyright © Huawei Technologies Co., Ltd.

Parameters

None

Views

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 in the public network instance or VPN instance.

Precautions

This command is valid for only PIM-SM.

PIM BFD depends on the BFD protocol. If the **bfd** command is not run to enable global BFD, the session status is **BFD global disable** though PIM BFD sessions can be set up.

This command is applicable to NBMA interfaces and broadcast interfaces rather than P2P interfaces.

Example

Enable PIM BFD on GE1/0/0.

```
<Huawei> system-view
[Huawei] bfd
[Huawei-bfd] quit
[Huawei] multicast routing-enable
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] pim sm
[Huawei-GigabitEthernet1/0/0] pim bfd enable
```

Related Topics

10.3.21 display pim bfd session

10.3.49 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.

 Copyright © Huawei Technologies Co., Ltd.

By default, the BSR boundary of a PIM-SM domain is not set.

Format

pim bsr-boundary

undo pim bsr-boundary

Parameters

None

Views

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 in the public network instance or VPN instance.

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 GE1/0/0.

```
<Huawei> system-view
[Huawei] multicast routing-enable
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] pim bsr-boundary
```

Related Topics

10.3.5 c-bsr (IPv4)

10.7.17 multicast boundary

 Copyright © Huawei Technologies Co., Ltd.

10.3.50 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

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 router can set up the PIM neighbor relationship with the neighboring device. The router then can process protocol packets received from PIM neighbors.

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.

Example

Enable PIM-DM on GE1/0/0.

```
<Huawei> system-view
[Huawei] multicast routing-enable
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] pim dm
```

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

10.3.62 pim sm

10.3.51 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

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In PIM, routers on the shared network segment candidates for the DR. The DR is responsible for the registering of the local multicast source and the joining of the receivers.

The DR election is based on the priority and the IP address. To elect the DR, the routers send the Hello message that contains the priority to each other. The router with the highest priority functions as the DR. If the routers have the same priority, the router with the largest IP address functions as the DR.

If there is at least one router that does not support Hello packets that contain the priority in the network, the DR election is based on the IP address of each router. The router with the largest IP address functions as the DR.

 Copyright © Huawei Technologies Co., Ltd.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command in the public network instance or VPN instance.

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 GE1/0/0 that is elected as DR to 3.

```
<Huawei> system-view
[Huawei] multicast routing-enable
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] pim hello-option dr-priority 3
```

Related Topics

10.3.33 hello-option dr-priority (IPv4)

10.3.52 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

Interface view

Copyright © Huawei Technologies Co., Ltd.

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On the PIM network, after the device receives a Hello message from its PIM neighbor, the device starts the timer. The timer value is the value of Holdtime in the Hello message. If the device does not receive any Hello message from its PIM neighbor after the timeout, the device 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 in the public network instance or VPN instance.

Precautions

The timeout period must be greater than the interval for sending Hello messages. You can run the **pim timer hello** command to set the interval for sending Hello messages.

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 GE1/0/0 waits to receive Hello messages from its neighbor to 120 seconds.

```
<Huawei> system-view
[Huawei] multicast routing-enable
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] pim hello-option holdtime 120
```

Related Topics

10.3.66 pim timer hello

10.3.34 hello-option holdtime (IPv4)

10.3.53 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.

Copyright © Huawei Technologies Co., Ltd.

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

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Hello messages sent by routers carry **lan-delay** and **override-interval**. The **lan-delay** parameter indicates the delay in transmitting messages in the LAN. When the values of **lan-delay** on all routers on the same link are different, the maximum value of these values is used.

When a router sends a Prune message to the upstream router in the same network segment, if other router still requests the multicast data, it needs to send a Join message to the upstream router in the override-interval period.

The value of the Prune-Pending Timer (PPT) is obtained by the value of **lan-delay** plus the value of **override-interval**. PPT refers to the delay during which the current router receives a Prune message from the downstream interface and performs the prune action. If the router receives a Join message from the downstream interface in PPT, the router cancels the prune action.

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 PIM-SM and PIM-DM.

If the prune delay is set too short, the upstream router stops forwarding multicast packets before the downstream router overrides Prune messages of neighbors. Exercise caution when you run this command.

 Copyright © Huawei Technologies Co., Ltd.

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, except for the 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 GE1/0/0.

```
<Huawei> system-view
[Huawei] multicast routing-enable
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] pim hello-option lan-delay 200
```

Related Topics

10.3.51 pim hello-option dr-priority
10.3.37 hello-option override-interval (IPv4)
10.3.35 hello-option lan-delay (IPv4)

10.3.54 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

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When sending a Hello message, the device generates a Generation ID and encapsulates it into the message. The Generation ID changes only when the device

 Copyright © Huawei Technologies Co., Ltd.

status changes. After receiving the Hello message, the neighboring device detects Generation ID change and immediately sends a Join message to the device to update the neighbor relationship. If multiple devices on the shared network segment 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. The upstream neighbor cannot update neighbor relationships with downstream devices because of 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 in the public network instance or VPN instance.

Precautions

This command is valid for only PIM-SM.

Neighbor tracking can be implemented only when on 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 in GE1/0/0.

```
<Huawei> system-view
[Huawei] multicast routing-enable
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] pim hello-option neighbor-tracking
```

Related Topics

10.3.36 hello-option neighbor-tracking (IPv4)

10.3.55 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.

Copyright © Huawei Technologies Co., Ltd.

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

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Hello messages sent by routers carry **lan-delay** and **override-interval**. The **override-interval** parameter refers to the period during which a downstream router overrides the prune action.

When a router sends a Prune message to the upstream router in the same network segment, if other router still requests the multicast data, it needs to send a Join message to the upstream router in the override-interval period.

When the values of **override-interval** on all routers on the same link are different, the maximum value of these values is used.

The value of PPT is obtained by the value of **lan-delay** plus the value of **override-interval**. When receiving a Prune message from a downstream interface, the router does not perform the prune action until the PPT times out. If the router 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 in the public network instance or VPN instance.

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

 Copyright © Huawei Technologies Co., Ltd.

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 GE1/0/0.

```
<Huawei> system-view
[Huawei] multicast routing-enable
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] pim hello-option override-interval 2000
```

Related Topics

10.3.53 pim hello-option lan-delay

10.3.35 hello-option lan-delay (IPv4)

10.3.37 hello-option override-interval (IPv4)

10.3.56 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

Interface view

Default Level

2: Configuration level

Copyright © Huawei Technologies Co., Ltd.

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 retains 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 in the public network instance or VPN instance.

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 GE1/0/0 to keep the Assert state to 100s.

```
<Huawei> system-view
[Huawei] multicast routing-enable
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] pim holdtime assert 100
```

Related Topics

10.3.39 holdtime join-prune (IPv4)

10.3.57 pim holdtime join-prune

10.3.38 holdtime assert (IPv4)

10.3.57 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*

Copyright © Huawei Technologies Co., Ltd.

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

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After receiving a Join/Prune message from the downstream device, the router starts the holdtime timer. If the router does not receive subsequent Join/Prune messages from the downstream device within the holdtime interval, the router 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 in the public network instance or VPN instance.

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 GE1/0/0 to 280 seconds.

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

 Copyright © Huawei Technologies Co., Ltd.

```
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] pim holdtime join-prune 280
```

Related Topics

10.3.38 holdtime assert (IPv4)

10.3.56 pim holdtime assert

10.3.39 holdtime join-prune (IPv4)

10.3.58 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* | **acl-name** *acl-name* } | **ssm** { *advanced-acl-number* | **acl-name** *acl-name* } | *advanced-acl-number* | **acl-name** *acl-name* }

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.
acl-name *acl-name*	Specifies the name of a named ACL. **NOTE** **acl-name** *acl-name* can only be the name of a named advanced ACL.	The value is a string of 1 to 32 case-sensitive characters without spaces. The value must start with a letter (case sensitive).
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.

Copyright © Huawei Technologies Co., Ltd.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To prevent unauthorized users from joining multicast groups on the PIM-SM network, run the **pim join-policy** command to enable the system to filter join information in Join/Prune messages.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command in the public network instance or VPN instance.

Configuration Impact

The **pim join-policy** command and the **acl** command are used together.

- If **asm** is specified, in the basic ACL view, you can set the multicast group address range of join information by specifying the **source** parameter in the **rule** command.
- If **ssm** is specified, in the advanced ACL view, you can set the source address range and multicast group address range of join information by respectively specifying the **source** parameter and **destination** parameter in the **rule** command.

The rule configurations for a named ACL and an advanced ACL are the same. The **time-range** parameter takes effect in the **rule** command only for the named ACL.

Example

Configure GE1/0/0 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 1/0/0
[Huawei-GigabitEthernet1/0/0] pim join-policy asm 2001
```

10.3.59 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.

 Copyright © Huawei Technologies Co., Ltd.

Format

pim neighbor-policy { *basic-acl-number* | **acl-name** *acl-name* }

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.
acl-name *acl-name*	Specifies the ACL name. **NOTE** **acl-name** *acl-name* can only be the name of a named advanced ACL.	The value is a string of 1 to 32 case-sensitive characters without spaces. The value must start with a letter (case sensitive).

Views

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 router 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 in the public network instance or VPN instance.

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.

For the named ACL, in the ACL view, when the **rule** command is used to configure a filtering rule, the filtering rule takes effect for only the multicast group address range specified by **source** and the time range specified by **time-range**.

Precautions

This command is valid for both PIM-DM and PIM-SM.

If a PIM device has established a neighbor relationship with the router but its IP address is not in the configured range of valid neighbor addresses, the router will

 Copyright © Huawei Technologies Co., Ltd.

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 router is terminated.

Example

Allow GE1/0/0 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 1/0/0
[Huawei-GigabitEthernet1/0/0] pim neighbor-policy 2001
```

10.3.60 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

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After an interface on the device is enabled with PIM, the device generates a random number as the generation ID of the Hello message. If the status of the device is updated, the device generates a new Generation ID. When the device finds that the Hello message received from a PIM neighbor contains a different Generation ID, the device considers that the status of the PIM neighbor changes.

 Copyright © Huawei Technologies Co., Ltd.

To ensure that connected 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 in the public network instance or VPN instance.

Precautions

This command is valid for both PIM-DM and PIM-SM.

Example

Configure GE1/0/0 to reject the Hello messages without the generation ID.

```
<Huawei> system-view
[Huawei] multicast routing-enable
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] pim require-genid
```

10.3.61 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

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To protect the router 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

 Copyright © Huawei Technologies Co., Ltd.

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 router can be connected to this network segment.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command in the public network instance or VPN instance.

Precautions

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 routers 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 GE1/0/0.

```
<Huawei> system-view
[Huawei] multicast routing-enable
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] pim silent
```

10.3.62 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

Interface view

Copyright © Huawei Technologies Co., Ltd.

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After PIM-SM is enabled on interfaces, routers can set up PIM neighbor relationships with each other and process protocol packets received from PIM neighbors.

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-SM and IGMP need to be enabled on the same interface, enable PIM-SM, and then enable IGMP.

Example

Enable PIM-SM on GE1/0/0.

```
<Huawei> system-view
[Huawei] multicast routing-enable
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] pim sm
```

Related Topics

10.3.50 pim dm

10.3.63 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

Copyright © Huawei Technologies Co., Ltd.

Views

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 router in the pruned state resets the prune-status timer. As a result, the downstream interface cannot forward packets before the prune-status timer times out.

After PIM-DM state refresh is disabled, the interface starts to forward multicast data when the prune timer times out. The downstream routers that do not want to receive the data can send Prune messages. The process is performed periodically, which wastes a lot of network resources. Enabling PIM-DM state refresh can optimize the network traffic.

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 GE1/0/0.

```
<Huawei> system-view
[Huawei] multicast routing-enable
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] undo pim state-refresh-capable
```

Related Topics

10.3.80 state-refresh-interval (IPv4)

10.3.81 state-refresh-rate-limit (IPv4)

10.3.82 state-refresh-ttl (IPv4)

10.3.64 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.

Copyright © Huawei Technologies Co., Ltd.

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

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

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-SM.

Example

Enable PIM DR switching delay on GE1/0/0 and set the delay to 20 seconds.

```
<Huawei> system-view
[Huawei] multicast routing-enable
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] pim timer dr-switch-delay 20
```

10.3.65 pim timer graft-retry

Function

The **pim timer graft-retry** command sets the interval for retransmitting Graft messages on an interface.

Copyright © Huawei Technologies Co., Ltd.

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

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In PIM-DM mode, when a member joins a pruned group, the router sends a Graft message and waits to receive an ACK message from the upstream router. If the downstream router does not receive the ACK message in the period configured through the command, the router resends the Graft message until the router receives the ACK message from the upstream router.

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 GE1/0/0.

```
<Huawei> system-view
[Huawei] multicast routing-enable
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] pim timer graft-retry 80
```

 Copyright © Huawei Technologies Co., Ltd.

10.3.66 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

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 in the public network instance or VPN instance.

Precautions

The interval for sending Hello messages must be shorter than the timeout period of PIM neighbors. You can run the **hello-option holdtime (IPv4)** command to set the timeout period of PIM neighbors.

The configuration is the same as the **timer hello (IPv4)** command in the PIM view, except for the 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.

Copyright © Huawei Technologies Co., Ltd.

Example

Set the interval for sending Hello messages to 40 seconds on GE1/0/0.

```
<Huawei> system-view
[Huawei] multicast routing-enable
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] pim timer hello 40
```

Related Topics

10.3.84 timer hello (IPv4)

10.3.67 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

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

 Copyright © Huawei Technologies Co., Ltd.

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 in the public network instance or VPN instance.

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 GE1/0/0.

```
<Huawei> system-view
[Huawei] multicast routing-enable
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] pim timer join-prune 80
```

Related Topics

10.3.85 timer join-prune (IPv4)

10.3.68 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.

Copyright © Huawei Technologies Co., Ltd.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

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

IP multicast routing has been enabled using the **multicast routing-enable** command in the public network instance or VPN instance.

Example

Set the maximum delay for triggering the Hello message to 3 seconds on GE1/0/0.

```
<Huawei> system-view
[Huawei] multicast routing-enable
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] pim triggered-hello-delay 3
```

10.3.69 probe-interval (IPv4)

Function

The **probe-interval** command sets the interval for a router 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 router 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.

Copyright © Huawei Technologies Co., Ltd.

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 in the public network instance or VPN instance.

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 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
```

Related Topics

10.3.73 register-suppression-timeout (IPv4)

10.3.70 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.

Copyright © Huawei Technologies Co., Ltd.

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 checksum calculation and improves encapsulation of multicast data in Register messages.

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-SM.

Example

Calculate the checksum based only on the header of a Register message in the public network instance.

```
<Huawei> system-view
[Huawei] multicast routing-enable
[Huawei] pim
[Huawei-pim] register-header-checksum
```

Related Topics

10.3.71 register-policy (IPv4)

10.3.73 register-suppression-timeout (IPv4)

Copyright © Huawei Technologies Co., Ltd.

10.3.71 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* | **acl-name** *acl-name* }

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.
acl-name *acl-name*	Specifies the name of a Named ACL. **NOTE** **acl-name** *acl-name* can only be the name of a named advanced ACL.	The value is a string of 1 to 32 case-sensitive characters without spaces. The value must start with a letter (case sensitive).

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.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command in the public network instance or VPN instance.

Precautions

Copyright © Huawei Technologies Co., Ltd.

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
```

Configure a Named ACL: the RP receives 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 name myacl
[Huawei-acl-adv-myacl] rule permit ip source 10.10.0.0 0.0.255.255 destination 225.1.0.0 0.0.255.255
[Huawei-acl-adv-myacl] quit
[Huawei] multicast routing-enable
[Huawei] pim
[Huawei-pim] register-policy acl-name myacl
```

Related Topics

10.3.73 register-suppression-timeout (IPv4)

10.3.72 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

Copyright © Huawei Technologies Co., Ltd.

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 in the public network instance or VPN instance.

Precautions

The command is effective only when the specified interface is in Up state.

Example

In the 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
```

10.3.73 register-suppression-timeout (IPv4)

Function

The **register-suppression-timeout** command sets the timeout period during which a router keeps the register suppression state.

The **undo register-suppression-timeout** command restores the default timeout period.

By default, a router keeps the register suppression state for 60 seconds.

Copyright © Huawei Technologies Co., Ltd.

Format

register-suppression-timeout *interval*

undo register-suppression-timeout

Parameters

Parameter	Description	Value
interval	Specifies the timeout period during which the router 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 router immediately stops sending Register messages and enters the register suppression state.

The **register-suppression-timeout** command determines how long the router keeps the register suppression state. When the timeout period expires, the router (source DR) starts to send Register messages to the RP.

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 timeout period is too short, the RP receives burst multicast data more frequently. If the timeout period is too long, the delay for a new receiver to join a group is long when an (S, G) entry on the RP times out.

You can use the **probe-interval (IPv4)** command to configure the router 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.

 Copyright © Huawei Technologies Co., Ltd.

Example

In the public network instance, set the timeout period during which the router keeps the register suppression state to 70 seconds.

```
<Huawei> system-view
[Huawei] multicast routing-enable
[Huawei] pim
[Huawei-pim] register-suppression-timeout 70
```

Related Topics

10.3.69 probe-interval (IPv4)

10.3.71 register-policy (IPv4)

10.3.74 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 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-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

Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

Usage Scenario

If a PIM-enabled interface on the device has been forwarding multicast packets in a long period of time, the device stores statistics on a large number of Cotrol 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 the GE1/0/0 in the public network instance.

```
<Huawei> reset pim control-message counters interface gigabitethernet 1/0/0
```

Related Topics

10.3.24 display pim control-message counters

10.3.75 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 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 *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.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
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 GE1/0/0 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 gigabitethernet 1/0/0
```

 Copyright © Huawei Technologies Co., Ltd.

10.3.76 source-lifetime (IPv4)

Function

The **source-lifetime** command specifies the timeout period of an (S, G) or (*, G) entry on the router.

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*

undo source-lifetime

Parameters

Parameter	Description	Value
interval	Specifies the timeout period of an (S, G) or (*, G) entry on the router.	The value is an integer that ranges from 60 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 router 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.

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 both PIM-DM and PIM-SM.

Copyright © Huawei Technologies Co., Ltd.

Example

In the public network instance, set the timeout period of an (S, G) or (*, G) entry of the router to 200 seconds.

```
<Huawei> system-view
[Huawei] multicast routing-enable
[Huawei] pim
[Huawei-pim] source-lifetime 200
```

10.3.77 source-policy (IPv4)

Function

The **source-policy** command configures the router 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 router does not filter received multicast data packets based on source addresses or source/group addresses.

Format

source-policy { *acl-number* | **acl-name** *acl-name* }

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.
acl-name *acl-name*	Specifies the name of a named ACL. **NOTE** **acl-name** *acl-name* can only be the name of a named advanced ACL.	The value is a string of 1 to 32 case-sensitive characters without spaces. The value must start with a letter (case sensitive).

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 router to filter received multicast data packets based on source addresses or source/group addresses.

 Copyright © Huawei Technologies Co., Ltd.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command in the public network instance or VPN instance.

Configuration Impact

If **source-policy** and the basic ACL are applied, all multicast data packets received should match the source address. Packets that do not pass the filtering are discarded.

If **source-policy** and the advanced ACL are used, the source addresses and group addresses of all received multicast data packets should be matched. Packets that do not pass the filtering are discarded.

The configurations of the Named ACL and 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.

Precautions

This command is valid for both PIM-DM and PIM-SM.

Example

In the public network instance, configure the router 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
```

In the public network instance, configure a Named ACL where multicast data packets with the source address of 10.10.1.2 are received, and those with the source address of 10.10.1.1 are dropped.

```
<Huawei> system-view
[Huawei] acl name myacl
[Huawei-acl-adv-myacl] rule permit ip source 10.10.1.2 0
[Huawei-acl-adv-myacl] rule deny ip source 10.10.1.1 0
[Huawei-acl-adv-myacl] quit
[Huawei] multicast routing-enable
[Huawei] pim
[Huawei-pim] source-policy acl-name myacl
```

10.3.78 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.

 Copyright © Huawei Technologies Co., Ltd.

Format

spt-switch-threshold { *traffic-rate* | **infinity** } [**group-policy** { *basic-acl-number* | **acl-name** *acl-name* } [**order** *order-value*]]

undo spt-switch-threshold [*traffic-rate* | **infinity**] [**group-policy** { *basic-acl-number* | **acl-name** *acl-name* }]

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.
acl-name *acl-name*	Specifies the name of a Named ACL. **NOTE** **acl-name** *acl-name* can only be the name of a named advanced ACL.	The value is a string of 1 to 32 case-sensitive characters without spaces. The value must start with a letter (case sensitive).
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.

 Copyright © Huawei Technologies Co., Ltd.

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 a 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 in the public network instance or VPN instance.

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 command that is first matched according to the order takes effect.

Example

In the 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 router 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
```

 Copyright © Huawei Technologies Co., Ltd.

In the public network instance, create a group-policy that uses ACL 2010, set the traffic rate threshold to 100 kbit/s, and order 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 100 group-policy 2010 order 1
```

In the public network instance, create a group-policy that uses ACL **myacl**, set the traffic rate threshold to 100 kbit/s, and order ACL **myacl** in the group-policy to 1.

```
<Huawei> system-view
[Huawei] acl name myacl
[Huawei-acl-adv-myacl] rule permit ip destination 225.1.0.0 0.0.255.255
[Huawei-acl-adv-myacl] quit
[Huawei] multicast routing-enable
[Huawei] pim
[Huawei-pim] spt-switch-threshold 100 group-policy acl-name myacl order 1
```

10.3.79 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* | **acl-name** *acl-name* }

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.
acl-name *acl-name*	Specifies the name of a Named ACL. **NOTE** **acl-name** *acl-name* can only be the name of a named advanced ACL.	The value is a string of 1 to 32 case-sensitive characters without spaces. The value must start with a letter (case sensitive).

Views

PIM view of public network instance or PIM view of VPN instance

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

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 beyond 232.0.0.0/8.

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-SM.

Example

In the 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
```

In the public network instance, configure a Named ACL: the PIM SSM multicast address range is 232.1.0.0/16.

```
<Huawei> system-view
[Huawei] acl name myacl
[Huawei-acl-adv-myacl] rule permit ip destination 232.1.0.0 0.0.255.255
[Huawei-acl-adv-myacl] quit
[Huawei] multicast routing-enable
[Huawei] pim
[Huawei-pim] ssm-policy acl-name myacl
```

Related Topics

10.1.50 ssm-mapping (IGMP)

10.3.80 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*

Copyright © Huawei Technologies Co., Ltd.

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 routers directly connected to a source.

Example

Set the interval for sending PIM State-Refresh messages to 70s in the public network instance.

```
<Huawei> system-view
[Huawei] multicast routing-enable
[Huawei] pim
[Huawei-pim] state-refresh-interval 70
```

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

10.3.39 holdtime join-prune (IPv4)

10.3.81 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 router 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 router discards the received duplicate State-Refresh messages.
- After the State-Refresh timer times out, the router can receive the next State-Refresh message.

Prerequisites

 Copyright © Huawei Technologies Co., Ltd.

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 public network instance.

```
<Huawei> system-view
[Huawei] multicast routing-enable
[Huawei] pim
[Huawei-pim] state-refresh-rate-limit 45
```

10.3.82 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, the router decreases the value of the TTL in the message by 1, and then sends the message to the downstream router until

Copyright © Huawei Technologies Co., Ltd.

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

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 routers directly connected to a source.

Example

Set the TTL value for sending PIM State-Refresh messages to 45 in the public network instance.

```
<Huawei> system-view
[Huawei] multicast routing-enable
[Huawei] pim
[Huawei-pim] state-refresh-ttl 45
```

10.3.83 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* | **acl-name** *acl-name*] [**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.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
acl-name *acl-name*	Specifies the name of a named ACL. **NOTE** **acl-name** *acl-name* can only be the name of a named advanced ACL.	The value is a string of 1 to 32 case-sensitive characters without spaces. The value must start with a letter (case sensitive).
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 to exchange information between the C-RPs and the 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 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.

The **static-rp** and **acl** commands are used together.

- For the numbered ACL, in the ACL view, 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.

 Copyright © Huawei Technologies Co., Ltd.

- 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 time period specified by the **time-range** parameter.
- For the numbered ACL, 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.
- For the Named ACL, 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 **destination** parameter in the **rule** command. The filtering rule is effective only with the **destination** parameter and the time period specified by the **time-range** parameter.

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.

This command is valid only for PIM-SM.

Example

In the public network instance, configure the router 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
```

In the public network instance, configure the router with address 10.110.0.6 as a static RP serving the groups permitted by ACL **myacl**, and configure the static RP to be preferred.

```
<Huawei> system-view
[Huawei] acl name myacl
[Huawei-acl-adv-myacl] rule permit ip destination 225.1.0.0 0.0.255.255
[Huawei-acl-adv-myacl] quit
[Huawei] multicast routing-enable
[Huawei] pim
[Huawei-pim] static-rp 10.110.0.6 acl-name myacl preferred
```

Related Topics

10.3.30 display pim rp-info

10.3.84 timer hello (IPv4)

Function

The **timer hello** command sets the interval at which the PIM router sends Hello messages.

The **undo timer hello** command restores the default interval.

By default, the interval at which the PIM router 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 in the public network instance or VPN instance.

Configuration Impact

This command is valid for both PIM-DM and PIM-SM.

The interval at which the PIM router 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

 Copyright © Huawei Technologies Co., Ltd.

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 public network instance.

```
<Huawei> system-view
[Huawei] multicast routing-enable
[Huawei] pim
[Huawei-pim] timer hello 40
```

Related Topics

10.3.66 pim timer hello

10.3.34 hello-option holdtime (IPv4)

10.3.85 timer join-prune (IPv4)

Function

The **timer join-prune** command configures the interval at which Join/Prune messages are sent to an upstream router.

The **undo timer join-prune** command restores the default interval.

By default, the interval at which Join/Prune messages are sent to an upstream router 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

 Copyright © Huawei Technologies Co., Ltd.

The router sends join information to the upstream device, requesting the upstream device to forward multicast data. The router 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 in the public network instance or VPN instance.

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 public network instance.

```
<Huawei> system-view
[Huawei] multicast routing-enable
[Huawei] pim
[Huawei-pim] timer join-prune 80
```

Related Topics

10.3.67 pim timer join-prune

10.3.86 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

Copyright © Huawei Technologies Co., Ltd.

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 in the public network instance or VPN instance.

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 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
```

Related Topics

10.3.78 spt-switch-threshold (IPv4)

Copyright © Huawei Technologies Co., Ltd.

10.4 PIM (IPv6) Configuration Commands

NOTE

AR120 series do not support this function.

10.4.1 anycast-rp (IPv6)

Function

The **anycast-rp** command configures an Anycast RP and displays the Anycast-RP view or directly displays the existing Anycast-RP view.

The **undo anycast-rp** command deletes the configurations of an Anycast RP.

By default, no Anycast RP is configured.

Format

anycast-rp *rp-address*

undo anycast-rp *rp-address*

Parameters

Parameter	Description	Value
rp-address	Indicates the Anycast RP address.	The value must be a legal IPv6 global unicast IP address in hexadecimal notation.

Views

PIM-IPv6 view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In a traditional PIM-SM (IPv6) domain, all multicast groups map to one RP. When the network is overloaded or traffic concentrates on an RP, the RP may be overburdened. If the RP fails, routes are converged slowly or multicast packets are forwarded over non-optimal paths.

Configuring the Anycast RP in the PIM-SM (IPv6) domain can address this problem. IPv6 routing will automatically select the topologically closest RP for each source and receiver. This releases burdens on RPs, implements RP backup, and optimizes the forwarding paths.

 Copyright © Huawei Technologies Co., Ltd.

Prerequisites

IPv6 multicast routing has been enabled using the **multicast ipv6 routing-enable** command in the system view.

Configuration Impact

If PIM (IPv6) Anycast RP is configured, after an RP receives a Register message, it checks the source address of the Register message. If the Register message is sent by the source's DR, the RP forwards the Register message to Anycast RP peers. If the Register message is sent by an Anycast RP peer, it does not forward the Register message. In such a manner, Anycast RP peers can learn source/group information from each other.

Precautions

- The Anycast RP address must be the same as that of the elected RP on the current network.
- Either static or dynamic RPs can be used on the network. Configuring RPs on loopback interfaces is recommended. You need to configure the same RP address on the devices to be deployed with the Anycast RP. If the dynamic RP is used on the network, before configuring an Anycast RP address, run the **display pim ipv6 rp-info** command to check the address of the RP on the current network.

Example

Set the Anycast RP address to FC00:0:0:2001::1 in the PIM-IPv6 view and enter the Anycast-RP view.

```
<Huawei> system-view
[Huawei] multicast ipv6 routing-enable
[Huawei] pim-ipv6
[Huawei-pim6] anycast-rp fc00:0:0:2001::1
[Huawei-pim6-anycast-rp-fc00:0:0:2001::1]
```

Related Topics

10.4.42 local-address (IPv6)
10.4.44 peer (IPv6)
10.4.28 display pim ipv6 rp-info

10.4.2 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

 Copyright © Huawei Technologies Co., Ltd.

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 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 it can solve the problem faced by IP fragmentation that all fragments become unavailable due to loss of fragment information.

Precautions

 Copyright © Huawei Technologies Co., Ltd.

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 PIM-IPv6 view.

```
<Huawei> system-view
[Huawei] multicast ipv6 routing-enable
[Huawei] pim-ipv6
[Huawei-pim6] bsm semantic fragmentation
```

Related Topics

10.4.4 c-bsr (IPv6)

10.4.3 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* | **acl6-name** *acl6-name* }

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.
acl6-name *acl6-name*	Specifies the name of a named ACL6. **NOTE** **acl6-name** *acl6-name* can only be the name of a named advanced ACL.	The value is a string of 1 to 32 case-sensitive characters without spaces. The value must start with a letter (case sensitive).

Views

PIM-IPv6 view

Copyright © Huawei Technologies Co., Ltd.

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On a PIM-SM network that applies the BSR mechanism, you can configure any router as a C-BSR to elect the BSR. Once being elected as the BSR, the router is responsible for advertising RP information in the network. To prevent the valid BSR from being maliciously replaced, use the following measures:

- Certain hosts try changing the RP mapping to spoof the router by forging BSR packets.

  Solution: The attack often occurs on edge routers because the BSR packet is a multicast packet and the TTL value of the BSR packet is 1. The BSR is inside the network, and hosts are outside the network. The routers can perform neighbor check and RPF check on the received BSR packets to prevent the attack.
- Certain attackers control the router on the network, or unauthorized users connect to the router. The attackers configure the router as a C-BSR, and help the router win the BSR election. The attackers obtain the right of advertising RP information in the network.

  Solution: After the router is configured as a C-BSR, the router spreads BSR packets in the network. The BSR packets are multicast packets. The TTL value of BSR packets is 1. The BSR packets are forwarded hop by hop. As long as the neighboring router cannot receive the packets, the packets are not spread in the entire network. The solution is to use the **bsr-policy** command on every router in the network to limit the valid BSR range. For example, only routers FC00:0:0:2001::1/62 and FC00:0:0:2001::2/64 are elected as BSRs; therefore, the routers do not receive or forward other BSR packets. This type of attack is prevented.

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 using the **multicast ipv6 routing-enable** command in the system view.

Configuration Impact

After the **bsr-policy** command is run, the router 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.

When you use the **rule (basic ACL6 view)** command to configure a filtering rule for the Named ACL, the rule is effective only within the source address range specified by the **source** parameter and within the time period specified by the **time-range** parameter.

 Copyright © Huawei Technologies Co., Ltd.

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
```

In the PIM-IPv6 view, use a Named ACL to configure address FC00:0:0:2001::/64 as the valid BSR address range.

```
<Huawei> system-view
[Huawei] acl ipv6 name myacl6
[Huawei-acl6-adv-myacl6] rule permit ipv6 source fc00:0:0:2001:: 64
[Huawei-acl6-adv-myacl6] quit
[Huawei] multicast ipv6 routing-enable
[Huawei] pim-ipv6
[Huawei-pim6] bsr-policy acl6-name myacl6
```

Related Topics

10.4.4 c-bsr (IPv6)

10.4.4 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.

Copyright © Huawei Technologies Co., Ltd.

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 C-BSRs. The BSR 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 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 better than the current BSR, the C-BSR replaces its BSR address with the address of the BSR 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.

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
```

Related Topics

10.4.59 pim ipv6 sm

Copyright © Huawei Technologies Co., Ltd.

10.4.12 c-rp (IPv6)

10.4.5 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 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 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 serves all multicast groups that do not belong to any BSR administrative domains. The global domain maintains a BSR that serves multicast groups that do not belong to any BSR administrative domains.

Prerequisites

IPv6 multicast routing has been enabled using the **multicast ipv6 routing-enable** command in the system view.

Precautions

 Copyright © Huawei Technologies Co., Ltd.

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
```

Related Topics

10.4.6 c-bsr global (IPv6)

10.4.11 c-bsr scope

10.4.6 c-bsr global (IPv6)

Function

The **c-bsr global** command configures the router 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

Copyright © Huawei Technologies Co., Ltd.

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 router as a C-BSR in the global domain. The BSR in the global domain is generated through election.

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. This means that the **c-bsr global** command can be used to enable a device in a 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 router 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
```

Related Topics

10.4.5 c-bsr admin-scope (IPv6)

10.4.11 c-bsr scope

10.4.7 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

Copyright © Huawei Technologies Co., Ltd.

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 router 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
```

Related Topics

10.4.4 c-bsr (IPv6)

Copyright © Huawei Technologies Co., Ltd.

10.4.8 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, the C-BSR periodically sends Bootstrap messages carrying the IPv6 address of the C-BSR 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 hold time.
- 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

 Copyright © Huawei Technologies Co., Ltd.

IPv6 multicast routing has been enabled using the **multicast ipv6 routing-enable** command in the system view.

Precautions

In actual application, all C-BSRs in the same PIM domain must use the same BS_interval and holdtime, and BS_interval must be smaller than holdtime. If C-BSRs use different BS_interval or holdtime values or if BS_interval must is larger than the holdtime, the BSR changes frequently, causing multicast forwarding errors.

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
```

Related Topics

10.4.4 c-bsr (IPv6)

10.4.9 c-bsr interval (IPv6)

10.4.9 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

Copyright © Huawei Technologies Co., Ltd.

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After a C-BSR is elected as the BSR, the C-BSR periodically sends Bootstrap messages carrying the IPv6 address of the C-BSR and the RP-set information to the network.

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 fail in the election triggers a new BSR election. 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, and BS_interval must be smaller than the holdtime. If C-BSRs use different BS_interval or holdtime values or BS_interval must is larger than the holdtime, the BSR changes frequently, causing multicast forwarding errors.

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
```

Related Topics

10.4.4 c-bsr (IPv6)

10.4.8 c-bsr holdtime (IPv6)

Copyright © Huawei Technologies Co., Ltd.

10.4.10 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 following situations occur:

- The router with the highest priority wins in the BSR election.
- In the case of the same priority, the router 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 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**

Copyright © Huawei Technologies Co., Ltd.

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
```

Related Topics

10.4.4 c-bsr (IPv6)

10.4.11 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

Copyright © Huawei Technologies Co., Ltd.

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.

Example

In the PIM-IPv6 view, configure the router 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
```

Related Topics

10.4.5 c-bsr admin-scope (IPv6)

10.4.6 c-bsr global (IPv6)

10.4.12 c-rp (IPv6)

Function

The **c-rp** command configures the router 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* | **acl6-name** *acl6-name* } | **scope** *scope-id*] | **holdtime** *hold-interval* | **priority** *priority*] *

undo c-rp *ipv6-address* [**scope** *scope-id*]

Copyright © Huawei Technologies Co., Ltd.

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.
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.
acl6-name *acl6-name*	Specifies the name of a named ACL6. **NOTE** **acl6-name** *acl6-name* can only be the name of a named advanced ACL.	The value is a string of 1 to 32 case-sensitive characters without spaces. The value must start with a letter (case sensitive).
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

 Copyright © Huawei Technologies Co., Ltd.

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:

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. In case of the same priority, hash functions are operated. The C-RP with the greatest calculated value wins.
4. If all the preceding factors are the same, the C-RP with the largest IPv6 address wins.

Prerequisites

IPv6 multicast routing has been enabled using the **multicast ipv6 routing-enable** command in the system view.

Configuration Impact

The **group-policy** { *basic-acl6-number* | **acl6-name** *acl6-name* }, **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* | **acl6-name** *acl6-name* } 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.

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
```

 Copyright © Huawei Technologies Co., Ltd.

In the PIM-IPv6 view, use a named ACL6 **myacl6** to configure an interface with the IPv6 address FC00:0:0:2001::1 as a C-RP of the PIM-SM (IPv6) multicast domain ff02:0:1391::/96. Set the priority to of the C-RP to 10.

```
<Huawei> system-view
[Huawei] acl ipv6 name myacl6
[Huawei-acl6-adv-myacl6] rule permit ipv6 destination ff02:0:1391:: 96
[Huawei-acl6-adv-myacl6] quit
[Huawei] multicast ipv6 routing-enable
[Huawei] pim-ipv6
[Huawei-pim6] c-rp fc00:0:0:2001::1 group-policy acl6-name myacl6 priority 10
```

Related Topics

10.4.59 pim ipv6 sm

10.4.4 c-bsr (IPv6)

10.4.13 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.

Copyright © Huawei Technologies Co., Ltd.

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
```

Related Topics

10.4.12 c-rp (IPv6)

10.4.14 c-rp holdtime (IPv6)

10.4.14 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.

Copyright © Huawei Technologies Co., Ltd.

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
```

Related Topics

10.4.12 c-rp (IPv6)

10.4.13 c-rp advertisement-interval (IPv6)

10.4.15 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.

Copyright © Huawei Technologies Co., Ltd.

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:

- The C-RP with the interface address that has the longest mask wins.
- The C-RP with highest priority wins.
- In case of the same priority, hash functions are operated. The C-RP with the greatest calculated value wins.
- If all the preceding factors are the same, 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 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.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> system-view
[Huawei] multicast ipv6 routing-enable
[Huawei] pim-ipv6
[Huawei-pim6] c-rp priority 5
```

Related Topics

10.4.12 c-rp (IPv6)

10.4.16 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* | **acl6-name** *acl6-name* }

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.
acl6-name *acl6-name*	Specifies the name of a named ACL. **NOTE** **acl6-name** *acl6-name* can only be the name of a named advanced ACL.	The value is a string of 1 to 32 case-sensitive characters without spaces. The value must start with a letter (case sensitive).

Views

PIM-IPv6 view

Default Level

2: Configuration level

Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

Usage Scenario

On a PIM SM network that uses the BSR mechanism, any router 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 as the RP-set, and floods it through BSR messages on the entire network. The local router then works out the RP serving a specific multicast group address range according to the RP-set.

To protect valid C-RP from being spoofed, configure **crp-policy** on BSR routers 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 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.

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
```

Use a named ACL to configure a C-RP policy on the C-BSR: only FC00:0:0:2001::1/128 can function as the C-RP, and the C-RP is allowed to service only the multicast groups in the range of FF13::101/128.

```
<Huawei> system-view
[Huawei] acl ipv6 name myacl6
[Huawei-acl6-adv-myacl6] rule permit ipv6 source fc00:0:0:2001::1 128 destination ff13::101 128
[Huawei-acl6-adv-myacl6] quit
[Huawei] multicast ipv6 routing-enable
[Huawei] pim-ipv6
[Huawei-pim6] crp-policy acl6-name myacl6
```

Related Topics

10.4.12 c-rp (IPv6)

 Copyright © Huawei Technologies Co., Ltd.

10.4.17 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
```

 Copyright © Huawei Technologies Co., Ltd.

```
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 10-56 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.
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.
Source-lifetime	Timeout period of an (S, G) entry. This parameter is configured by the **source-lifetime (IPv6)** command.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
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.
Interface View Default Configurations	Default configurations in the interface view.
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. 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.

Copyright © Huawei Technologies Co., Ltd.

Item	Description
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 state-refresh-capable	Whether State-Refresh is enabled on the interface. This parameter is configured by the **pim ipv6 state-refresh-capable** 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 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.
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 neighbor-policy	Whether the neighbor-policy is set on the interface. This parameter is configured by the **pim ipv6 neighbor-policy** command.

Copyright © Huawei Technologies Co., Ltd.

10.4.18 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
```

 Copyright © Huawei Technologies Co., Ltd.

```
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 10-57 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.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
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.
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.

Copyright © Huawei Technologies Co., Ltd.

Item	Description
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.
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.

Copyright © Huawei Technologies Co., Ltd.

Item	Description
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 bsr-boundary	Whether the PIM boundary is configured on the interface. This parameter is configured by the **pim ipv6 bsr-boundary** 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.

Copyright © Huawei Technologies Co., Ltd.

Item	Description
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.
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 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.

10.4.19 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

Copyright © Huawei Technologies Co., Ltd.

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
```

 Copyright © Huawei Technologies Co., Ltd.

Table 10-58 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.
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.
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.

Copyright © Huawei Technologies Co., Ltd.

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 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.

Copyright © Huawei Technologies Co., Ltd.

Item	Description
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 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.

10.4.20 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

 Copyright © Huawei Technologies Co., Ltd.

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 router 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 10-59 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.

 Copyright © Huawei Technologies Co., Ltd.

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 router exceeds the threshold, the value is 1.

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

10.4.4 c-bsr (IPv6)
10.4.12 c-rp (IPv6)

10.4.21 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: GigabitEthernet1/0/0, RPF neighbor: FE80::A01:100:1
    Referenced route/mask: FC00:0:0:2001::/64
    Referenced route type: igp
    The (S, G) or (*, G) list dependent on this route entry
    (FC00:0:0:2001::2, FF03::1)
```


Copyright © Huawei Technologies Co., Ltd.

Table 10-60 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.
The (S, G) or (*, G) list dependent on this route entry	List of multicast entries based on RPF routes.

10.4.22 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 the device.

```
<Huawei> display pim ipv6 control-message counters
VPN-Instance: public net
 Register* - Register Anycast-RP, Probe* - Probe Anycast-RP
 ------------------------------------------------------------------------------
 PIM global control-message counters:
 Message Type     Received        Sent          Invalid         Filtered
 Register         0               0             0               0
 Register-Stop    0               0             0               0
 Probe            0               0             0               0
 C-RP             0               0             0               0
 Register*        0               0             0               0
 Probe*           0               0             0               0
```

 Copyright © Huawei Technologies Co., Ltd.

```
PIM control-message counters for interface: GigabitEthernet1/0/1
Message Type      Received          Sent             Invalid          Filtered
Assert            0                 0                0                0
Graft             0                 0                0                0
Graft-Ack         0                 0                0                0
Hello             0                 35               0                0
Join-prune        0                 0                0                0
State-Refresh     0                 0                0                0
BSR               0                 0                0                0
```

Table 10-61 Description of the display pim ipv6 control-message counters command output

Item	Description
VPN-Instance	VPN instance to which the statistics of PIM messages belong.
PIM global control-message counters	Number of PIM control messages in the public network.
PIM control-message counters for interface	Name of the interface for collecting statistics on PIM control messages
Message Type	Type of the control message.
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.
Register	Number of Register messages.
Register-Stop	Number of Register-Stop messages.
Probe	Number of Probe messages.
C-RP	Number of Advertisement 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.
Register*	Number of Register messages for anycast RP.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Probe*	Number of Probe messages for anycast RP.

Related Topics

10.4.70 reset pim ipv6 control-message counters

10.4.23 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 router 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 10-62 Description of the display pim ipv6 grafts command output

Item	Description
Source	Multicast source address.

Copyright © Huawei Technologies Co., Ltd.

Item	Description
Group	Multicast group address.
Expire	Timeout period of an (S, G) entry.
RetransmitIn	Amount of time before the next Graft message is transmitted.

10.4.24 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.	-
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.

 Copyright © Huawei Technologies Co., Ltd.

Example

Display PIM (IPv6) information on GE1/0/0.

```
<Huawei> display pim ipv6 interface gigabitethernet 1/0/0
 VPN-Instance: public net
 Interface      State  NbrCnt  HelloInt  DR-Pri     DR-Address
 GE1/0/0         up     0        30         1         FE80::2E0:3FFF:FE27:AE01(local)
```

Table 10-63 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 GE1/0/0.

```
<Huawei> display pim ipv6 interface gigabitethernet 1/0/0 verbose
 VPN-Instance: public net
 Interface: GigabitEthernet1/0/0, 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: -
```

 Copyright © Huawei Technologies Co., Ltd.

Table 10-64 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.
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.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
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 border is configured on the interface.
PIM dr-switch-delay timer	DR switching delay.
Number of routers on link not using DR priority	Number of routers 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 routers 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 routers 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.

Related Topics

10.4.26 display pim ipv6 neighbor

10.4.25 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** }] *

 Copyright © Huawei Technologies Co., Ltd.

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.	-
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.	-

Copyright © Huawei Technologies Co., Ltd.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

When a fault occurs on an 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.

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

AnycastRP 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
```

 Copyright © Huawei Technologies Co., Ltd.

```
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 10-65 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.
AnycastRP Register invalid packet	Statistics about invalid Register packets in the anycast-RP scenario.
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.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
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.
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.

 Copyright © Huawei Technologies Co., Ltd.

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          :  GigabitEthernet1/0/0
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 10-66 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.

Copyright © Huawei Technologies Co., Ltd.

Related Topics

10.8.12 multicast ipv6 invalid-packet

10.4.26 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 GE1/0/0.

```
<Huawei> display pim ipv6 neighbor interface gigabitethernet 1/0/0 verbose
 VPN-Instance: public net
```

 Copyright © Huawei Technologies Co., Ltd.

```
Total Number of Neighbors on this interface  = 1

Neighbor: FE80::FFE0:FFFF:FE4A:8E04
    Interface: GigabitEthernet1/0/0
    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 10-67 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.

Related Topics

10.4.24 display pim ipv6 interface

 Copyright © Huawei Technologies Co., Ltd.

10.4.27 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** }] *

NOTE

If you specify the **register** keyword before **mode**, the value of **mode** can only be **sm**.

After the PIM mode is set to **dm** or **ssm**, the **register** keyword cannot be specified in the command.

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.	-

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
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.	-
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.	The value is an integer that ranges from 0 to 2048.
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

 Copyright © Huawei Technologies Co., Ltd.

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 10-68 lists the values of the **flags** *flag-value* parameter.

Table 10-68 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 router 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 router and PIM (IPv6) is the owner of the downstream interface.
sgjoin	Indicates that the (S, G) receiver of S exists on the local router 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.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
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: GigabitEthernet1/0/0
             Protocol: static, UpTime: 00:57:31, Expires: never

 (FC00:0:0:2001::2, FFE3::1)
     Protocol: pim-sm, Flag: SWT ACT
     UpTime: 00:04:24
     Upstream interface: GigabitEthernet2/0/0
         Upstream neighbor: FE80::A01:100:1
         RPF prime neighbor: FE80::A01:100:1
     Downstream interface(s) information:
     Total number of downstreams: 1
         1: GigabitEthernet1/0/0
             Protocol: pim-sm, UpTime: 00:04:24, Expires:  -
```

Table 10-69 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.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
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.
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.
GigabitEthernet1/0/0	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: GE1/0/0
     Number of downstreams: 2
 00002.(*, FF25::1)
     Upstream interface: GE1/0/0
     Number of downstreams: 2
```

Table 10-70 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.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
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
```

Related Topics

10.8.4 display multicast ipv6 routing-table

10.4.28 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

Copyright © Huawei Technologies Co., Ltd.

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 10-71 Description of the display pim ipv6 rp-info command output

Item	Description
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

Related Topics

10.4.12 c-rp (IPv6)

10.4.29 embedded-rp

Function

The **embedded-rp** command enables the embedded RP function.

 Copyright © Huawei Technologies Co., Ltd.

The **undo embedded-rp** command disables the embedded RP function.

By default, the embedded RP function is enabled.

Format

embedded-rp [*basic-acl6-number* | **acl6-name** *acl6-name*]

undo embedded-rp [*basic-acl6-number* | **acl6-name** *acl6-name*]

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.
acl6-name *acl6-name*	Specifies the name of an IPv6 Named ACL. **NOTE** **acl6-name** *acl6-name* can only be the name of a named advanced ACL.	The value is a string of 1 to 32 case-sensitive characters without spaces. The value must start with a letter (case sensitive).

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 router to obtain the RP address from the IPv6 multicast address of a received multicast packet, so that the router does not need to know the RP information beforehand.

By default, the router can parse group addresses in the range of FF7x::/12. The value of x can 0 or any integer in the range of 3 to F. When the router receives a multicast packet with an IPv6 group address in this range, the router 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 router 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 using the **multicast ipv6 routing-enable** command in the system view.

Precautions

 Copyright © Huawei Technologies Co., Ltd.

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.

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
```

Configure a named ACL6 to enable the embedded RP on the multicast group ff73::.

```
<Huawei> system-view
[Huawei] acl ipv6 name myacl6
[Huawei-acl6-adv-myacl6] rule permit ipv6 destination ff73:: 12
[Huawei-acl6-adv-myacl6] quit
[Huawei] multicast ipv6 routing-enable
[Huawei] pim-ipv6
[Huawei-pim6] embedded-rp acl6-name myacl6
```

Related Topics

10.4.59 pim ipv6 sm

10.4.30 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.

NOTE

Only the AR3200 series routers support PIM GR (IPv6).

Format

graceful-restart

undo graceful-restart

Parameters

None

Views

PIM-IPv6 view

 Copyright © Huawei Technologies Co., Ltd.

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On the PIM-SM (IPv6) network, after an active/standby switchover is performed on the router equipped with two MPUs, the new active MPU deletes original PIM (IPv6) forwarding entries. Because the active MPU on the router cannot create new PIM (IPv6) forwarding entries in a short time, multicast data transmission is interrupted.

PIM GR enables the router to back up join and prune information in PIM (IPv6) routing entries to the new MPU when an active/standby switchover is performed on the router. This ensures normal multicast data forwarding during restoration of the multicast distribution tree.

Prerequisites

IPv6 multicast routing has been enabled using the **multicast ipv6 routing-enable** command in the system view.

Precautions

At least one router interface is enabled with PIM-SM (IPv6) so that the **graceful-restart** command takes 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
```

Related Topics

10.4.59 pim ipv6 sm

10.4.31 graceful-restart period (IPv6)

10.4.31 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.

NOTE

Only the AR3200 series routers support PIM GR (IPv6).

Copyright © Huawei Technologies Co., Ltd.

Format

graceful-restart period *period*

undo graceful-restart period

Parameters

Parameter	Description	Value
period	Specifies the minimum PIM GR period.	It 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 minimal time for maintaining forwarding entries.

Prerequisites

IPv6 multicast routing has been enabled using the **multicast ipv6 routing-enable** command in the system view.

Precautions

PIM GR is on the basis of unicast GR; therefore, the minimum PIM GR period should be longer than the corresponding unicast GR period.

The PIM GR period also depends on the complexity of the network topology and increases as 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
```

Related Topics

10.4.59 pim ipv6 sm

10.4.30 graceful-restart (IPv6)

Copyright © Huawei Technologies Co., Ltd.

10.4.32 hello-option dr-priority (IPv6)

Function

The **hello-option dr-priority** command configures the DR (Designated Router) priority for the router.

The **undo hello-option dr-priority** command restores the default DR priority.

By default, the DR priority for the router is 1.

Format

hello-option dr-priority *priority*

undo hello-option dr-priority

Parameters

Parameter	Description	Value
priority	Specifies the DR priority of the router.	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

In PIM-SM (IPv6), routers on the shared network segment candidates for the DR. The DR is responsible for the registering of the local multicast source and the joining of the receivers.

The DR election is based on the priority and the IPv6 address. To elect the DR, the routers send the Hello message that contains the priority to each other. The router with the highest priority functions as the DR. If the routers have the same priority, the router with the largest IPv6 address functions as the DR.

If there is at least one router that does not support Hello packets that contain the priority in the network, the DR election is based on the IPv6 address of each router. The router 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

 Copyright © Huawei Technologies Co., Ltd.

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 router to 3.

```
<Huawei> system-view
[Huawei] multicast ipv6 routing-enable
[Huawei] pim-ipv6
[Huawei-pim6] hello-option dr-priority 3
```

Related Topics

10.4.48 pim ipv6 hello-option dr-priority

10.4.33 hello-option holdtime (IPv6)

Function

The **hello-option holdtime** command sets the timeout period for a router 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 router 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 router 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

Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

Usage Scenario

On the PIM (IPv6) network, after the device receives a Hello message from its PIM neighbor, the device starts the timer. The timer value is the value of Holdtime in the Hello message. If the device does not receive any Hello message from its PIM neighbor after the timeout, the device considers the neighbor invalid or unreachable.

The **hello-option holdtime (IPv6)** 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 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 router 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
```

Related Topics

10.4.49 pim ipv6 hello-option holdtime

10.4.34 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.

Copyright © Huawei Technologies Co., Ltd.

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 by devices carry **lan-delay** and **override-interval**. The **lan-delay** parameter indicates the delay in transmitting messages in the LAN. When the values of **lan-delay** on all devices on the same link are different, the maximum value of these values is used.

When a device sends a Prune message to the upstream device in the same network segment, if other device still requests the multicast data, it needs to send a Join message to the upstream device in the override-interval period.

The value of the Prune-Pending Timer (PPT) is obtained by the value of **lan-delay** plus the value of **override-interval**. PPT refers to the delay during which the current device receives a Prune message from the downstream interface and performs the prune action. If the device receives a Join message from the downstream interface in PPT, the device 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.

 Copyright © Huawei Technologies Co., Ltd.

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
```

Related Topics

10.4.36 hello-option override-interval (IPv6)

10.4.50 pim ipv6 hello-option lan-delay

10.4.35 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 device generates a Generation ID and encapsulates it into the message. The Generation ID changes only when the device status changes. After receiving the Hello message, the neighboring device detects Generation ID change and immediately sends a Join message to the device to update the neighbor relationship. If multiple devices on the shared network segment send Join messages to the same upstream PIM neighbor, only one device

 Copyright © Huawei Technologies Co., Ltd.

is allowed to send the Join message. After other devices detect the Join message, they do not send Join messages to the upstream neighbor. The upstream neighbor cannot update neighbor relationships with downstream devices because of Generation ID change.

When the device with neighbor tracking enabled 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 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 neighnor-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
```

Related Topics

10.4.51 pim ipv6 hello-option neighbor-tracking

10.4.36 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

Copyright © Huawei Technologies Co., Ltd.

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 by routers carry **lan-delay** and **override-interval**. The **override-interval** parameter refers to the period during which a downstream router overrides the prune action.

When a router sends a Prune message to the upstream router in the same network segment, if other router still requests the multicast data, it needs to send a Join message to the upstream router in the override-interval period.

When the values of **override-interval** on all routers on the same link are different, the maximum value of these values is used.

The value of PPT is obtained by the value of **lan-delay** plus the value of **override-interval**. When receiving a Prune message from a downstream interface, the router does not perform the prune action until the PPT times out. If the router receives a Join message from the downstream interface in PPT, the interface 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).

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.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> system-view
[Huawei] multicast ipv6 routing-enable
[Huawei] pim-ipv6
[Huawei-pim6] hello-option override-interval 2000
```

Related Topics

10.4.34 hello-option lan-delay (IPv6)

10.4.52 pim ipv6 hello-option override-interval

10.4.37 holdtime assert (IPv6)

Function

The **holdtime assert** command sets the timeout period for all PIM interfaces to keep the Assert state on the local router.

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 router 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

 Copyright © Huawei Technologies Co., Ltd.

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 router keeps the Assert state to 100s.

```
<Huawei> system-view
[Huawei] multicast ipv6 routing-enable
[Huawei] pim-ipv6
[Huawei-pim6] holdtime assert 100
```

Related Topics

10.4.53 pim ipv6 holdtime assert

10.4.38 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.

Copyright © Huawei Technologies Co., Ltd.

Views

PIM-IPv6 view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After receiving a Join/Prune message from the downstream device, the device starts the holdtime timer. After the timeout interval, if the device does not receive subsequent Join/Prune messages from the downstream device, the downstream interface of a multicast group is suppressed from forwarding Join/Prune messages with information about multicast group joining. If Join/Prune messages carry information about multicast group prune, the downstream interface of the multicast group is restored.

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 router 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
```

Related Topics

10.4.54 pim ipv6 holdtime join-prune

10.4.39 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.

Copyright © Huawei Technologies Co., Ltd.

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 single Join/Prune message carrying a lot of (S, G) entries, the maximum size of each Join/Prune message can be set to a small value to limit the number of (S, G) entries in each message, relieving the burden on the peer device.

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 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
```

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

10.4.40 join-prune periodic-messages queue-size (IPv6)
10.4.41 join-prune triggered-message-cache disable (IPv6)

10.4.40 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, change the length of a queue for periodically sending messages to a small value 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 using the **multicast ipv6 routing-enable** command in the system view.

 Copyright © Huawei Technologies Co., Ltd.

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
```

Related Topics

10.4.39 join-prune max-packet-length (IPv6)
10.4.41 join-prune triggered-message-cache disable (IPv6)

10.4.41 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 to send a package of Join/Prune messages than to send a large number of individual Join/Prune messages. A device sends

 Copyright © Huawei Technologies Co., Ltd.

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 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
```

Related Topics

10.4.39 join-prune max-packet-length (IPv6)

10.4.40 join-prune periodic-messages queue-size (IPv6)

10.4.42 local-address (IPv6)

Function

The **local-address** command sets a local address for an Anycast RP.

The **undo local-address** command deletes the local address set for an Anycast RP.

By default, no local address is set for an Anycast RP.

Format

local-address *local-address*

undo local-address

Parameters

Parameter	Description	Value
local-address	Specifies the local address of Anycast RP.	The value must be a legal IPv6 unicast IP address in hexadecimal notation.

Views

Anycast-RP view

Copyright © Huawei Technologies Co., Ltd.

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If PIM (IPv6) Anycast RP is configured, after an RP receives a Register message, it checks the source address of the Register message. If the Register message is sent by the source's DR, the RP forwards the Register message to Anycast RP peers. If the Register message is sent by an Anycast RP peer, it does not forward the Register message.

When forwarding a PIM Register message to other Anycast RP peers, the local RP needs to use its own IPv6 address (called the local address) as the source address of the Register message and use the addresses of Anycast RP peers as the destination addresses of the Register message. In such a manner, Anycast RP peers can learn source/group information from each other. This command is used to set a local address for an Anycast RP.

Prerequisites

The local address specified for Anycast RP must be an existing interface IPv6 address.

Precautions

The local address must be different from the Anycast RP address.

NOTE

Setting a Loopback interface address as the local address of the Anycast RP is recommended.

Example

In the Anycast RP view, set the Anycast RP address to FC00:0:0:2001::1 and local address of Anycast RP to FC00:0:0:1::1.

```
<Huawei> system-view
[Huawei] multicast ipv6 routing-enable
[Huawei] pim-ipv6
[Huawei-pim6] anycast-rp fc00:0:0:2001::1
[Huawei-pim6-anycast-rp-2001::1] local-address fc00:0:0:1::1
```

Related Topics

10.4.1 anycast-rp (IPv6)
10.4.44 peer (IPv6)

10.4.43 neighbor-check (IPv6)

Function

The **neighbor-check** command enables the PIM neighbor check function.

The **undo neighbor-check** command restores the default setting.

 Copyright © Huawei Technologies Co., Ltd.

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 PIM-SM (IPv6) and PIM-DM (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
```

 Copyright © Huawei Technologies Co., Ltd.

```
[Huawei] pim-ipv6
[Huawei-pim6] neighbor-check receive
```

10.4.44 peer (IPv6)

Function

The **peer** command configures Anycast RP peers.

The **undo peer** command removes the configurations of Anycast RPs.

By default, no Anycast RP peer is configured.

Format

peer *peer-address*

undo peer *peer-address*

Parameters

Parameter	Description	Value
peer-address	Specifies the address of an Anycast RP peer.	The value is in hexadecimal notation.

Views

Anycast-RP view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If PIM (IPv6) Anycast RP is configured, after an RP receives a Register message, it checks the source address of the Register message. If the Register message is sent by the source's DR, the RP forwards the Register message to Anycast RP peers. If the Register message is sent by an Anycast RP peer, it does not forward the Register message.

When forwarding a PIM Register message to other Anycast RP peers, the local RP needs to use its own IPv6 address (called the local address) as the source address of the Register message and use the addresses of Anycast RP peers as the destination addresses of the Register message. In such a manner, Anycast RP peers can learn source/group information from each other. This command is used to configure an address for an Anycast RP peer. This address is used as the destination address of the Register message to be sent by the local RP.

Precautions

You can specify a maximum of 16 Anycast RP peers for each Anycast RP.

 Copyright © Huawei Technologies Co., Ltd.

In a PIM-SM (IPv6) domain, all the devices deployed with Anycast RP must be fully connected logically. Anycast RP peer relationships need to be configured between every two devices deployed with the Anycast RP.

Example

In the Anycast RP view, set the Anycast RP address to FC00:0:0:3::3 and the peer address to FC00:0:0:2::2.

```
<Huawei> system-view
[Huawei] multicast ipv6 routing-enable
[Huawei] pim-ipv6
[Huawei-pim6] anycast-rp fc00:0:0:3::3
[Huawei-pim6-anycast-rp-fc00:0:0:3::3] peer fc00:0:0:2::2
```

Related Topics

10.4.42 local-address (IPv6)

10.4.1 anycast-rp (IPv6)

10.4.45 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

 Copyright © Huawei Technologies Co., Ltd.

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]
```

Related Topics

10.8.16 multicast ipv6 routing-enable

10.4.46 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

Interface view

Default Level

2: Configuration level

Copyright © Huawei Technologies Co., Ltd.

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 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 GE1/0/0.

```
<Huawei> system-view
[Huawei] multicast ipv6 routing-enable
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] pim ipv6 bsr-boundary
```

Related Topics

10.4.4 c-bsr (IPv6)

10.4.47 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

Interface view

Copyright © Huawei Technologies Co., Ltd.

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 network with densely-distributed group members.

After PIM-DM (IPv6) is enabled on an interface, the router can set up the PIM neighbor relationship with the neighboring device. The router 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.

Example

Enable PIM-DM (IPv6) on GE1/0/0.

```
<Huawei> system-view
[Huawei] multicast ipv6 routing-enable
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] pim ipv6 dm
```

Related Topics

10.8.16 multicast ipv6 routing-enable

10.4.59 pim ipv6 sm

10.4.48 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

Copyright © Huawei Technologies Co., Ltd.

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

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In PIM (IPv6), devices on the shared network segment candidates for the DR. The DR is responsible for the registering of the local multicast source and the joining of the receivers.

The DR election is based on the priority and the IPv6 address. To elect the DR, the devices send the Hello message that contains the priority to each other. The device with the highest priority functions as the DR. If the devices have the same priority, the device with the largest IPv6 address functions as the DR.

If there is at least one device that does not support Hello packets that contain the priority in the network, the DR election is based on the IPv6 address of each device. 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 GE1/0/0 that is elected as DR to 3.

```
<Huawei> system-view
[Huawei] multicast ipv6 routing-enable
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] pim ipv6 hello-option dr-priority 3
```

Related Topics

10.4.32 hello-option dr-priority (IPv6)

Copyright © Huawei Technologies Co., Ltd.

10.4.49 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

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On the PIM (IPv6) network, after the device receives a Hello message from its PIM neighbor, the device starts the timer. The timer value is the value of Holdtime in the Hello message. If the device does not receive any Hello message from its PIM neighbor after the timeout, the device 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 using the **multicast ipv6 routing-enable** command in the system view.

Precautions

Copyright © Huawei Technologies Co., Ltd.

The timeout period must be greater than the interval for sending Hello messages. You can run the **pim ipv6 time hello** command to set the interval for sending Hello messages.

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 GE1/0/0 waits to receive Hello messages from its neighbor to 120 seconds.

```
<Huawei> system-view
[Huawei] multicast ipv6 routing-enable
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] pim ipv6 hello-option holdtime 120
```

Related Topics

10.4.33 hello-option holdtime (IPv6)

10.4.50 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

Interface view

Copyright © Huawei Technologies Co., Ltd.

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Hello messages sent by devices carry **lan-delay** and **override-interval**. The **lan-delay** parameter indicates the delay in transmitting messages in the LAN. When the values of **lan-delay** on all devices on the same link are different, the maximum value of these values is used.

When a device sends a Prune message to the upstream device in the same network segment, if other device still requests the multicast data, it needs to send a Join message to the upstream device in the override-interval period.

The value of the Prune-Pending Timer (PPT) is obtained by the value of **lan-delay** plus the value of **override-interval**. PPT refers to the delay during which the current device receives a Prune message from the downstream interface and performs the prune action. If the device receives a Join message from the downstream interface in PPT, the device 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 GE1/0/0.

```
<Huawei> system-view
[Huawei] multicast ipv6 routing-enable
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] pim ipv6 hello-option lan-delay 200
```

Related Topics

10.4.52 pim ipv6 hello-option override-interval

10.4.34 hello-option lan-delay (IPv6)

 Copyright © Huawei Technologies Co., Ltd.

10.4.51 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

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When sending a Hello message, the device generates a Generation ID and encapsulates it into the message. The Generation ID changes only when the device status changes. After receiving the Hello message, the neighboring device detects Generation ID change and immediately sends a Join message to the device to update the neighbor relationship. If multiple devices on the shared network segment 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. The upstream neighbor cannot update neighbor relationships with downstream devices because of 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 using the **multicast ipv6 routing-enable** command in the system view.

Precautions

 Copyright © Huawei Technologies Co., Ltd.

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 GE1/0/0.

```
<Huawei> system-view
[Huawei] multicast ipv6 routing-enable
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] pim ipv6 hello-option neighbor-tracking
```

Related Topics

10.4.35 hello-option neighbor-tracking (IPv6)

10.4.52 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

Interface view

Default Level

2: Configuration level

Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

Usage Scenario

Hello messages sent by devices carry **lan-delay** and **override-interval**. The **override-interval** parameter refers to the period during which a downstream router overrides the prune action.

When a device sends a Prune message to the upstream device in the same network segment, if other device still requests the multicast data, it needs to send a Join message to the upstream device in the override-interval period.

When the values of **override-interval** on all devices on the same link are different, the maximum value of these values is used.

The value of PPT is obtained by the value of **lan-delay** plus the value of **override-interval**. When receiving a Prune message from a downstream interface, the device does not perform the prune action until the PPT times out. If the device receives a Join message from the downstream interface in PPT, the interface cancels the Prune action.

Prerequisites

IPv6 multicast routing has been enabled 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 GE1/0/0.

```
<Huawei> system-view
[Huawei] multicast ipv6 routing-enable
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] pim ipv6 hello-option override-interval 2000
```

Related Topics

10.4.50 pim ipv6 hello-option lan-delay

10.4.36 hello-option override-interval (IPv6)

10.4.53 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.

Copyright © Huawei Technologies Co., Ltd.

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

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 retains 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 GE1/0/0 to keep the Assert state to 100s.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> system-view
[Huawei] multicast ipv6 routing-enable
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] pim ipv6 holdtime assert 100
```

Related Topics

10.4.37 holdtime assert (IPv6)

10.4.54 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

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After receiving a Join/Prune message from the downstream device, the router starts the holdtime timer. After the timeout interval, if the router does not receive subsequent Join/Prune messages from the downstream device, the downstream interface of a multicast group is suppressed from forwarding Join/Prune messages with information about multicast group joining. If Join/Prune messages carry information about multicast group prune, the downstream interface of the multicast group is restored.

Copyright © Huawei Technologies Co., Ltd.

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 GE1/0/0 to 280 seconds.

```
<Huawei> system-view
[Huawei] multicast ipv6 routing-enable
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] pim ipv6 holdtime join-prune 280
```

Related Topics

10.4.38 holdtime join-prune (IPv6)

10.4.55 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* | **acl6-name** *acl6-name* } | **ssm** { *advanced-acl6-number* | **acl6-name** *acl6-name* } | *advanced-acl6-number* | **acl6-name** *acl6-name* }

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.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
acl6-name *acl6-name*	Specifies the name of a named ACL. **NOTE** **acl6-name** *acl6-name* can only be the name of a named advanced ACL.	The value is a string of 1 to 32 case-sensitive characters without spaces. The value must start with a letter (case sensitive).
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

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, run the **pim ipv6 join-policy** command to enable the system to filter join information in Join/Prune messages.

Prerequisites

IPv6 multicast routing has been enabled using the **multicast ipv6 routing-enable** command in the system view.

Configuration Impact

The **pim ipv6 join-policy** command and the **acl ipv6 (system view)** command are used together.

- If **asm** is specified, in the basic ACL6 view, you can set the multicast group address range of join information by specifying the **source** parameter in the **rule (basic ACL6 view)** command.
- If **ssm** is specified, in the advanced ACL6 view, you can set the source address range and multicast group address range of join information by respectively specifying the **source** parameter and **destination** parameter in the **rule (advanced ACL6 view)** command.

The rule configurations for a named ACL and an advanced ACL are the same. The **time-range** parameter takes effect in the **rule** command only for the named ACL.

 Copyright © Huawei Technologies Co., Ltd.

Example

Configure GE1/0/0 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 1/0/0
[Huawei-GigabitEthernet1/0/0] pim ipv6 join-policy asm 2001
```

Use a named ACL6 to configure GE1/0/0 to accept the Join messages with the source address FC00:0:0:2001::4 and group address FF35::1.

```
<Huawei> system-view
[Huawei] acl ipv6 name myacl
[Huawei-acl6-adv-myacl] rule permit ipv6 source fc00:0:0:2001::4 128 destination ff35::1 128
[Huawei-acl6-adv-myacl] quit
[Huawei] multicast ipv6 routing-enable
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] pim ipv6 join-policy ssm acl6-name myacl
```

10.4.56 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* | **acl6-name** *acl6-name* }

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.
acl6-name *acl6-name*	Specifies the ACL name. **NOTE** **acl6-name** *acl6-name* can only be the name of a named advanced ACL.	The value is a string of 1 to 32 case-sensitive characters without spaces. The value must start with a letter (case sensitive).

Views

Interface view

Copyright © Huawei Technologies Co., Ltd.

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 device 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 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.

For the named ACL, in the ACL view, when the **rule** command is used to configure a filtering rule, the filtering rule takes effect for only the multicast group address range specified by **source** and the time range specified by **time-range**.

Precautions

This command is valid for both PIM-DM (IPv6) and PIM-SM (IPv6).

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 GE1/0/0 to set up the PIM neighbor relationship with the router 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 1/0/0
[Huawei-GigabitEthernet1/0/0] pim ipv6 neighbor-policy 2001
```

10.4.57 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.

 Copyright © Huawei Technologies Co., Ltd.

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

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After an interface on the device is enabled with PIM, the device generates a random number as the generation ID of the Hello message. If the status of the device is updated, the device generates a new Generation ID. When the device finds that the Hello message received from a PIM neighbor contains a different Generation ID, the device considers that the status of the PIM neighbor changes.

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 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 GE1/0/0 to reject the Hello messages without the generation ID.

```
<Huawei> system-view
[Huawei] multicast ipv6 routing-enable
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] pim ipv6 require-genid
```

 Copyright © Huawei Technologies Co., Ltd.

10.4.58 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

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To protect the router 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 router 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

 Copyright © Huawei Technologies Co., Ltd.

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 routers 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 GE1/0/0.

```
<Huawei> system-view
[Huawei] multicast ipv6 routing-enable
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] pim ipv6 silent
```

10.4.59 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

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

 Copyright © Huawei Technologies Co., Ltd.

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.

Example

Enable PIM-SM (IPv6) on GE1/0/0.

```
<Huawei> system-view
[Huawei] multicast ipv6 routing-enable
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] pim ipv6 sm
```

Related Topics

10.8.16 multicast ipv6 routing-enable

10.4.47 pim ipv6 dm

10.4.60 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

Interface view

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

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 router in the pruned state resets the prune-status timer. As a result, the downstream interface cannot forward packets before the prune-status timer times out.

After PIM-DM (IPv6) state-refresh is disabled, the interface starts to forward multicast data when the prune timer times out. The downstream routers that do not want to receive the data can send Prune messages. The process is performed periodically, which wastes a lot of network resources. Enabling PIM-DM (IPv6) State-Refresh can optimize the network traffic.

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 GE1/0/0.

```
<Huawei> system-view
[Huawei] multicast ipv6 routing-enable
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] undo pim ipv6 state-refresh-capable
```

10.4.61 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

Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
interval	Specifies the delay.	The value is an integer that ranges from 10 to 3600, in seconds.

Views

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).

Example

Enable PIM DR switching delay on GE1/0/0 and set the delay to 20 seconds.

```
<Huawei> system-view
[Huawei] multicast ipv6 routing-enable
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] pim ipv6 timer dr-switch-delay 20
```

10.4.62 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.

Copyright © Huawei Technologies Co., Ltd.

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

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In PIM-DM (IPv6) mode, when a member joins a pruned group, the router sends a Graft message and waits to receive an ACK message from the upstream router. If the downstream router does not receive the ACK message in the period configured through the command, the router resends the Graft message until the router receives the ACK message from the upstream router.

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 GE1/0/0.

```
<Huawei> system-view
[Huawei] multicast ipv6 routing-enable
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] pim ipv6 timer graft-retry 80
```

10.4.63 pim ipv6 timer hello

Function

The **pim ipv6 timer hello** command sets the interval for sending Hello messages on an interface.

Copyright © Huawei Technologies Co., Ltd.

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

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 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, except for the 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 Hello messages to 40 seconds on GE1/0/0.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> system-view
[Huawei] multicast ipv6 routing-enable
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] pim ipv6 timer hello 40
```

Related Topics

10.4.80 timer hello (IPv6)

10.4.49 pim ipv6 hello-option holdtime

10.4.64 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

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.

Copyright © Huawei Technologies Co., Ltd.

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).

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 GE1/0/0.

```
<Huawei> system-view
[Huawei] multicast ipv6 routing-enable
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] pim ipv6 timer join-prune 80
```

Related Topics

10.4.81 timer join-prune (IPv6)

10.4.54 pim ipv6 holdtime join-prune

10.4.65 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.

Copyright © Huawei Technologies Co., Ltd.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

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 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 gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] pim ipv6 triggered-hello-delay 3
```

10.4.66 probe-interval (IPv6)

Function

The **probe-interval** command sets the interval for a router 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 router 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.

Copyright © Huawei Technologies Co., Ltd.

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 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
```

Related Topics

10.4.69 register-suppression-timeout (IPv6)

10.4.67 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.

Copyright © Huawei Technologies Co., Ltd.

Format

register-policy { *advanced-acl6-number* | **acl6-name** *acl6-name* }

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.
acl6-name *acl6-name*	Specifies the name of a Named ACL. **NOTE** **acl6-name** *acl6-name* can only be the name of a named advanced ACL.	The value is a string of 1 to 32 case-sensitive characters without spaces. The value must start with a letter (case sensitive).

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.

Prerequisites

IPv6 multicast routing has been enabled 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.

 Copyright © Huawei Technologies Co., Ltd.

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
```

Configure an IPv6 Named ACL, the RP receives 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 name myacl6
[Huawei-acl6-adv-myacl6] rule permit ipv6 source fc00:0:0:2001::2 64 destination ff02:13:: 64
[Huawei-acl6-adv-myacl6] quit
[Huawei] multicast ipv6 routing-enable
[Huawei] pim-ipv6
[Huawei-pim6] register-policy acl6-name myacl6
```

10.4.68 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.	The value is a 32-digit hexadecimal number, in the format X:X:X:X:X:X:X:X.

Views

PIM-IPv6 view

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

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 using the **multicast ipv6 routing-enable** command in the system view.

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
```

10.4.69 register-suppression-timeout (IPv6)

Function

The **register-suppression-timeout** command sets the timeout period during which a router keeps the register suppression state.

The **undo register-suppression-timeout** command restores the default timeout period.

By default, a router 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 router keeps the register suppression state.	The value is an integer that ranges from 11 to 3600, in seconds.

Views

PIM-IPv6 view

Copyright © Huawei Technologies Co., Ltd.

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After receiving a Register-Stop message from the RP, the router immediately stops sending Register messages and enters the register suppression state.

The **register-suppression-timeout** command determines how long the router keeps the register suppression state. When the timeout period expires, the router (source DR) starts to send Register messages to the RP.

Prerequisites

IPv6 multicast routing has been enabled 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, the delay for a new receiver to join a group is long when an (S, G) entry on the RP times out.

You can use the **probe-interval (IPv6)** command to configure the router 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 router 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
```

Related Topics

10.4.66 probe-interval (IPv6)

10.4.70 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*]

Copyright © Huawei Technologies Co., Ltd.

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 on the device has been forwarding multicast packets in a long period of time, the device 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
```

Related Topics

10.4.22 display pim ipv6 control-message counters

10.4.71 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*

Copyright © Huawei Technologies Co., Ltd.

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.
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 the sending of corresponding Join/Prune messages, which cause multicast service interruption.

 Copyright © Huawei Technologies Co., Ltd.

Example

Clear PIM status of the downstream interface GE1/0/0 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 gigabitethernet 1/0/0
```

10.4.72 source-lifetime (IPv6)

Function

The **source-lifetime** command specifies the timeout period of an (S, G) entry on the router.

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*

undo source-lifetime

Parameters

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

Views

PIM-IPv6 view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A router 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.

Prerequisites

IPv6 multicast routing has been enabled using the **multicast ipv6 routing-enable** command in the system view.

Precautions

Copyright © Huawei Technologies Co., Ltd.

This command is valid for both PIM-DM (IPv6) and PIM-SM (IPv6).

Example

Set the timeout period of an (S, G) entry of the router to 200 seconds.

```
<Huawei> system-view
[Huawei] multicast ipv6 routing-enable
[Huawei] pim-ipv6
[Huawei-pim6] source-lifetime 200
```

10.4.73 source-policy (IPv6)

Function

The **source-policy** command configures the router 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 router does not filter received multicast data packets based on source addresses or source/group addresses.

Format

source-policy { *acl6-number* | **acl6-name** *acl6-name* }

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.
acl6-name *acl6-name*	Specifies the name of a named ACL. **NOTE** **acl6-name** *acl6-name* can only be the name of a named advanced ACL.	The value is a string of 1 to 32 case-sensitive characters without spaces. The value must start with a letter (case sensitive).

Views

PIM-IPv6 view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

 Copyright © Huawei Technologies Co., Ltd.

To prevent unauthorized source information from being advertised on the PIM network, run the **source-policy** command to configure the router to filter received multicast data packets based on source addresses or source/group addresses.

Prerequisites

IPv6 multicast routing has been enabled using the **multicast ipv6 routing-enable** command in the system view.

Configuration Impact

If **source-policy** and the basic ACL are applied, all multicast data packets received should match the source address. Packets that do not pass the filtering are discarded.

If **source-policy** and the advanced ACL are used, the source addresses and group addresses of all received multicast data packets should be matched. Packets that do not pass the filtering are discarded.

The configurations of the Named ACL and 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.

Precautions

This command is valid for both PIM-DM (IPv6) and PIM-SM (IPv6).

Example

In the public network instance, configure the router 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
```

In the public network instance, configure a Named ACL where multicast data packets with the source address of FC00:0:0:3121::1 are received, and those with the source address of 3121::2 are dropped.

```
<Huawei> system-view
[Huawei] acl ipv6 name myacl6
[Huawei-acl6-adv-myacl6] rule permit ipv6 source fc00:0:0:3121::1 128
[Huawei-acl6-adv-myacl6] rule deny ipv6 source fc00:0:0:3121::2 128
[Huawei-acl6-adv-myacl6] quit
[Huawei] multicast ipv6 routing-enable
[Huawei] pim-ipv6
[Huawei-pim6] source-policy acl6-name myacl6
```

10.4.74 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.

 Copyright © Huawei Technologies Co., Ltd.

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* | **acl6-name** *acl6-name* } [**order** *order-value*]]

undo spt-switch-threshold [*traffic-rate* | **infinity**] [**group-policy** { *basic-acl6-number* | **acl6-name** *acl6-name* }]

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.	-
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.
acl6-name *acl6-name*	Specifies the name of a Named ACL. **NOTE** **acl6-name** *acl6-name* can only be the name of a named advanced ACL.	The value is a string of 1 to 32 case-sensitive characters without spaces. The value must start with a letter (case sensitive) and can contain numbers, hyphens (-), or underlines (_).

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
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 a 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 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 command that is first matched according to the order 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).

 Copyright © Huawei Technologies Co., Ltd.

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 router 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
```

Add a group-policy: the ACL name, rate threshold, and order of the group-policy are myacl6, 100 kbit/s, and 1 respectively.

```
<Huawei> system-view
[Huawei] acl ipv6 name myacl6
[Huawei-acl6-adv-myacl6] rule permit ipv6 destination ff03::101 128
[Huawei-acl6-adv-myacl6] quit
[Huawei] multicast ipv6 routing-enable
[Huawei] pim-ipv6
[Huawei-pim6] spt-switch-threshold 100 group-policy acl6-name myacl6 order 1
```

Related Topics

10.4.82 timer spt-switch (IPv6)

10.4.75 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, where x cannot be 1 or 2.

Format

ssm-policy { *basic-acl6-number* | **acl6-name** *acl6-name* }

undo ssm-policy

Copyright © Huawei Technologies Co., Ltd.

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.
acl6-name *acl6-name*	Specifies the name of a named ACL. **NOTE** **acl6-name** *acl6-name* can only be the name of a named advanced ACL.	The value is a string of 1 to 32 case-sensitive characters without spaces. The value must start with a letter (case sensitive).

Views

PIM-IPv6 view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

By default, the SSM group address range is FF3x::/32, where x cannot be 1 or 2. 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

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
```

Use a named ACL to set the PIM SSM group address range to FF31:0:8192::/96.

```
<Huawei> system-view
[Huawei] acl ipv6 name myacl6
[Huawei-acl6-adv-myacl6] rule permit ipv6 destination ff31:0:8192:: 96
[Huawei-acl6-adv-myacl6] quit
[Huawei] multicast ipv6 routing-enable
```

 Copyright © Huawei Technologies Co., Ltd.

```
[Huawei] pim-ipv6
[Huawei-pim6] ssm-policy acl6-name myacl6
```

Related Topics

10.2.42 ssm-mapping (MLD view)

10.4.76 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

Copyright © Huawei Technologies Co., Ltd.

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
```

Related Topics

10.4.60 pim ipv6 state-refresh-capable
10.4.77 state-refresh-rate-limit (IPv6)
10.4.78 state-refresh-ttl (IPv6)

10.4.77 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

Copyright © Huawei Technologies Co., Ltd.

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A router 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 router discards the received duplicate State-Refresh messages.
- After the State-Refresh timer times out, the router 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
```

Related Topics

10.4.60 pim ipv6 state-refresh-capable
10.4.76 state-refresh-interval (IPv6)
10.4.78 state-refresh-ttl (IPv6)

10.4.78 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*

Copyright © Huawei Technologies Co., Ltd.

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 router decreases the value of the TTL in the message by 1, and then sends the message to the downstream router 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
```

Related Topics

10.4.60 pim ipv6 state-refresh-capable

10.4.76 state-refresh-interval (IPv6)

10.4.77 state-refresh-rate-limit (IPv6)

Copyright © Huawei Technologies Co., Ltd.

10.4.79 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* | **acl6-name** *acl6-name*] [**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.
acl6-name *acl6-name*	Specifies the name of a Named ACL. **NOTE** **acl6-name** *acl6-name* can only be the name of a named advanced ACL.	The value is a string of 1 to 32 case-sensitive characters without spaces. The value must start with a letter (case sensitive).
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

 Copyright © Huawei Technologies Co., Ltd.

IPv6 multicast routing has been enabled 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.

The **static-rp** command and the **acl ipv6** command are used together.

- For the IPv6 numbered ACL, 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.
- For the IPv6 Named ACL, 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 **destination** parameter in the **rule** command. The filtering rule is effective only with the **destination** parameter and the time period specified by the **time-range** parameter.

Precautions

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 router 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
```

 Copyright © Huawei Technologies Co., Ltd.

Configure a Named ACL: the router with the address of FC00:0:0:1111::1111 functions as the static RP in the PIM-SM (IPv6) domain and serves groups defined by the ACL **myacl6**; preferential use of the static RP is enabled.

```
<Huawei> system-view
[Huawei] acl ipv6 name myacl6
[Huawei-acl6-adv-myacl6] rule permit ipv6 destination ff03::101 128
[Huawei-acl6-adv-myacl6] quit
[Huawei] multicast ipv6 routing-enable
[Huawei] pim-ipv6
[Huawei-pim6] static-rp fc00:0:0:1111::1111 acl6-name myacl6 preferred
```

Related Topics

10.4.28 display pim ipv6 rp-info

10.4.80 timer hello (IPv6)

Function

The **timer hello** command sets the interval at which the PIM router sends Hello messages.

The **undo timer hello** command restores the default interval.

By default, the interval at which the PIM router 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.

Copyright © Huawei Technologies Co., Ltd.

Prerequisites

IPv6 multicast routing has been enabled 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
```

Related Topics

10.4.63 pim ipv6 timer hello

10.4.33 hello-option holdtime (IPv6)

10.4.81 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.

Copyright © Huawei Technologies Co., Ltd.

Views

PIM-IPv6 view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The router sends join information to the upstream device, requesting the upstream device to forward multicast data. The router 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

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).

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
```

Related Topics

10.4.64 pim ipv6 timer join-prune

10.4.82 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.

Copyright © Huawei Technologies Co., Ltd.

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
```

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

10.4.74 spt-switch-threshold (IPv6)

10.5 MSDP Configuration Commands

NOTE

AR120 series do not support this function.

10.5.1 cache-sa-enable

Function

The **cache-sa-enable** command enables the SA cache function on a router. After receiving an SA message, the router 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 router.

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 router enabled with the SA cache function locally saves (S, G) information carried in the received SA messages. When the router receives requests for receiving multicast data, it directly obtains (S, G) information from the SA cache.

A router no long 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 router receives requests for receiving

Copyright © Huawei Technologies Co., Ltd.

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 according to whether the sending of SA Request messages is enabled.
  - 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 router in the public network instance.

```
<Huawei> system-view
[Huawei] multicast routing-enable
[Huawei] msdp
[Huawei-msdp] undo cache-sa-enable
```

Related Topics

10.5.12 msdp

10.7.28 multicast routing-enable

10.5.20 peer request-sa-enable

10.5.2 display default-parameter msdp

Function

The **display default-parameter msdp** command displays default configurations about MSDP.

Format

display default-parameter msdp

Copyright © Huawei Technologies Co., Ltd.

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 10-72 Description of the display default-parameter msdp command output

Item	Description
MSDP View Default Configurations	Default configurations in the MSDP view.
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.

Copyright © Huawei Technologies Co., Ltd.

Item	Description
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 router 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 router 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 router does not filter the received or forwarded SA messages. This parameter is configured using the **peer sa-policy** command.
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.

Related Topics

10.5.1 cache-sa-enable

Copyright © Huawei Technologies Co., Ltd.

10.5.10 encap-data-enable
10.5.14 peer connect-interface (MSDP)
10.5.15 peer description (MSDP)
10.5.18 peer minimum-ttl
10.5.20 peer request-sa-enable
10.5.23 peer sa-request-policy
10.5.22 peer sa-policy
10.5.30 timer retry

10.5.3 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 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-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.	-
down	Indicates the MSDP peers in Down state.	-
listen	Indicates the MSDP peers in Listen state.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
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.

Example

Display summary information about MSDP peers in the public network instance.

```
<Huawei> display msdp brief
MSDP Peer Brief Information of VPN-Instance: public net
 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 10-73 Description of the display msdp brief command output

Item	Description
MSDP Peer Brief Information of VPN-Instance	VPN instance to which summary information about MSDP peers corresponds.
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.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
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 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.

Related Topics

10.5.6 display msdp peer-status
10.5.27 reset msdp statistics

 Copyright © Huawei Technologies Co., Ltd.

10.5.4 display msdp control-message counters

Function

The **display msdp control-message counters** command displays statistics about MSDP messages.

Format

display msdp [**vpn-instance** *vpn-instance-name* | **all-instance**] **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
vpn-instance *vpn-instance-name*	Specifies a VPN instance. *vpn-instance-name* specifies the name of the VPN instance.	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-instance	Indicates all instances, including the public network instance and all VPN instances. If **vpn-instance** or **all-instance** is not specified, only statistics about the public network instance is displayed.	-
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.	-

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
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.	-
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 in the public network instance.

```
<Huawei> display msdp control-message counters peer 192.168.3.3
 VPN-Instance: public net
```

 Copyright © Huawei Technologies Co., Ltd.

```
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 10-74 Description of the display msdp control-message counters peer 192.168.3.3 command output

Item	Description
VPN-Instance	VPN instance in which MSDP message statistics are collected.
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.
Source-Active	Source-Active message.
Source-Active Request	Source-Active Request message.
Source-Active Response	Source-Active Response message.
KeepAlive	Keepalive message.
Notification	Notification message.
Traceroute Request	Traceroute Request message.
Traceroute Reply	Traceroute Reply message.
Data Packets	Data packets.
Unknown Type	Unknown type message.

Related Topics

10.5.6 display msdp peer-status
10.5.24 reset msdp control-message counters

10.5.5 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.

 Copyright © Huawei Technologies Co., Ltd.

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 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-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.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
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.

Example

Display statistics about invalid MSDP messages received by a device in the public network instance.

```
<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
------------------------------------------------------------------------------
```

 Copyright © Huawei Technologies Co., Ltd.

Table 10-75 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.
MSDP SA invalid packet	Invalid SA 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 RP addresses.
RP Loop	Messages whose RP addresses are local addresses.
MSDP SA Response invalid packet	Invalid SA Response messages.
MSDP SA Request invalid packet	Invalid SA 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 in the public network instance.

```
<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
------------------------------------------------------
```

 Copyright © Huawei Technologies Co., Ltd.

Table 10-76 Description of the display msdp invalid-packet 1 verbose command output

Item	Description
Detailed information of invalid packets	Details about invalid MSDP messages.
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.

Related Topics

10.7.23 multicast invalid-packet

10.5.6 display msdp peer-status

Function

The **display msdp peer-status** command displays the detailed information about MSDP peers.

Copyright © Huawei Technologies Co., Ltd.

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 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-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 MSPD 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.

 Copyright © Huawei Technologies Co., Ltd.

Example

Display the detailed information about the MSDP peer 10.110.11.11 in the public network instance.

```
<Huawei> display msdp peer-status 10.110.11.11
MSDP Peer Information of VPN-Instance: public net
  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
  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 10-77 Description of the display msdp peer-status command output

Item	Description
MSDP Peer Information of VPN-Instance	VPN instance to which MSDP peer information belongs.
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.

Copyright © Huawei Technologies Co., Ltd.

Item	Description
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.
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. By default, the SA messages received and forwarded are not filtered. The MSDP peer receives and forwards all the SA messages. The item is expressed by none.

Copyright © Huawei Technologies Co., Ltd.

Item	Description
Information about SA-Requests	• Policy to accept SA-Request messages: restricts the SA request messages received from an MSDP peer by the router. By default, the router 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 router to send SA request messages to a specified MSDP peer when the router receives a Join message. By default, when receiving a Join message, the router does not send the SA Request message to its MSDP peers, but waits for the next SA message. You can configure the router to send SA Request messages using the **peer request-sa-enable** command.
Minimum TTL to forward SA with encapsulated data	If the SA message received is encapsulated with the multicast data packet, the router 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 router 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.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
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.

Related Topics

10.5.3 display msdp brief
10.5.14 peer connect-interface (MSDP)
10.5.16 peer keychain (MSDP)
10.5.18 peer minimum-ttl
10.5.19 peer password (MSDP)
10.5.20 peer request-sa-enable
10.5.23 peer sa-request-policy
10.5.21 peer sa-cache-maximum
10.5.22 peer sa-policy
10.5.25 reset msdp peer

10.5.7 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*

Copyright © Huawei Technologies Co., Ltd.

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 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-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 SA messages from being forwarded circularly between MSDP peers, MSDP performs RPF check on received SA messages to control the incoming SA messages. SA messages that do not comply with RPF rules are discarded.

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 works improperly, this command helps you locate the faulty node.

Precautions

A device does not perform the RPF peer check 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.

 Copyright © Huawei Technologies Co., Ltd.

- 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. It is a member of a 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 in the public network instance.

```
<Huawei> display msdp rpf-peer original-rp 192.168.4.5
MSDP RPF peer information of VPN-Instance: public net
 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 10-78 Description of the display msdp rpf-peer original-rp command output

Item	Description
MSDP RPF peer information of VPN-Instance: public net	VPN instance to which MSDP peer information belongs.
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.
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.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
RPF route type	RPF route type: • mbgp: MBGP route. • unicast(bgp): BGP route • multicast(static): static multicast route. • unicast: IGP route (unicast route).

10.5.8 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 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-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.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
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

After 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 has been enabled. By default, SA cache is enabled.

Example

Display (S, G) entries in the SA cache in the public network instance.

```
<Huawei> display msdp sa-cache
MSDP Source-Active Cache Information of VPN-Instance: public net
 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 10-79 Description of the display msdp sa-cache command output

Item	Description
MSDP Source-Active Cache Information of VPN-Instance	MSDP SA cache in the public network instance.

Copyright © Huawei Technologies Co., Ltd.

Item	Description
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.
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.
Expires	Time when the (S, G) entry in the cache times out.

Related Topics

10.5.1 cache-sa-enable

10.5.26 reset msdp sa-cache

10.5.9 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*]

Copyright © Huawei Technologies Co., Ltd.

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 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-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

After 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. By default, the SA cache function is enabled.

Example

Display the number of (S, G) entries in the SA cache in the public network instance.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> display msdp sa-count
MSDP Source-Active Count Information of VPN-Instance: public net
  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 10-80 Description of the display msdp sa-count command output

Item	Description
MSDP Source-Active Count Information of VPN-Instance	VPN instance to which the SA cache information belongs.
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.
Number of source	Number of sources in the AS.
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.

Related Topics

10.5.1 cache-sa-enable

10.5.21 peer sa-cache-maximum

10.5.10 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.

 Copyright © Huawei Technologies Co., Ltd.

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 used on the RP at the source side, 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 used on the MSDP peer, the router 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
```

Related Topics

10.5.12 msdp

10.7.28 multicast routing-enable

 Copyright © Huawei Technologies Co., Ltd.

10.5.11 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* | *acl-name* }]

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.
acl-name	Specifies the name of a named ACL. **NOTE** *acl-name* can only be the name of a named advanced ACL.	The value is a string of 1 to 32 case-sensitive characters without spaces. The value must start with a letter (case sensitive).

Views

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

Default Level

2: Configuration level

Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

Usage Scenario

When the **import-source** command is used, MSDP filters advertised (S, G) forwarding entries based on source addresses when creating SA messages. Therefore, when creating SA messages, MSDP can control the transmission of information about multicast sources.

You can also run the **peer sa-policy** command to filter the SA messages to be forwarded.

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 in the public network instance. 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
```

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 in the public network instance using a named ACL.

```
<Huawei> system-view
[Huawei] acl name myacl
[Huawei-acl-adv-myacl] rule permit ip source 10.10.0.0 0.0.255.255 destination 225.1.0.0 0.0.255.255
[Huawei-acl-adv-myacl] quit
[Huawei] multicast routing-enable
[Huawei] msdp
[Huawei-msdp] import-source acl myacl
```

Related Topics

10.5.12 msdp

10.7.28 multicast routing-enable

Copyright © Huawei Technologies Co., Ltd.

10.5.22 peer sa-policy

10.5.12 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 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

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To configure MSDP in the public network instance or the VPN instance, 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 in the public network instance view or VPN instance view.

Configuration Impact

Running the **undo msdp** command interrupts MSDP services. Therefore, use this command with caution.

 Copyright © Huawei Technologies Co., Ltd.

Example

Enable MSDP in the public network instance and enter the MSDP view of the public network instance.

```
<Huawei> system-view
[Huawei] multicast routing-enable
[Huawei] msdp
[Huawei-msdp]
```

Enable MSDP in the VPN instance **mytest** and enter the MSDP view of the VPN instance.

```
<Huawei> system-view
[Huawei] ip vpn-instance mytest
[Huawei-vpn-instance-mytest] route-distinguisher 100:1
[Huawei-vpn-instance-mytest-af-ipv4] multicast routing-enable
[Huawei-vpn-instance-mytest-af-ipv4] quit
[Huawei-vpn-instance-mytest] quit
[Huawei] msdp vpn-instance mytest
[Huawei-msdp-mytest]
```

Related Topics

10.7.28 multicast routing-enable

10.5.13 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.	The routes on multicast tunnel interfaces (MTIs) are not advertised to private networks, so do not use the addresses of MTIs as the logical RP addresses.

Views

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

Copyright © Huawei Technologies Co., Ltd.

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 address 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 GE1/0/0 as the logical RP for the SA message in the public network instance.

```
<Huawei> system-view
[Huawei] multicast routing-enable
[Huawei] msdp
[Huawei-msdp] originating-rp gigabitethernet 1/0/0
```

Related Topics

10.5.12 msdp

10.7.28 multicast routing-enable

10.5.14 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*

 Copyright © Huawei Technologies Co., Ltd.

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 router uses the primary address of the interface as the source IP address to set up the TCP connection with the remote MSDP peer.	The routes on multicast tunnel interfaces (MTIs) are not advertised to private networks, so do not use the addresses of MTIs as the logical RP addresses.

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 router.

- 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 prompts 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.

 Copyright © Huawei Technologies Co., Ltd.

Example

Configure IP address 10.10.7.6 for the remote MSDP peer and specify GE1/0/0 as the local interface in the public network instance.

```
<Huawei> system-view
[Huawei] multicast routing-enable
[Huawei] msdp
[Huawei-msdp] peer 10.10.7.6 connect-interface gigabitethernet 1/0/0
```

Related Topics

10.5.12 msdp

10.7.28 multicast routing-enable

10.5.29 static-rpf-peer

10.5.15 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

Copyright © Huawei Technologies Co., Ltd.

If multiple MSDP peers are configured on the network, the MSDP peers cannot be easily distinguished only based on IP addresses. The administrator can distinguish the MSDP peers by setting the description texts for them.

Prerequisites

MSDP peers have been configured using the **peer connect-interface (MSDP)** command.

Example

Add an description **ClientA** for the MSDP peer with the IP address being 10.10.7.6 in the public network instance.

```
<Huawei> system-view
[Huawei] multicast routing-enable
[Huawei] msdp
[Huawei-msdp] peer 10.10.7.6 connect-interface gigabitethernet 1/0/0
[Huawei-msdp] peer 10.10.7.6 description ClientA
```

Related Topics

10.5.6 display msdp peer-status

10.5.12 msdp

10.7.28 multicast routing-enable

10.5.14 peer connect-interface (MSDP)

10.5.16 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.

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.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
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 improves security on TCP connections between MSDP peers. Keychain authentication supports multiple algorithms. Compared to MD5 authentication, keychain authentication applies to networks 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 router and the peer 10.1.1.2 and configure a keychain named **huawei** in the public network instance.

```
<Huawei> system-view
[Huawei] keychain huawei mode absolute
[Huawei-keychain-huawei] key-id 1
[Huawei-keychain-huawei-keyid-1] algorithm sha-256
[Huawei-keychain-huawei-keyid-1] key-string cipher Huawei@1234
[Huawei-keychain-huawei-keyid-1] quit
[Huawei-keychain-huawei] quit
[Huawei] multicast routing-enable
```

 Copyright © Huawei Technologies Co., Ltd.

```
[Huawei] msdp
[Huawei-msdp] peer 10.1.1.2 connect-interface gigabitethernet 1/0/0
[Huawei-msdp] peer 10.1.1.2 keychain huawei
```

Related Topics

19.20.4 keychain
10.5.12 msdp
10.7.28 multicast routing-enable
10.5.19 peer password (MSDP)

10.5.17 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 the RPF check on each received SA messages, which brings a heavy load to the system.

 Copyright © Huawei Technologies Co., Ltd.

Configuring multiple MSDP peers to join the same mesh group can reduce the number of SA messages transmitted between these MSDP peers and release the load of 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 configured to join different mesh groups for 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** in the public network instance

```
<Huawei> system-view
[Huawei] multicast routing-enable
[Huawei] msdp
[Huawei-msdp] peer 10.10.7.6 connect-interface gigabitethernet 1/0/0
[Huawei-msdp] peer 10.10.7.6 mesh-group Group1
```

Related Topics

10.5.12 msdp

10.7.28 multicast routing-enable

10.5.14 peer connect-interface (MSDP)

10.5.18 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.

Copyright © Huawei Technologies Co., Ltd.

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 is used to limit the forwarding of SA messages with multicast data packets encapsulated.

After the TTL threshold is set for a specified peer, the router checks the TTL of a multicast data packet before encapsulating the multicast data packet in an SA message. Only the multicast data packet with the TTL being greater than the threshold is encapsulated in an SA message and sent to the peer of the router.

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 in the public network instance.

```
<Huawei> system-view
[Huawei] multicast routing-enable
[Huawei] msdp
[Huawei-msdp] peer 10.10.10.1 connect-interface gigabitethernet 1/0/0
[Huawei-msdp] peer 10.10.10.1 minimum-ttl 10
```

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

10.5.6 display msdp peer-status
10.5.12 msdp
10.7.28 multicast routing-enable
10.5.14 peer connect-interface (MSDP)

10.5.19 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.

Copyright © Huawei Technologies Co., Ltd.

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 router and the peer 10.1.1.1 and set the authentication password to **Huawei@1234** in the cipher text.

```
<Huawei> system-view
[Huawei] multicast routing-enable
[Huawei] msdp
```

 Copyright © Huawei Technologies Co., Ltd.

```
[Huawei-msdp] peer 10.1.1.1 connect-interface gigabitethernet 1/0/0
[Huawei-msdp] peer 10.1.1.1 password cipher Huawei@1234
```

Related Topics

10.5.12 msdp

10.7.28 multicast routing-enable

10.5.14 peer connect-interface (MSDP)

10.5.16 peer keychain (MSDP)

10.5.20 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 router does not send an SA Request messages 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.

Copyright © Huawei Technologies Co., Ltd.

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. Then after 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 router, disable SA cache on the local router and enable SA cache on the peer of the specified *peer-address*. Therefore, when the local router has new receiving requests, it can actively send SA Request messages to the peer and receive responses from the peer.

Example

Configure the router to send SA Request messages to the MSDP peer 10.10.7.6 when receiving a new Join message in the public network instance.

```
<Huawei> system-view
[Huawei] multicast routing-enable
[Huawei] msdp
[Huawei-msdp] peer 10.10.7.6 connect-interface gigabitethernet 1/0/0
[Huawei-msdp] peer 10.10.7.6 request-sa-enable
```

Related Topics

10.5.1 cache-sa-enable

10.5.6 display msdp peer-status

10.5.12 msdp

10.7.28 multicast routing-enable

10.5.14 peer connect-interface (MSDP)

10.5.21 peer sa-cache-maximum

Function

The **peer sa-cache-maximum** command sets the maximum number of (S, G) entries that are learned from MSDP peers and cached in the SA cache.

The **undo peer sa-cache-maximum** command restores the maximum number of (S, G) entries that are learned from MSDP peers and cached in the SA cache to the default value.

By default, the maximum number of (S, G) entries in the SA cache is 1638.

Copyright © Huawei Technologies Co., Ltd.

Format

peer *peer-address* **sa-cache-maximum** *sa-limit*

undo peer *peer-address* **sa-cache-maximum**

Parameters

Parameter	Description	Value
peer-address	Specifies the IP address of an MSDP peer.	The address is in dotted decimal notation.
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

It is recommended that you perform this configuration on all MSDP peers on a 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 router, the maximum number of (S, G) entries in SA-Cache is 1638.

For the (S, G) entries of a single peer, the following situations occur:

- If the number of (S, G) entries is not set or exceeds 1638, the maximum number of (S, G) entries in the SA cache can be set to 1638.
- If the number of (S, G) entries is smaller than 1638, 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 learned from MSDP peer 10.10.7.6 in the public network instance and cached in the SA cache to 100.

Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> system-view
[Huawei] multicast routing-enable
[Huawei] msdp
[Huawei-msdp] peer 10.10.7.6 connect-interface gigabitethernet 1/0/0
[Huawei-msdp] cache-sa-enable
[Huawei-msdp] peer 10.10.7.6 sa-cache-maximum 100
```

Related Topics

10.5.1 cache-sa-enable
10.5.9 display msdp sa-count
10.5.6 display msdp peer-status
10.5.3 display msdp brief
10.5.12 msdp
10.7.28 multicast routing-enable
10.5.14 peer connect-interface (MSDP)

10.5.22 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, the SA messages received and forwarded are not filtered. That is, all (S, G) entries are received and forwarded to MSDP peers.

Format

peer *peer-address* **sa-policy** { **import** | **export** } [**acl** { *advanced-acl-number* | *acl-name* }]

undo peer *peer-address* **sa-policy** { **import** | **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. After the **import** parameter is used, when an SA message reaches the local router from the specified peer, the local router filters the message using the import policy to determine whether to process the SA message.	-

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
export	Forwards the SA messages to a specified MSDP peer. After the **export** parameter is used, a router filters an SA message using the export policy to determine whether to forward the SA message.	-
acl	Indicates the ACL that defines the import or export policy. • In the import policy, if this parameter is not configured, the router does not receive SA messages from any MSDP peer; if this parameter is configured, the router receives SA messages that carry the (S, G) entry only from a specified MSDP peer. • In the export policy, if this parameter is not configured, the router does not forward SA messages from any MSDP peer; if this parameter is configured, the router forwards SA messages that carry the (S, G) entry only to a specified MSDP peer.	-
advanced-acl-number	Specifies the number of the advanced ACL.	The number is an integer that ranges from 3000 to 3999.
acl-name	Specifies the name of a named ACL. **NOTE** *acl-name* can only be the name of a named advanced ACL.	The value is a string of 1 to 32 case-sensitive characters without spaces. The value must start with a letter (case sensitive).

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 used, MSDP can filter (S, G) forwarding entries carried in the SA message received from or forwarded to specified MSDP

 Copyright © Huawei Technologies Co., Ltd.

peers according to multicast sources. The transmission of multicast source information is controlled when SA messages are received and forwarded.

Besides controlling the transmission of SA messages, you can run the **import-source** command on the peer nearest to the source to control the creation of SA messages.

Prerequisites

MSDP peers have been configured using the **peer connect-interface (MSDP)** command.

Example

Configure the router to forward only the SA messages that pass the ACL3100 filtering to peer 10.10.7.6 in the public network instance.

```
<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 gigabitethernet 1/0/0
[Huawei-msdp] peer 10.10.7.6 sa-policy export acl 3100
```

Configure a named ACL so that the router forwards SA messages only to peer 10.10.7.6 in the public network instance.

```
<Huawei> system-view
[Huawei] acl name myacl
[Huawei-acl-adv-myacl] rule permit ip source 10.15.0.0 0.0.255.255 destination 225.1.0.0 0.0.255.255
[Huawei-acl-adv-myacl] quit
[Huawei] msdp
[Huawei-msdp] peer 10.10.7.6 connect-interface gigabitethernet 1/0/0
[Huawei-msdp] peer 10.10.7.6 sa-policy export acl myacl
```

Related Topics

10.5.6 display msdp peer-status

10.5.11 import-source

10.5.12 msdp

10.7.28 multicast routing-enable

10.5.14 peer connect-interface (MSDP)

10.5.23 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 router responds to the SA message immediately.

The **undo peer sa-request-policy** command restores the default configuration.

By default, the router responds to all SA request messages sent by all MSDP peers.

Copyright © Huawei Technologies Co., Ltd.

Format

peer *peer-address* **sa-request-policy** [**acl** { *basic-acl-number* | *acl-name* }]

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.
acl-name	Specifies the name of a named ACL. **NOTE** *acl-name* can only be the name of a named advanced ACL.	The value is a string of 1 to 32 case-sensitive characters without spaces. The value must start with a letter (case sensitive).

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 router 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.

Copyright © Huawei Technologies Co., Ltd.

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.
- In the advanced ACL view of a named ACL, 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 with the time period specified by the **time-range** parameter.

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 in the public network instance.

```
<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 gigabitethernet 1/0/0
[Huawei-msdp] peer 10.58.6.5 sa-request-policy acl 2001
```

Configure a named 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 in the public network instance.

```
<Huawei> system-view
[Huawei] acl name myacl
[Huawei-acl-adv-myacl] rule permit ip destination 225.1.1.0 0.0.0.255
[Huawei-acl-adv-myacl] quit
[Huawei] msdp
[Huawei-msdp] peer 10.58.6.5 connect-interface gigabitethernet 1/0/0
[Huawei-msdp] peer 10.58.6.5 sa-request-policy acl myacl
```

Related Topics

10.5.6 display msdp peer-status

10.5.12 msdp

10.7.28 multicast routing-enable

10.5.14 peer connect-interface (MSDP)

10.5.24 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*]

Copyright © Huawei Technologies Co., Ltd.

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 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-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 in the public network instance.

```
<Huawei> reset msdp control-message counters peer 10.3.3.3
```

Related Topics

10.5.4 display msdp control-message counters

10.5.6 display msdp peer-status

Copyright © Huawei Technologies Co., Ltd.

10.5.25 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 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-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 or clear statistics about the specified MSDP peer, run the **reset msdp peer** command.

Copyright © Huawei Technologies Co., Ltd.

Use the **reset msdp statistics** command to clear the statistics about an MSDP peer without resetting the MSDP peer.

Configuration Impact

NOTICE

After this command is run, 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 fails. 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 in the public network instance.

```
<Huawei> reset msdp peer 10.10.7.6
```

Related Topics

10.5.6 display msdp peer-status

10.5.27 reset msdp statistics

10.5.26 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 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.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
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 in the public network instance.

```
<Huawei> reset msdp sa-cache 225.5.4.3
```

Related Topics

10.5.1 cache-sa-enable

10.5.8 display msdp sa-cache

Copyright © Huawei Technologies Co., Ltd.

10.5.27 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 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-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.

Copyright © Huawei Technologies Co., Ltd.

Example

Clear the statistics of MSDP peer 10.10.7.6 in the public network instance.

```
<Huawei> reset msdp statistics 10.10.7.6
```

Related Topics

10.5.3 display msdp brief
10.5.25 reset msdp peer

10.5.28 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

Copyright © Huawei Technologies Co., Ltd.

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. You do not need to run the **peer connect-interface (MSDP)** command to reconfigure the MSDP peer.

Example

Close MSDP peer 10.10.7.6 in the public network instance.

```
<Huawei> system-view
[Huawei] multicast routing-enable
[Huawei] msdp
[Huawei-msdp] peer 10.10.7.6 connect-interface gigabitethernet 1/0/0
[Huawei-msdp] shutdown 10.10.7.6
```

Related Topics

10.5.3 display msdp brief

10.5.6 display msdp peer-status

10.5.12 msdp

10.7.28 multicast routing-enable

10.5.14 peer connect-interface (MSDP)

10.5.29 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 are free from the RPF check.

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.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
rp-policy *ip-prefix-name*	Specifies the filtering policy based on RP addresses. The filtering policy 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 message that does not comply with the RPF rules are discarded.

To protect the SA messages transmitted between MSDP peers from being discarded because of RPF rules 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 router and a specified RPF peer using the **peer connect-interface (MSDP)** command.

Configuration Impact

You can specify multiple remote static RPF peers for the router using the **static-rpf-peer** *peer-address* command repeatedly.

Precautions

When you specify multiple static RPF peers for the router, 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 router, the local router filters the SA messages according to specified **rp-policy** on the peers, and receives only the SA messages passing the filtering.
- None of the peers is configured with **rp-policy**

  The local router receives all the SA messages from the static RPF peers in the active state.

 Copyright © Huawei Technologies Co., Ltd.

Example

Configure 192.168.3.2 as a static RPF peer, with the source RP address range of 192.168.0.0/16 in the public network instance.

```
<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 gigabitethernet 1/0/0
[Huawei-msdp] static-rpf-peer 192.168.3.2 rp-policy list-df
```

Related Topics

10.5.6 display msdp peer-status

9.9.47 ip ip-prefix

10.5.12 msdp

10.7.28 multicast routing-enable

10.5.14 peer connect-interface (MSDP)

10.5.30 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

Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

Usage Scenario

The TCP connection needs to be set up between the MSDP peers. MSDP requires the peer with the larger IP address to listen at the port 639, and the peer with the smaller IP address to start a connection. If the connection fails, the peer restarts the connection after a period of time. Such a period of time is called "interval retrying to set up an MSDP peer relationship".

You need to establish a TCP connection between MSDP peers when an MSDP peer is created, the closed MSDP peer connection is restarted, or the faulty MSDP peer tries to restore the 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 in the public network instance.

```
<Huawei> system-view
[Huawei] multicast routing-enable
[Huawei] msdp
[Huawei-msdp] timer retry 60
```

Related Topics

10.5.6 display msdp peer-status

10.5.12 msdp

10.7.28 multicast routing-enable

10.6 Multicast VPN (IPv4) Configuration Commands in Rosen Mode

NOTE

The feature is just for beta test, and is not for commercial use. If the feature is required in the test, contact technical support personnel.

10.6.1 auto-discovery

Function

The **auto-discovery** command configures the auto-discovery (A-D) mode for the multicast VPN, ensuring the transmission of multicast VPN services on the public network tunnel which is based on the Protocol Independent Multicast-Source-Specific Multicast (PIM-SSM) multicast distribution tree (MDT), and associates an inbound multicast route-policy with the IPv4 address family of the current VPN instance.

Copyright © Huawei Technologies Co., Ltd.

The **undo auto-discovery** command deletes the configurations of the A-D mode for the multicast VPN and removes the association between the inbound multicast route-policy and the IPv4 address family of the current VPN instance.

By default, the A-D mode for the multicast VPN is not configured and the IPv4 address family of the current VPN instance is not associated with an inbound multicast route-policy.

Format

auto-discovery { **mdt** | **mvpn** } [**import route-policy** *route-policy-name*]

undo auto-discovery

Parameters

Parameter	Description	Value
mdt	Specifies that the multicast VPN adopts the MDT-Subsequent Address Family Identifier (SAFI) A-D mode.	-
mvpn	Specifies that the multicast VPN adopts the MCAST-VPN SAFI A-D mode.	-
route-policy *route-policy-name*	Specifies the inbound multicast route-policy to associate 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 mechanism of implementing the multicast VPN is that all Provider Edges (PEs) on the network know information about the Rendezvous Point (RP); in this manner, the PIM-SM MDT is established on the public network to transmit multicast VPN services. 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.

 Copyright © Huawei Technologies Co., Ltd.

To solve this problem, in an autonomous system (AS), you can configure the BGP A-D mode to enable the automatic discovery of the PE information about PEs in the same VPN. In this manner, multicast VPN services can be transmitted on 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: defines a new address family 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 RD. If the RDs are the same, it indicates the remote PE is in the same VPN with 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: defines a new address family 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 additional extensions, and carries more multicast VPN attributes and information for establishing the public network tunnel. Therefore, the MCAST-VPN SAFI A-D mode is applied to the next-generation multicast VPN.

Prerequisites

The **multicast routing-enable** command has been run 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 an A-D address family in the BGP view so that the corresponding 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, you cannot implement the A-D mode.

NOTE

This command is applied to the single-AS scenario, with no RP configured on the public network.

In the same VPN enabled with the IPv4 address family, only one A-D mode can be adopted. Different VPNs enabled with the IPv4 address family on the same PE can adopt different A-D modes. In this case, you need to enable two kinds of A-D address families in the BGP view, and then the specific A-D mode is adopted by each VPN 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. When the Share-Group address is in the Any-Source Multicast (ASM) address range, or the PIM-DM protocol is adopted on the public network, multicast VPN traffic can still be transmitted along the multicast tunnel in PIM-SM mode or in PIM-DM mode on the public network.

 Copyright © Huawei Technologies Co., Ltd.

Example

Configure the MDT-SAFI A-D mode for vpn1 enabled with the IPv4 address family, implementing the transmission of multicast VPN services along the public network tunnel (PIM-SSM MDT) in vpn1.

```
<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-instatnce 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
```

Related Topics

10.6.5 display multicast-domain vpn-instance share-group

9.8.87 ipv4-family

10.6.2 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.

 Copyright © Huawei Technologies Co., Ltd.

```
<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 10-81 Description of the **display default-parameter mvpn** command output

Item	Description
MVPN Instance View Default Configurations	Indicates the default configurations in the MVPN instance view.
Multicast-domain switch-delay	Indicates the delay in switching from the share-multicast distribution tree (MDT) to the switch-MDT.
Multicast-domain switch threshold	Indicates the threshold of the multicast packet rate that can trigger the switch to the switch-MDT.
Multicast-domain holddown-time	Indicates the delay in switching from the switch-MDT to the share-MDT.
Multicast-domain log switch-group-reuse	Indicates whether recording logs about switch-group address reuse is configured.
Multicast-domain share-group	Indicates whether the share-group address is configured and whether the Multicast Tunnel Interface (MTI) is bound to a VPN instance.
Multicast-domain switch-group-pool	Indicates whether the range of the switch-MDT switch-group-pool and the switch condition are configured.
Multicast-domain auto-discovery	Indicates whether the auto-discovery (A-D) mode is configured for the VPN.
Multicast-domain switch-without-register	Indicates whether the source Provider Edge (PE) sends the null Register message to the Rendezvous Point (RP) to establish the shortest path tree (SPT) on the public network before the Switch-Group address is used to encapsulate VPN data.
Multicast extranet select-rpf rule	Indicates whether the multicast routing policy configured for a VPN is configured.

 Copyright © Huawei Technologies Co., Ltd.

10.6.3 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. *vpn-instance-name* specifies the 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

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 set the **vpn-instance** *vpn-instance-name* parameter so as to view statistics about sent and received MDT switch messages in a specified VPN instance.

Example

Displays statistics about sent and received MDT switch messages in VPN instance **red**.

```
<Huawei> display multicast-domain vpn-instance red control-message counters
VPN-Inastance red:
 Message Type     Received        Sent          Invalid
 Switch           5000            0             5000
```

 Copyright © Huawei Technologies Co., Ltd.

Table 10-82 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. The value can only be: Switch: MDT switch message
Received	Number of received messages
Sent	Number of sent messages
Invalid	Number of received invalid messages

10.6.4 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. *vpn-instance-name* specifies the VPN instance name.	The value is a string of case-sensitive characters.
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.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
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 a shortest path tree (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.

You can run the following related commands to view information about specific invalid MDT switch messages:

- Run the **display multicast-domain vpn-instance** *vpn-instance-name* **invalid-packet** command to view statistics about invalid MDT switch messages received in a specified VPN instance.
- Run the **display multicast-domain invalid-packet** *packet-number* **verbose** command to view details of invalid MDT switch messages recently received. Currently, details of a maximum of 10 invalid MDT switch messages can be displayed.

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
------------------------------------------------------------------------------
```

 Copyright © Huawei Technologies Co., Ltd.

Table 10-83 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          :  10.10.10.10
Time               :  2010-6-1 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 10-84 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)
Interface	Interface receiving the invalid MDT switch message

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
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

Related Topics

10.7.23 multicast invalid-packet

10.6.5 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 in a multicast domain (MD).

Format

display multicast-domain vpn-instance *vpn-instance-name* **share-group** [**local** | **remote**]

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Specifies the name of a VPN instance.	The name is a case-sensitive character string.
local	Indicates the locally configured share-group address.	-

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
remote	Indicates the share-group address learned through BGP Update packets.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

In an autonomous system (AS), BGP Auto-Discovery (BGP A-D) ensures the automatic discovery of peers in a multicast VPN. In this manner, a Protocol Independent Multicast-Source-Specific Multicast (PIM-SSM) multicast distribution tree (MDT) can be directly established on the public network to transmit multicast VPN services. The **display multicast-domain vpn-instance share-group** command displays information about the Share-Group of the remote peer, peer IP address, and tunnel type, which facilitates you to determine whether the multicast tunnel is correctly established to forward multicast services.

When **display multicast-domain vpn-instance share-group** command is used, the following situations occur:

- If **local** is specified, only the information of the share-group configured locally is displayed.
- If **remote** is specified, the share-group information learned through the BGP Update packets is displayed.
- If both **local** and **remote** are not specified, information of all share-groups is displayed.

The share-group information learned through BGP Update packets is displayed in an ascending order of share-groups. If the share-groups are the same, the information is displayed in an ascending order of peer addresses.

Example

Display the share-group information of a specified VPN instance in an MD.

```
<Huawei> display multicast-domain vpn-instance BLUE share-group
MD local share-group information for VPN-Instance: BLUE
  Share-group: 232.2.2.0
  MTunnel address: 3.3.3.3
MD remote share-group information for VPN-Instance: BLUE
  Share-group     Peer-address    Tunnel-type
  232.2.2.0       1.1.1.1         PIM SSM
```

 Copyright © Huawei Technologies Co., Ltd.

Table 10-85 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	Configured share-group address on the local device
MTunnel address	Configured IP address of the MTI bound to the share-group on the local device
MD remote share-group information for VPN-Instance	VPN instance to which remote share-group information in the multicast domain belongs
Share-group	Share-group address of the remote provider edge (PE)
Peer-address	IP address of the remote PE
Tunnel-type	Tunnel type, including: • PIM SM: indicates that the Share-Group address of the remote PE is in the any-source multicast (ASM) address range. • PIM SSM: indicates that the Share-Group address of the remote PE is in the source-specific multicast (SSM) address range. **NOTE** The Tunnel-type field is displayed only if the remote PE is configured with the MCAST-SAFI A-D mode.

Related Topics

10.6.12 multicast-domain share-group

10.6.6 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**

Copyright © Huawei Technologies Co., Ltd.

display multicast-domain vpn-instance *vpn-instance-name* **switch-group receive** [**active** | **group** *group-address* | **sender** *source-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*	Specifies a VPN instance. *vpn-instance-name* specifies the name of the VPN instance.	The name is a string of 1 to 31 characters.
active	Displays the received Switch-Group that joins the Switch-multicast distribution tree (MDT).	-
brief	Displays brief information about the received Switch-Group.	-
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 address is in dotted decimal notation and ranges from 224.0.0.0 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 address 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 address 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 VPN multicast source address.	The mask 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 address 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.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
group-mask	Specifies the mask of VPN multicast group address.	The mask is in dotted decimal notation.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Use the **display multicast-domain vpn-instance switch-group receive** command is run to display the Switch-Group information received by the local router:

- Each VPN instance corresponds to a multicast domain (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, the brief information of all Switch-Groups is displayed in an ascending order of the Switch-Group address.
- If **active** is specified, only the information of the Switch-Group that joins the Switch-Group is displayed in an ascending order of the VPN (S, G).
- If **group** is specified, only the Switch-Group information related to the multicast group of the public network is displayed.
- If the **sender** is specified, only the Switch-Group information related to the multicast source of the public network is displayed.
- If *vpn-source-address* is specified, only information about the Switch-Group related to a specified VPN multicast source is displayed.
- If *vpn-group-address* is specified, only information about the Switch-Group related to a specified VPN multicast group is displayed.

Example

Display Switch-Group information received by a specified VPN instance 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:  172.100.1.1 active count: 8
    (192.6.1.5, 239.1.1.1)
    Up time: 01:20:20  expire time: 00:03:10  active
    (192.6.1.5, 239.1.1.158)
    Up time: 01:20:20  expire time: 00:03:10  active
    (192.6.1.5, 239.1.2.12)
    Up time: 01:20:20  expire time: 00:03:10  active
    (192.6.1.5, 239.1.2.197)
    Up time: 01:20:20  expire time: 00:03:10  active
    (192.6.1.5, 239.1.3.62)
    Up time: 01:20:20  expire time: 00:03:10  active
    (192.6.1.2, 225.1.1.109)
    Up time: 01:20:20  expire time: 00:03:10  active
```

 Copyright © Huawei Technologies Co., Ltd.

```
  (192.6.1.2, 225.1.4.80)
  Up time: 01:20:20  expire time: 00:03:10  active
  (192.6.1.2, 225.1.4.173)
  Up time: 01:20:20  expire time: 00:03:10  active
<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 10-86 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
expire time	Timeout period of switching messages in which the VPN multicast (S, G) entry are referenced by the Switch-group

Related Topics

10.6.7 display multicast-domain vpn-instance switch-group send

10.6.7 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 a multicast domain (MD).

Format

display multicast-domain vpn-instance *vpn-instance-name* **switch-group send** [**group** *group-address* | **reuse** *interval* | *vpn-source-address* [**mask** { *source-mask-length* | *source-mask* }] | *vpn-group-address* [**mask** { *group-mask-length* | *group-mask* }]] *

Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Specifies the VPN instance. *vpn-instance-name* specifies the name of the VPN instance.	The name is a string of 1 to 31 characters.
group *group-address*	Displays the Switch-Group information related to a multicast group G. The *group-address* indicates multicast group address.	The address is in dotted decimal notation format. The address ranges from 224.0.0.0 to 239.255.255.255.
reuse *interval*	Displays Switch-Group information that is reused by an MD in the specified period. The *interval* indicates the specified period.	The value of the interval is an integer that ranges from 1 to 2147483647 seconds.
vpn-source-address	Displays the Switch-Group information related to the specified VPN multicast source.	The address is in dotted decimal notation format.
mask	Indicates the mask of VPN multicast group or source address.	-
source-mask-length	Specifies the mask length of a VPN multicast source address.	The value is an integer that ranges from 0 to 32.
source-mask	Specifies the mask of a VPN multicast source address.	The address is in dotted decimal notation.
vpn-group-address	Displays the Switch-Group information related to the specified VPN multicast group G.	The address is in dotted decimal notation and ranges from 224.0.0.0 to 239.255.255.255.
group-mask-length	Specifies the mask length of a VPN multicast group address.	The value is an integer that ranges from 4 to 32.
group-mask	Specifies the mask of a VPN multicast group address.	The address mask is in dotted decimal notation.

Views

All views

Default Level

1: Monitoring level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

Use the **display multicast-domain vpn-instance switch-group send** command to display the Switch-Group information sent by the local Huawei:

- Each VPN instance corresponds to an MD. *vpn-instance-name* specifies the 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 an 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 an ascending order of Switch-Group address.

Example

Display the Switch-Group information sent by a specified VPN instance 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
    (192.168.1.5, 239.1.1.1)              switch time: 00:00:21
    (192.168.1.5, 239.1.1.158)             switch time: 00:00:21
    (192.168.1.5, 239.1.2.50)              switch time: 00:00:05
  226.1.1.1 reference_count: 3
    (192.168.1.2, 225.1.1.1)              switch time: 00:00:21
    (192.168.1.2, 225.1.2.50)              switch time: 00:00:05
    (192.168.1.5, 239.1.1.159)             switch time: 00:00:21
<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 10-87 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: 3	Number of VPN multicast groups referenced by the Switch-group sent
switch time	Switching time of the VPN multicast (S, G) entry referenced by the Switch-group
226.1.1.0 reuse_count: 1	Number of times of reusing the Switch-group sent in the specified period

Related Topics

10.6.6 display multicast-domain vpn-instance switch-group receive

 Copyright © Huawei Technologies Co., Ltd.

10.6.8 mtu (MTI view)

Function

The **mtu** command sets the MTU for an MTI.

The **undo mtu** command restores the default MTU of an MTI.

By default, the MTU of an MTI is 1472 bytes.

Format

mtu *mti-mtu*

undo mtu

Parameters

Parameter	Description	Value
mti-mtu	Specifies the MTU value of an MTI.	The value is an integer that ranges from 128 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.

To enable an MTI to fragment a VPN multicast packet before performing GRE encapsulation, run the **mtu** command to set a smaller MTU for the MTI. This method reduces unnecessary fragmentation on the public network and packet reassembly, improving packet transmission efficiency.

Configuration Impact

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.

 Copyright © Huawei Technologies Co., Ltd.

Example

Set the MTU of MTunnel 10 to 1400.

```
<Huawei> system-view
[Huawei] interface mtunnel 10
[Huawei-MTunnel10] mtu 1400
```

10.6.9 multicast extranet select-rpf

Function

The **multicast extranet select-rpf** command configures a multicast routing policy, setting the upstream of the Reverse Path Forwarding (RPF) route selected by the PIM entry corresponding to a multicast group address to another VPN instance or the public network instance.

The **undo multicast extranet select-rpf** command deletes the multicast routing policy configured for a VPN.

By default, no multicast routing policy is configured for a VPN.

Format

multicast extranet select-rpf { **vpn-instance** *vpn-instance-name* | **public** } **group** *group-address* { *group-mask* | *group-mask-length* }

undo multicast extranet select-rpf { **all** | { **vpn-instance** *vpn-instance-name* | **public** } **group** *group-address* { *group-mask* | *group-mask-length* } }

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Specifies a source VPN instance. *vpn-instance-name* specifies the name of the source VPN instance.	The value is a string of 1 to 31 case-sensitive characters.
public	Indicates that the source VPN instance is a public network instance.	-
group *group-address*	Specifies the range of the addresses of multicast groups running the multicast VPN extranet service.	The value ranges from 224.0.0.0 to 239.255.255.255, in dotted decimal notation.
group-mask	Indicates the mask of a group address.	The value ranges from 240.0.0.0 to 255.255.255.255, in dotted decimal notation.
group-mask-length	Indicates the length of the mask of a group address.	The value is an integer ranging from 4 to 32.
all	Indicates all multicast routing policies.	-

Copyright © Huawei Technologies Co., Ltd.

Views

VPN instance view, VPN IPv4 address family view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In regular multicast VPN applications, multicast traffic can be transmitted only among different VPN sites in the same VPN, and VPN sites that belong to different VPNs cannot access each other.

In actual situations, enterprises in different VPNs need to communicate with each other, or service providers need to provide multicast services for users who reside in other VPNs. Multicast services need to be transmitted between different VPNs so that the multicast data from a VPN user needs to be provided for other VPN users.

Multicast VPN extranet is therefore introduced. Through this feature, receivers in a VPN can receive multicast data sent by the multicast sources in other VPNs or in the public network.

In multicast VPN extranet, the multicast source and the multicast receiver can belong to different VPN instances or the multicast source belongs to the public network instance whereas the multicast receiver belongs to a VPN instance. The public network and the VPN can be only PIM-SM/Source-Specific Multicast (SSM) networks.

Prerequisites

The **multicast routing-enable** command has been run in the public network instance view or the VPN instance view.

Precautions

The **multicast extranet select-rpf** command applies to MVPN extranet in remote cross scenarios. When using this command, note the following precautions:

- The VPN instance specified in the **vpn-instance** parameter cannot be the VPN instance in which view the command is run.
- If a public network instance is specified on the upstream device, a public network instance must be specified using the **public** parameter on the local device.
- If a VPN instance is specified on the upstream device, a VPN instance must be specified using the **vpn-instance** parameter on the local device. By default, an MVPN selects its tunnel interface as the upstream interface. Therefore, the remote-cross source VPN instance specified for VPN groups in a specified group address range must the same as the source VPN instance of the route to the multicast source.
- The rendezvous point (RP) set for source VPN and receiver VPN must be a static RP and the static RP must reside at the source VPN side to serve the multicast groups adopting the multicast VPN extranet service. RPs that server

 Copyright © Huawei Technologies Co., Ltd.

other multicast groups in this VPN can be either dynamic or static. The anycast RP function will not be affected.

- The address range of the multicast groups adopting the multicast VPN extranet service cannot overlap the multicast group address range used by the local VPN; the address range of the multicast groups adopting the multicast VPN extranet service set in the newly configured multicast routing policy cannot overlap the address range that has been configured for the multicast groups adopting the multicast VPN extranet service.
- The SSM group address range must be set consistently for both the source VPN and the receiver VPN for providing the multicast VPN extranet service.

Example

Configure a multicast routing policy for VPN RED, specifying VPN BLUE as the upstream of the RPF route selected by group 225.1.1.0/24.

```
<Huawei> system-view
[Huawei] ip vpn-instance RED
[Huawei-vpn-instance-RED] ipv4-family
[Huawei-vpn-instance-RED-af-ipv4] multicast routing-enable
[Huawei-vpn-instance-RED-af-ipv4] multicast extranet select-rpf vpn-instance BLUE group 225.1.1.0 24
```

Related Topics

10.3.29 display pim routing-table
10.7.11 display multicast routing-table
10.7.13 display multicast rpf-info

10.6.10 multicast-domain holddown-time

Function

The **multicast-domain holddown-time** command sets the delay for the switching from the switch-multicast distribution tree (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.

Copyright © Huawei Technologies Co., Ltd.

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 around 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 holddown timer. The system will perform the switchover after the holddown timer expires.

Prerequisites

The **multicast-domain share-group** command has been run in the corresponding VPN.

Precautions

In actual switchover, from the time when flow changes to the time when device senses the change, there is a delay about 1 to 30 seconds. That is, the delay from the time when the forwarding rate of the data changes and the time when system starts Holddown timer is about 1 to 30 seconds. The delay is not added to the value of the holddown-time. The total delay from the time when the forwarding rate of the data changes to the time when the system completes, the switchover is longer than the Holddown period by 1 to 30 seconds.

When *interval* is set to 0, the system finds that the forwarding rate is below the threshold and switches from the switch-MDT to the share-MDT.

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] ipv4-family
[Huawei-vpn-instance-mytest-af-ipv4] multicast-domain holddown-time 80
```

10.6.11 multicast-domain log switch-group-reuse

Function

The **multicast-domain log switch-group-reuse** command enables the output of log information about reusing Switch-Group.

The **undo multicast-domain log** command restores the default configuration.

 Copyright © Huawei Technologies Co., Ltd.

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

If Share-Group is not configured in a VPN, you are not recommended to run this command.

Example

Enable the output of log information about reusing Switch-Group in VPN **mytest**.

```
<Huawei> system-view
[Huawei] ip vpn-instance mytest
[Huawei-vpn-instance-mytest] ipv4-family
[Huawei-vpn-instance-mytest-af-ipv4] multicast-domain log switch-group-reuse
```

10.6.12 multicast-domain share-group

Function

The **multicast-domain share-group binding mtunnel** command specifies the Share-multicast distribution tree (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

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
group-address	Specifies the multicast group address.	The address 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 number is an integer that ranges from 0 to 1023.

Views

VPN IPv4 address family view

Default Level

2: Configuration level

Usage Guidelines

On the same Provider Edge (PE), different VPN instances are configured with the different group addresses. The value of *group-address* must be different from the Switch-Group address of all the instances on this PE. *number* cannot be the same as that of the MTI.

You cannot perform the same configuration repeatedly in the same VPN instance view. Instead, you can configure the new address and the MTI only after the previous configuration is deleted.

The IP address and Maximum Transmission Unit (MTU) can be configured on the MTI. The MTU is an integer that ranges from 46 to 1500 bytes.

Run the **undo multicast-domain share-group** command to delete all configurations related to the MTI.

Enable multicast routing in the VPN before running the command.

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] ipv4-family
[Huawei-vpn-instance-mytest-af-ipv4] multicast-domain share-group 224.1.1.1 binding mtunnel 0
```

Related Topics

10.7.28 multicast routing-enable

Copyright © Huawei Technologies Co., Ltd.

10.6.13 multicast-domain source-interface

Function

The **multicast-domain source-interface** command allows a Multicast Tunnel Interface (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 or VPN IPv4 address family view

Default Level

2: Configuration level

Usage Guidelines

The **multicast-domain source-interface** command can take effect only after multicast routing is enabled.

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 run in the system view, but not in 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. If an IP address is manually configured on an MTI, the default interface address specified using this command does not take effect.

 Copyright © Huawei Technologies Co., Ltd.

Example

Configure the MTI to use the IP address of the default interface named **loopback 1**.

```
<Huawei> system-view
[Huawei] multicast-domain source-interface loopback 1
```

10.6.14 multicast-domain switch-delay

Function

The **multicast-domain switch-delay** command specifies delay for the switching from Share-multicast distribution tree (MDT) to Switch-MDT.

The **undo multicast-domain switch-delay** command restores the default value of the delay.

By default, the delay for the switching from 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 switching from 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

When a downstream Provider Edge (PE) joins the Switch-Group, it takes certain time to set up the Switch-MDT in the public network. Therefore, the switching delay needs to be configured. The upstream PE sends a switching message. After the delay expires, the system uses the Switch-Group to encapsulate data. That is, data is switched from Share-MDT to Switch-MDT. Before the switch-delay timer times out, the system continues to detect the data forwarding rate. If the rate is always higher than the switchover threshold, the data packets are switched to the Switch-MDT. Otherwise, the packets are still forwarded by using the Share-MDT.

 Copyright © Huawei Technologies Co., Ltd.

Prerequisites

The **multicast-domain share-group** command has been run in the corresponding VPN.

Configuration Impact

If the **multicast-domain switch-delay** command is run several times in the same VPN instance view, the latest configuration will overwrite the previous ones.

Precautions

In actual switchover, from the time when flow changes to the time when device senses the change, there is a delay about 1 to 30 seconds. That is, the delay from the time when the forwarding rate of the data changes and the time when system starts the switch-delay timer is about 1 to 30 seconds. The delay is not added to the value of the switch-delay. The total delay from the time when the forwarding rate of the data changes to the time when the system completes the switchover time is longer than the switch-delay period by 1 to 30 seconds.

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] ipv4-family
[Huawei-vpn-instance-mytest-af-ipv4] multicast-domain switch-delay 20
```

10.6.15 multicast-domain switch-group-pool

Function

The **multicast-domain switch-group-pool** command specifies the range of the Switch-multicast distribution tree (MDT) switch-group-pool and the switching condition.

The **undo multicast-domain switch-group-pool** command restores the default configuration.

By default, switch-group-pool is not specified, and the switching 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* | *acl-name* }] *

undo multicast-domain switch-group-pool

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
switch-group-pool	Specifies the start address of Switch-Group-pool.	The address is in dotted decimal notation and ranges from 224.0.1.0 to 239.255.255.255.
network-mask	Specifies the mask of Switch-Group-pool address.	The mask 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 Switch-Group-pool address.	The value is an integer that ranges from 24 to 32; that is, the range of the group address in Switch-MDT switch-group-pool is from 0 to 255.
threshold *threshold-value*	Specifies the switching 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 number is an integer that ranges from 3000 to 3999.
acl-name	Specifies the name of a Named ACL. **NOTE** *acl-name* can only be the name of a named advanced ACL.	It is case-sensitive.

Views

VPN instance view, VPN IPv4 address family view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Between the Provider Edge (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 therefore 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.

 Copyright © Huawei Technologies Co., Ltd.

Prerequisites

A share-group has been configured in the corresponding VPN.

Configuration Impact

In some cases, the forwarding rate of VPN multicast data fluctuates around the switchover threshold. If the rate remains higher than the switchover threshold, data packets are switched to the switch-MDT. Otherwise, the packets are still forwarded by using the share-MDT.

This command is cyclical in nature. That is, the latest command overwrites the previous one, and takes effect.

Precautions

The Named ACL includes the basic ACL and the advanced ACL, whose configurations are same with the numbered ACL.

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

Set the Switch-group-pool of VPN instance named **mytest** to be from 225.2.2.1 to 225.2.2.15.

```
<Huawei> system-view
[Huawei] ip vpn-instance mytest
[Huawei-vpn-instance-mytest] ipv4-family
[Huawei-vpn-instance-mytest-af-ipv4] multicast-domain switch-group-pool 225.2.2.1 28
```

Use a Named ACL to set the Switch-group-pool to be from 225.2.2.1 to 225.2.2.15.

```
<Huawei> system-view
[Huawei] acl name myacl
[Huawei-acl-adv-myacl] rule permit ip source 1.1.1.1 0 destination 225.1.0.0 0.0.255.255
[Huawei] ip vpn-instance mytest
[Huawei-vpn-instance-mytest] ipv4-family
[Huawei-vpn-instance-mytest-af-ipv4] multicast-domain switch-group-pool 225.2.2.1 28 acl myacl
```

Related Topics

10.6.6 display multicast-domain vpn-instance switch-group receive
10.6.7 display multicast-domain vpn-instance switch-group send

10.6.16 multicast-domain switch-without-register

Function

The **multicast-domain switch-without-register** command disables the source Provider Edge (PE) from sending null Register messages to the Rendezvous Point (RP) to establish the shortest path tree (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.

 Copyright © Huawei Technologies Co., Ltd.

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 Any-Source Multicast (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 rendezvous point tree (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. Afterwards, the forwarding entries are created on the source PE, and the source PE encapsulates the data to 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. Then, the receiver PEs trigger the SPT switchover towards the source PE. In this manner, the SPT is established on the public network.

When the entries with the SPT switchover are in a large number, the speed of sending Register messages is limited. 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 solve the preceding problem, before configuring the VPN to use the Switch-Group address to encapsulate the VPN data, you can configure the source PE to send the null Register message to the RP to establish the SPT on the public network.

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

 Copyright © Huawei Technologies Co., Ltd.

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 vpn1, 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-instatnce vpn1
[Huawei-vpn-instance-vpn1] ipv4-family
[Huawei-vpn-instance-vpn1-af-ipv4] multicast-domain switch-without-register
```

Related Topics

10.6.5 display multicast-domain vpn-instance share-group
10.6.15 multicast-domain switch-group-pool

10.6.17 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. *vpn-instance-name* specifies the VPN instance name.	The value is a string of case-sensitive characters.
all-instance	Clears statistics about sent and received MDT switch messages in all VPN instances.	-

 Copyright © Huawei Technologies Co., Ltd.

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 normally 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
```

10.6.18 multicast extranet traffic-forward type

Function

The **multicast extranet traffic-forward type** command enables the traffic forwarding function for VLANIF interfaces on a multicast VPN extranet.

The **undo multicast extranet traffic-forward type** command restores the default configuration.

By default, the traffic forwarding function is disabled for VLANIF interfaces on a multicast VPN extranet.

Format

multicast extranet traffic-forward type vlanif

undo multicast extranet traffic-forward type vlanif

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
vlanif	Enables the traffic forwarding function for VLANIF interfaces on a multicast VPN extranet.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

By default, VLANIF interfaces do not forward traffic on a multicast VPN extranet, causing traffic interruptions. To resolve this issue, run the **multicast extranet traffic-forward type** command to enable the traffic forwarding function for VLANIF interfaces. After this command is run, forwarding information on the VLANIF interfaces will be delivered from the VPN routing and forwarding (VRF) table for receivers to the VRF table for multicast sources. Then, the VLANIF interfaces will be capable of forwarding traffic to receivers.

Precautions

The **multicast extranet traffic-forward type** command configuration is ineffective for existing multicast entries. To resolve this issue, run the **reset multicast forwarding-table** command to delete the existing multicast entries. After the multicast entries are regenerated, the **multicast extranet traffic-forward type** command will become effective for them.

Example

Enable the traffic forwarding function for VLANIF interfaces on a multicast VPN extranet.

```
<Huawei> system-view
[Huawei] multicast extranet traffic-forward type vlanif
```

10.6.19 rpf-vector compatible standard

Function

The **rpf-vector compatible standard** command configures a device to use the standard format defined in a relevant RFC to encapsulate Hello or Join/Prune messages carrying vector attributes.

The **undo rpf-vector compatible standard** command enables a device to use a private format to encapsulate Hello or Join/Prune messages carrying vector attributes.

Copyright © Huawei Technologies Co., Ltd.

By default, a private format is used to encapsulate Hello or Join/Prune messages carrying vector attributes.

Format

rpf-vector compatible standard

undo rpf-vector compatible standard

Parameters

None

Views

Public network instance PIM view or VPN instance PIM view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The vector attribute needs to be added to Join/Prune messages as the join attribute on PEs in an inter-AS MVPN Option B scenario. The **rpf-vector compatible standard** command can be used to configure the Provider Edges (PEs) to use the standard format to encapsulate Hello or Join/Prune messages carrying vector attributes. This command configuration facilitates device communication.

Prerequisites

The **multicast routing-enable** command has been run in the public network instance view or the VPN instance view.

Example

Configure a device on the public network to use the standard format to encapsulate Hello and Join/Prune messages carrying vector attributes.

```
<Huawei> system-view
[Huawei] multicast routing-enable
[Huawei] pim
[Huawei-pim] rpf-vector compatible standard
```

10.6.20 rpf-vector

Function

The **rpf-vector** command enables a device to add the vector attribute to a Join/Prune message as the join attribute.

The **undo rpf-vector** command disables a device from adding the vector attribute to a Join/Prune message as the join attribute.

 Copyright © Huawei Technologies Co., Ltd.

By default, a device is disabled from adding the vector attribute to a Join/Prune message as the join attribute.

Format

rpf-vector rd

undo rpf-vector rd

Parameters

Parameter	Description	Value
rd	Specifies the RD attribute in a vector.	-

Views

Public network instance PIM view or VPN instance PIM view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **rpf-vector rd** command needs to be run on Provider Edges (PEs) in an inter-AS MVPN Option B scenario to enable the PEs to add vector attributes with Route Distinguishers (RDs) to Join/Prune messages as join attributes. Then MDTs can be set up and inter-AS MVPN can be implemented.

Prerequisites

The **multicast routing-enable** command has been run in the public network instance view or the VPN instance view.

Example

Enable a device on the public network to add the vector attribute to a Join/Prune message as the join attribute.

```
<Huawei> system-view
[Huawei] multicast routing-enable
[Huawei] pim
[Huawei-pim] rpf-vector rd
```

Enable a device in VPN RED to add the vector attribute to a Join/Prune message as the join attribute.

```
<Huawei> system-view
[Huawei] multicast routing-enable
[Huawei] pim vpn-instance RED
[Huawei-pim-RED] rpf-vector rd
```

 Copyright © Huawei Technologies Co., Ltd.

10.7 Multicast Route Management (IPv4) Commands

10.7.1 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
```

 Copyright © Huawei Technologies Co., Ltd.

Table 10-88 Description of the display default-parameter mrm command output

Item	Description
System View Default Configurations	Default configurations 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.
Multi-topology	The Multicast-Topology function.
Interface View Default Configurations	Default configurations 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.

Related Topics

10.7.24 multicast load-splitting

10.7.26 multicast load-splitting-timer

10.7.25 multicast load-splitting weight

Copyright © Huawei Technologies Co., Ltd.

10.7.2 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

None.

Example

Display brief information about the MIGP routing table.

```
<Huawei> display migp routing-table
Route Flags: R - relay, D - download to fib
------------------------------------------------------------------------------
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        GigabitEthernet1/0/0
```

 Copyright © Huawei Technologies Co., Ltd.

```
10.5.5.5/32         OSPF   10   4           10.0.1.1        GigabitEthernet1/0/0
10.0.3.0/24         OSPF   10   3           10.0.1.1        GigabitEthernet1/0/0
192.168.3.0/24      OSPF   10   4           10.0.1.1        GigabitEthernet1/0/0
```

Table 10-89 Description of the display migp routing-table command output

Item	Description
Route Flags	Route flag that identifies the attribute of a route. • R: indicates that the route is an iterated route. • D: indicates that the route is delivered to the FIB table.
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
------------------------------------------------------------------------------
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: GigabitEthernet1/0/0
       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: GigabitEthernet1/0/0
       State: Active Adv           Age: 00h34m26s
```

 Copyright © Huawei Technologies Co., Ltd.

```
Destination: 10.0.2.0/24
    Protocol: ISIS           Process ID: 1
  Preference: 15                 Cost: 20
     NextHop: 10.0.1.1       Interface: GigabitEthernet1/0/0
       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: GigabitEthernet1/0/0
       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: GigabitEthernet1/0/0
       State: Active Adv          Age: 00h34m28s
```

Table 10-90 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.
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.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Age	Time that elapsed since a route is generated.

10.7.3 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 10-91 Description of the display migp routing-table statistics command output

Item	Description
Proto	Routing protocol.

Copyright © Huawei Technologies Co., Ltd.

Item	Description
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.

10.7.4 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 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.
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.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
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
------------------------------------------------------------------------------
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  GigabitEthernet1/0/0
```

Table 10-92 Description of the display mrt routing-table 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: 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.

Copyright © Huawei Technologies Co., Ltd.

Item	Description
Cost	Route cost.
Flags	Route flag 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
------------------------------------------------------------------------------
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: GigabitEthernet1/0/0
    TunnelID: 0x0                 Flags: R
```

Table 10-93 Description of the display mrt routing-table verbose command output

Item	Description
Routing Table: MRT	MRT routing table.
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.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
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.
Flags	Route flag in the header of the routing table.

10.7.5 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**

 Copyright © Huawei Technologies Co., Ltd.

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 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

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 10-94 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.

 Copyright © Huawei Technologies Co., Ltd.

10.7.6 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 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.
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.

 Copyright © Huawei Technologies Co., Ltd.

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        GigabitEthernet1/0/0
```

Table 10-95 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 flag in the header of the routing table.
NextHop	Next hop of a route.
Interface	Outbound interface to a reachable next hop.

10.7.7 display mtrace statistics

Function

The **display mtrace statistics** command displays statistics about multicast trace (Mtrace) packets.

Format

display mtrace statistics

Copyright © Huawei Technologies Co., Ltd.

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 10-96 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.

Related Topics

10.7.30 reset mtrace statistics

10.7.8 display multicast boundary

Function

The **display multicast boundary** command displays the multicast boundary configured on an interface.

Copyright © Huawei Technologies Co., Ltd.

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 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-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 in the public network instance.

```
<Huawei> display multicast boundary
Multicast boundary information of VPN-Instance: public net
```

 Copyright © Huawei Technologies Co., Ltd.

```
Total 1 Multicast IPv4 boundary
 Interface           Boundary
 GigabitEthernet1/0/0          225.1.1.0/24
```

Table 10-97 Description of the display multicast boundary command output

Item	Description
Multicast boundary information of VPN-Instance	VPN instance to which multicast boundary information belongs.
Total 1 Multicast IPv4 boundary	Total number of multicast boundaries configured on a router.
Interface	Interface configured with a multicast boundary.
Boundary	Information about the multicast boundary address.

Related Topics

10.7.17 multicast boundary

10.7.9 display multicast boundary policy

Function

The **display multicast boundary policy** command displays information about multicast boundary policies.

Format

display multicast [**vpn-instance** *vpn-instance-name* | **all-instance**] **boundary policy** [*group-address source-address* | **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 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-instance	Indicates all instances.	-
group-address	Specifies a multicast group address.	The value ranges from 224.0.1.0 to 239.255.255.255, in dotted decimal notation.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
source-address	Specifies a multicast source address.	The value is in dotted decimal notation. If the multicast source address is 0.0.0.0 in an entry, the entry is a (*, G) entry.
interface *interface-type interface-number*	Specifies the type and number of an interface on the router.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

Deploying a multicast forwarding boundary enhances multicast data security and prevents network congestion caused by forwarding multicast traffic within a large range. Multicast boundary policies can be used to defined multicast boundaries. Multicast boundary policies are classified into inbound multicast boundary policies, outbound multicast boundary policies, and inbound and outbound multicast boundary policies. The **display multicast boundary policy** command can be used to view information about multicast boundary policies.

Precautions

When using the **display multicast boundary policy** command, note the following points:

- If neither **vpn-instance** nor **all-instance** is specified, information about multicast boundary policies configured in the public network instance is displayed.
- If *group-address source-address* are specified, information about the multicast boundary policy that filters packets based on source and group addresses on each interface.
- If **interface** *interface-type interface-number* are specified, information about the multicast boundary on a specific interface is displayed.

Before running this command to check multicast boundary configuration, enable PIM in the interface view.

Example

Display information about multicast boundary policies in the public network instance.

```
<Huawei> display multicast boundary policy
Direction Flags: I - in, O - out, A - filter-autorp
------------------------------------------------------------------------
```

 Copyright © Huawei Technologies Co., Ltd.

```
Multicast boundary policy information of VPN-Instance: public net
Total 1 multicast IPv4 boundary policies
 Interface            Boundary policy     Direction          Result
 Eth0/0/1             2000                I O                --
```

Display information about the multicast boundary policy for (10.0.0.1, 225.0.0.0) in the public network instance.

```
<Huawei> display multicast boundary policy 225.0.0.0 10.0.0.1
Direction Flags: I - in, O - out, A - filter-autorp
------------------------------------------------------------------------
Multicast boundary policy information of VPN-Instance: public net
Total 1 multicast IPv4 boundary policies
 Interface            Boundary policy     Direction          Result
 Eth0/0/1             2000                I O                Block
```

Table 10-98 Description of the **display multicast boundary policy** command output

Item	Description
Direction Flags	Flag indicating the direction in which a multicast boundary policy takes effect: ● 1: indicates the inbound direction. ● O: indicates the outbound direction. ● A: filters Auto-RP packets.
Multicast boundary policy information of VPN-Instance	VPN instance to which multicast boundary information belongs
Total 2 multicast IPv4 boundary policies	Total number of multicast boundary policies configured on the router
Interface	Interface on which a multicast boundary is configured
Boundary policy	ACL applied to a multicast boundary policy on a specific interface
Direction	Flag indicating the direction in which a multicast boundary policy takes effect: ● 1: inbound direction ● O: indicates the outbound direction. ● A: filters Auto-RP packets.

Copyright © Huawei Technologies Co., Ltd.

Item	Description
Result	Whether a multicast boundary is configured in a specific direction for a specific multicast source and group on a specific interface: • Block: indicates that a multicast forwarding boundary is configured in a specific direction for a specific multicast source and group on a specific interface. • Unblock: indicates that no multicast forwarding boundary is configured in a specific direction for a specific multicast source and group on a specific interface. • --: indicates that the multicast source and group addresses are not identified.

Related Topics

10.7.18 multicast boundary policy

10.7.19 multicast boundary policy in

10.7.20 multicast boundary policy out

10.7.10 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** }] *

Copyright © Huawei Technologies Co., Ltd.

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 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-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 a multicast forwarding entry.	-
outgoing-interface	Indicates the outbound interface of a multicast forwarding entry.	-
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.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
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 detailed information about forwarding entries.	-
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 router 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 of the public network instance.

```
<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: GigabitEthernet1/0/0
    List of 1 outgoing interfaces:
      1:  GigabitEthernet2/0/0
          Activetime: 00:23:15
    Matched 1775842131 packets(113653895502 bytes), Wrong If 0 packets
    Forwarded 1769618431 packets(1071392 bytes)
```

 Copyright © Huawei Technologies Co., Ltd.

Table 10-99 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.
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.

 Copyright © Huawei Technologies Co., Ltd.

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. ● 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 LPU. ● SACK: indicates that the VPN instance has received the ACK message forwarded by software. ● 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.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
	• 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 • Multicast traffic that takes this interface as the outbound interface, in bytes • Number of packets with an incorrect incoming interface • Forwarded multicast traffic, in bytes

Related Topics

10.7.21 multicast forwarding-table downstream-limit
10.7.22 multicast forwarding-table route-limit
10.7.11 display multicast routing-table
10.7.31 reset multicast forwarding-table

10.7.11 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* }] | **extranet** { **source-vpn-instance** { *vpn-instance-name* | **all** | **public** } | **receive-vpn-instance** { *vpn-instance-name* | **all** } } | **incoming-interface** { *interface-type interface-number* | **register** | **mcast-extranet** } | **outgoing-interface** { **include** | **exclude** | **match** } { *interface-type interface-number* | **register** | **none** | **vpn-instance** *vpn-instance-name*}] * [**outgoing-interface-number** [*number*]]

Copyright © Huawei Technologies Co., Ltd.

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 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-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.
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
extranet	Indicates multicast extranet routing entries.	-
source-vpn-instance *vpn-instance-name*	Indicates the source VPN instance. *vpn-instance-name* specifies the name of the source VPN instance.	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	Indicates all instances.	-
public	Indicates the public network instance.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
receive-vpn-instance *vpn-instance-name*	Indicates the receiver VPN instance. *vpn-instance-name* specifies the name of the receiver VPN instance.	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.
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.	-
mcast-extranet	Indicates that the upstream interface is an extranet interface.	-
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.	-
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.

 Copyright © Huawei Technologies Co., Ltd.

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 of the public network instance.

```
<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: GigabitEthernet1/0/0
      List of 2 downstream interfaces
         1:  GigabitEthernet2/0/0
         2:  GigabitEthernet3/0/0
```

Table 10-100 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.
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.
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 in the public network instance.

```
<Huawei> display multicast routing-table outgoing-interface-number
Multicast routing table of VPN-Instance: public net
 Total 2 entries

 00001. (10.1.1.22, 232.1.1.1)
      Uptime: 00:00:07
      Upstream Interface: GigabitEthernet1/0/0
      List of 20 downstream interfaces
```

 Copyright © Huawei Technologies Co., Ltd.

```
00002. (10.1.1.22, 232.1.2.1)
     Uptime: 00:00:07
     Upstream Interface: GigabitEthernet2/0/0
     List of 20 downstream interfaces
```

Table 10-101 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.

Related Topics

10.7.10 display multicast forwarding-table

10.7.32 reset multicast routing-table

10.7.12 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 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.
config	Displays the configuration of the multicast static routes.	-
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.

Copyright © Huawei Technologies Co., Ltd.

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.

Example

Display all multicast static routes in the public network instance.

```
<Huawei> display multicast routing-table static
Multicast Routing Table
Routes : 1

 Mroute 10.1.0.0/24
        Interface = GigabitEthernet1/0/0       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 10-102 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.
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.

Copyright © Huawei Technologies Co., Ltd.

Item	Description
Order	Order of a route.
Running Configuration	Command line for configuring a static route.

Related Topics

10.7.14 ip rpf-route-static

10.7.13 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 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-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.
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.	-

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
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 in the public network instance.

```
<Huawei> display multicast rpf-info 192.168.0.1
 VPN-Instance: public net
 RPF information about source: 192.168.0.1
    RPF interface: GigabitEthernet1/0/0, 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 10-103 Description of the display multicast rpf-info command output

Item	Description
VPN-Instance	VPN instance to which displayed information belongs.
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.

 Copyright © Huawei Technologies Co., Ltd.

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.

Related Topics

10.7.11 display multicast routing-table
10.7.10 display multicast forwarding-table
10.7.14 ip rpf-route-static

10.7.14 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**]

 Copyright © Huawei Technologies Co., Ltd.

[**route-policy** *route-policy-name*] { *rpf-nbr* | *interface-type interface-number* } [**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 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.
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.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
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.
rpf-nbr	Specifies the IP address of the RPF neighbor.	-
interface-type interface-number	Specifies the type and the number of an interface, used to specify an interface.	-
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 router receives multicast data packets from the multicast source, it performs RPF check using the configured RPF route. Packets sent from the source to the router through other interfaces fail the RPF check.
- Connect RPF routes.

 Copyright © Huawei Technologies Co., Ltd.

If the unicast route on a network segment is incomplete, multicast packets cannot be forwarded due to lack of an RPF route. For example, when two adjacent devices run different routing protocols but 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 check 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 router 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 router 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 a P2MP 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
```

Related Topics

10.7.12 display multicast routing-table static
10.7.13 display multicast rpf-info

10.7.15 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 router on which the **mtrace** command is executed.

Format

mtrace [**-l** [*stat-times*] [**-st** *stat-int*] | **-m** *max-ttl* | [**-mr** | **-ur** *resp-dest*] | **-q** *nqueries* | **-tr** *ttl* | **-ts** *ttl* | **-v** | **-vpn-instance** *vpn-instance-name* | **-w** *timeout*] * **source** *source-address*

 Copyright © Huawei Technologies Co., Ltd.

mtrace -g *group* [**-l** [*stat-times*] [**-st** *stat-int*] | **-m** *max-ttl* | [**-mr** | **-ur** *resp-dest*] | **-q** *nqueries* | **-tr** *ttl* | **-ts** *ttl* | **-v** | **-vpn-instance** *vpn-instance-name* | **-w** *timeout*] * **source** *source-address*

mtrace { **-gw** *last-hop-router* | **-d** } **-r** *receiver* [**-a** *source-ip-address* | **-l** [*stat-times*] [**-st** *stat-int*] | **-m** *max-ttl* | [**-mr** | **-ur** *resp-dest*] | **-q** *nqueries* | **-tr** *ttl* | **-ts** *ttl* | **-v** | **-vpn-instance** *vpn-instance-name* | **-w** *timeout*] * **source** *source-address*

mtrace { **-gw** *last-hop-router* | **-b** | **-d** } **-r** *receiver* **-g** *group* [**-a** *source-ip-address* | **-l** [*stat-times*] [**-st** *stat-int*] | **-m** *max-ttl* | [**-mr** | **-ur** *resp-dest*] | **-q** *nqueries* | **-tr** *ttl* | **-ts** *ttl* | **-v** | **-vpn-instance** *vpn-instance-name* | **-w** *timeout*] * **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*

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.

 Copyright © Huawei Technologies Co., Ltd.

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 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.
-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 router address, which ensures that unicast packets can be transmitted between the querier and the last-hop router. After this parameter is specified, the initiating mode of Mtrace is specified as last-hop.	-

Copyright © Huawei Technologies Co., Ltd.

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 router 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.

 Copyright © Huawei Technologies Co., Ltd.

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 router or detonation host in unicast mode.
  - When multiple routers are connected to the specified host, RPF paths from different routers can be different. You can specify the last-hop router 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 router 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 router.

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 router address. Unicast packets can be transmitted between the querier and the last-hop router.
- **-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 the 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 are replied in multicast mode. At present, however, manufacturers have no unified opinion on this issue. In Huawei AR, the Router Alert option is carried in a packet. If Huawei devices 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 in the command line.

The parameter **vpn-instance** is used on the PE to initiate a multicast VPN probe.

 Copyright © Huawei Technologies Co., Ltd.

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 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
```

 Copyright © Huawei Technologies Co., Ltd.

```
  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.
```

 Copyright © Huawei Technologies Co., Ltd.

Table 10-104 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 router.
-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 router is PIM.
In calculating-rate mode, current statistic times is: 1	The rate is calculated for the first time in the calculating rate mode.
-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 router 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.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
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.

10.7.16 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 router 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 router 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 router that is connected to the host.

- This command takes effect only on the last hop router, which is not the querier.

 Copyright © Huawei Technologies Co., Ltd.

- This command filers 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 router, note the following points:

- If *basic-acl-number* is not specified, the last hop router does not reject IGMP-Tracert-Query packets in unicast mode.
- If *basic-acl-number* is specified but the ACL is not defined on the router, the last hop router rejects any IGMP-Tracert-Query packet in unicast mode.
- If *basic-acl-number* is specified and this ACL is defined on the router, only the IGMP-Tracert-Query packets allowed by the ACL can be received.

Example

Apply the querier filtering rules to the last hop router.

```
<Huawei> system-view
[Huawei] mtrace query-policy 2000
```

10.7.17 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.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
all	Deletes all the multicast boundaries configured on an interface.	-

Views

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 in the public network instance or VPN instance.

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 GE1/0/0 as the boundary of group 239.2.0.0/16.

```
<Huawei> system-view
[Huawei] multicast routing-enable
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] multicast boundary 239.2.0.0 16
```

Related Topics

10.7.8 display multicast boundary

Copyright © Huawei Technologies Co., Ltd.

10.7.18 multicast boundary policy

Function

The **multicast boundary policy** command configures an inbound and outbound multicast boundary policy on a specific interface.

The **undo multicast boundary policy** command cancels the configuration.

By default, no inbound and outbound multicast boundary policy is configured on an interface.

Format

multicast boundary policy *basic-acl-number* [**filter-autorp**]

undo multicast boundary policy *basic-acl-number* [**filter-autorp**]

Parameters

Parameter	Description	Value
basic-acl-number	Specifies the number of a basic ACL.	The value is an integer ranging from 2000 to 2999.
filter-autorp	Filters Auto-RP messages received on the interface. If this parameter is not specified, whether Auto-RP messages received on the interface are filtered depends on the ACL specified in the command.	-

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Deploying a multicast forwarding boundary enhances multicast data security and prevents network congestion caused by forwarding multicast traffic within a large range. Multicast boundary policies can be used to defined multicast boundaries. Multicast boundary policies are classified into inbound multicast boundary policies, outbound multicast boundary policies, and inbound and outbound multicast boundary policies. An inbound and outbound multicast boundary policy

 Copyright © Huawei Technologies Co., Ltd.

has the functions of both an inbound multicast boundary policy and an outbound multicast boundary policy and filters auto-RP packets by multicast group address.

Configuration Impact

If you run the **multicast boundary policy** command several times, the latest configuration overrides the previous configurations.

Precautions

The **multicast boundary policy** command works with the **acl** command. The parameter **source** in the **rule** command in the ACL view can be used to specify a group address range for an inbound and outbound multicast boundary policy.

A multicast boundary policy and IGMP proxy are mutually exclusive on an interface.

NOTE

If the AR connects to a third-party device and needs to receive Auto-RP messages from the third-party device, you must configure a rule to allow packets with destination addresses 224.0.1.39 and 224.0.1.40 to pass in the ACL specified in the multicast boundary policy.

Example

Configure an inbound and outbound multicast boundary policy for multicast group 225.0.0.0 on GigabitEthernet 1/0/0.

```
<Huawei> system-view
[Huawei] multicast routing-enable
[Huawei] acl 2000
[Huawei-acl-basic-2000] rule permit source 225.0.0.0 0
[Huawei-acl-basic-2000] quit
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] multicast boundary policy 2000
```

Related Topics

10.7.9 display multicast boundary policy

10.7.19 multicast boundary policy in

Function

The **multicast boundary policy in** command configures an inbound multicast boundary policy on a specific interface.

The **undo multicast boundary policy in** command cancels the configuration.

By default, no inbound multicast boundary policy is configured on an interface.

Format

multicast boundary policy { **acl-name** *acl-name* | *basic-acl-number* | *advanced-acl-number* } **in**

undo multicast boundary policy { **acl-name** *acl-name* | *basic-acl-number* | *advanced-acl-number* } **in**

Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
acl-name *acl-name*	Specifies the name of a named ACL. Only named advanced ACLs are supported.	The value is a string of 1 to 32 case-sensitive characters without spaces. The value must start with a letter (case sensitive).
basic-acl-number	Specifies the number of a basic ACL.	The value is an integer ranging from 2000 to 2999.
advanced-acl-number	Specifies the number of an advanced ACL.	The value is an integer ranging from 3000 to 3999.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Deploying a multicast forwarding boundary enhances multicast data security and prevents network congestion caused by forwarding multicast traffic within a large range. Multicast boundary policies can be used to defined multicast boundaries. Multicast boundary policies are classified into inbound multicast boundary policies, outbound multicast boundary policies, and inbound and outbound multicast boundary policies. An inbound multicast boundary policy effectively controls sourcegroup-specific data packets that can enter the local domain. An inbound multicast boundary filters multicast data packets received by an interface and PIM JoinPrune and IGMP Report messages to be sent by the interface to control multicast data direction and reception on the protocol control and forwarding planes.

Configuration Impact

If you run the **multicast boundary policy in** command several times, the latest configuration overrides the previous configurations.

Precautions

The **multicast boundary policy in** command works with the **acl** command.

- The parameter **source** in the **rule** command in the view of a numbered basic ACL can be used to specify a group address range for an inbound multicast boundary policy.
- The parameter **source** in the **rule** command in the view of a numbered advanced ACL can be used to specify a source address range and the parameter **destination** in this command can be used to specify a group address range for an inbound multicast boundary policy.

 Copyright © Huawei Technologies Co., Ltd.

- A named ACL uses the same rules as a numbered advanced ACL. The parameter **source** in the **rule** command in the ACL view can be used to specify a source address range and the parameter **destination** in this command can be used to specify a group address range for an inbound multicast boundary policy.

A multicast boundary policy and IGMP proxy are mutually exclusive on an interface.

NOTE

If the AR connects to a third-party device and needs to receive Auto-RP messages from the third-party device, you must configure a rule to allow packets with destination addresses 224.0.1.39 and 224.0.1.40 to pass in the ACL specified in the multicast boundary policy.

Example

Use a numbered basic ACL to configure an inbound multicast boundary policy for multicast group 225.0.0.0 on GigabitEthernet 1/0/0.

```
<Huawei> system-view
[Huawei] multicast routing-enable
[Huawei] acl 2000
[Huawei-acl-basic-2000] rule permit source 225.0.0.0 0
[Huawei-acl-basic-2000] quit
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] multicast boundary policy 2000 in
```

Related Topics

10.7.9 display multicast boundary policy

10.7.20 multicast boundary policy out

Function

The **multicast boundary policy out** command configures an outbound multicast boundary policy on a specific interface.

The **undo multicast boundary policy out** command cancels the configuration.

By default, no outbound multicast boundary policy is configured on an interface.

Format

multicast boundary policy { **acl-name** *acl-name* | *basic-acl-number* | *advanced-acl-number* } **out**

undo multicast boundary policy { **acl-name** *acl-name* | *basic-acl-number* | *advanced-acl-number* } **out**

Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
acl-name *acl-name*	Specifies the name of a named ACL. Only named advanced ACLs are supported.	The value is a string of 1 to 32 case-sensitive characters without spaces. The value must start with a letter (case sensitive).
basic-acl-number	Specifies the number of a basic ACL.	The value is an integer ranging from 2000 to 2999.
advanced-acl-number	Specifies the number of an advanced ACL.	The value is an integer ranging from 3000 to 3999.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Deploying a multicast forwarding boundary enhances multicast data security and prevents network congestion caused by forwarding multicast traffic within a large range. Multicast boundary policies can be used to defined multicast boundaries. Multicast boundary policies are classified into inbound multicast boundary policies, outbound multicast boundary policies, and inbound and outbound multicast boundary policies. Outbound multicast boundary policy effectively controls data packets that can be sent out of the local domain. An interface on which an outbound multicast boundary policy is configured filters received PIM JoinPrune messages, and IGMP Report messages and controls the generation of downstream interface lists of entries.

Configuration Impact

If you run the **multicast boundary policy out** command several times, the latest configuration overrides the previous configurations.

Precautions

The **multicast boundary policy out** command works together with the **acl** command.

- The **source** parameter in the **rule** command in the view of a numbered basic ACL can be used to specify a group address range for an outbound multicast boundary policy.
- The parameter **source** in the **rule** command in the view of a numbered advanced ACL can be used to specify a source address range and the parameter **destination** in this command can be used to specify a group address range for an outbound multicast boundary policy.

 Copyright © Huawei Technologies Co., Ltd.

- A named ACL uses the same rules as a numbered advanced ACL. The parameter **source** in the **rule** command in the ACL view can be used to specify a source address range and the parameter **destination** in this command can be used to specify a group address range for an outbound multicast boundary policy.

A multicast boundary policy and IGMP proxy are mutually exclusive on an interface.

Example

Configure an outbound multicast boundary policy for multicast group 225.0.0.0 on GigabitEthernet 1/0/0.

```
<Huawei> system-view
[Huawei] multicast routing-enable
[Huawei] acl 2000
[Huawei-acl-basic-2000] rule permit source 225.0.0.0 0
[Huawei-acl-basic-2000] quit
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] multicast boundary policy 2000 out
```

Related Topics

10.7.9 display multicast boundary policy

10.7.21 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 is an integer that ranges from: 0 to 128.

Views

System view, VPN instance view, VPN IPv4 address family view

Copyright © Huawei Technologies Co., Ltd.

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the router receives a multicast packet, it copies the packet for each downstream node in the matching multicast forwarding entry. If the router has a large number of multicast forwarding entries or each entry has many downstream nodes, many system resources are consumed. To reduce the loads of the router, 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 in the public network instance or VPN instance.

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 in the public network instance.

```
<Huawei> system-view
[Huawei] multicast routing-enable
[Huawei] multicast forwarding-table downstream-limit 32
```

Related Topics

10.7.10 display multicast forwarding-table

10.7.22 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.

By default, the limit on the number of entries in the multicast forwarding table varies according to device models:

- AR150&AR200 series: 64
- AR2201-48FE, AR2202-48FE, AR2204-27GE, AR2204-27GE-P, AR2204-51GE-P, AR2204-51GE-R, AR2204E, AR2204E-D, and AR2204: 128

Copyright © Huawei Technologies Co., Ltd.

- AR100&AR120&AR160&AR1200 series, AR2220, AR2220L, AR2220E, AR2240C: 1000
- AR2204XE and AR2204XE-DC: 2000
- AR2240 and AR3200 series:
  - Configured with SRU40: 1000
  - Configured with SRU60: 1000
  - Configured with SRU80: 2000
  - Configured with SRU100E: 2000
  - Configured with SRU200: 3000
  - Configured with SRU200E: 3000
  - Configured with SRU400: 4000
- AR3600 series (SRUX5): 3000

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 64 for the AR150&AR200 series • 0 to 128 for the AR2201-48FE, AR2202-48FE, AR2204-27GE, AR2204-27GE-P, AR2204-51GE-P, AR2204-51GE-R, AR2204E, AR2204E-D, and AR2204 • 0 to 1000 for the AR100&AR120&AR160&AR1200 series, AR2220E, AR2240C, AR2220 • 0 to 2000 for the AR2204XE and AR2204XE-DC • AR2240 and AR3200 series: – Configured with SRU40: 0 to 1000 – Configured with SRU60: 0 to 1000 – Configured with SRU80: 0 to 2000 – Configured with SRU100: 0 to 2000 – Configured with SRU100E: 0 to 2000 – Configured with SRU200: 0 to 3000 – Configured with SRU200E: 0 to 3000 – Configured with SRU400: 0 to 4000 • 1 to 3000 for the AR3600 series (SRUX5)

 Copyright © Huawei Technologies Co., Ltd.

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 router. 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 in the public network instance or VPN instance.

Precautions

NOTICE

If the limit on the number of entries in the multicast forwarding table is set after multicast services are deployed on a router, ensure that the limit on the number of entries in the multicast forwarding table is equal to or greater than the number of current forwarding entries. Otherwise, faults may occur.

You are recommended to limit the number of entries in the multicast forwarding table according to the actual network environment before the router operates multicast services.

If the newly-configured limit on the number of entries are less than the number of existing entries, the excessive entries are not deleted immediately. The configured limit on the number of entries 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 of the public network instance to 60.

```
<Huawei> system-view
[Huawei] multicast routing-enable
[Huawei] multicast forwarding-table route-limit 60
```

Related Topics

10.7.10 display multicast forwarding-table

10.7.31 reset multicast forwarding-table

Copyright © Huawei Technologies Co., Ltd.

10.7.23 multicast invalid-packet

Function

The **multicast invalid-packet** command sets the maximum number of invalid multicast protocol packets that can be stored on the router.

The **undo multicast invalid-packet** command deletes the set maximum number of invalid multicast protocol packets that can be stored on the router.

By default, the router can save a maximum of 10 invalid packets for each specific multicast protocol.

Format

multicast invalid-packet { **igmp** | **msdp** | **pim** } **max-count** *max-number*

undo multicast invalid-packet { **igmp** | **msdp** | **pim** }

Parameters

Parameter	Description	Value
igmp	Sets the maximum number of invalid IGMP 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 router 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 router to 20.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> system-view
[Huawei] multicast invalid-packet igmp max-count 20
```

Related Topics

10.1.8 display igmp invalid-packet

10.5.5 display msdp invalid-packet

10.3.27 display pim invalid-packet

10.7.24 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.	-
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

Copyright © Huawei Technologies Co., Ltd.

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

By default, if there are multiple equal-cost routes to a multicast source, the router applies the following route selection rules during RPF check:

- If the equal-cost routes are in the same routing table, for example, unicast routing table, multicast static routing table, or MBGP routing table, the router selects the route with the largest next-hop address as the RPF route.
- If the equal-cost routes are in different routing tables, the router selects the route with the highest preference. If the routes have the same preference, the router selects the route with the longest mask length. If the routes have the same preference and mask length, the router uses certain algorithm to select a route as the RPF route.

No matter which rule is used, the router 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 router 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 in the public network instance or VPN instance.

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 on the router, the **balance-preferred** or **stable-preferred** policy cannot be used.

Example

Configure group address-based load splitting in the public network instance.

```
<Huawei> system-view
[Huawei] multicast routing-enable
[Huawei] multicast load-splitting group
```

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

10.7.26 multicast load-splitting-timer
10.7.25 multicast load-splitting weight

10.7.25 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

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. An interface with a larger weight value has more multicast routing entries with it as the upstream interface.

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 applicable only when the multicast load splitting policy is set to stable-preferred or balance-preferred.

 Copyright © Huawei Technologies Co., Ltd.

When the 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 multicast load splitting weight on GE1/0/0 to 10.

```
<Huawei> system-view
[Huawei] multicast routing-enable
[Huawei] interface gigabitethernet  1/0/0
[Huawei-GigabitEthernet1/0/0] multicast load-splitting weight 10
```

Related Topics

10.7.24 multicast load-splitting

10.7.26 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.

 Copyright © Huawei Technologies Co., Ltd.

Currently, setting a load splitting timer to change the waiting time before balancing entries is supported.

- If the network is relatively stable, such as 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, such as when entries are deleted or added frequently or equal-cost routes are changed frequently, set the load splitting timer value to a greater 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 in the public network instance or VPN instance.

Example

Set a load splitting timer to 100 seconds.

```
<Huawei> system-view
[Huawei] multicast routing-enable
[Huawei] multicast load-splitting-timer 100
```

Related Topics

10.7.24 multicast load-splitting

10.7.27 multicast longest-match

Function

The **multicast longest-match** command configures the router to select the RPF route based on the longest matching rule.

The **undo multicast longest-match** command restores the default configuration.

By default, the router 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

 Copyright © Huawei Technologies Co., Ltd.

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

By default, the router selects the RPF route based on route preference. This command changes the route selection policy used by the router during RPF check. After you run this command, the router selects the RPF route with the longest mask. If multiple routes have the same mask length, the router selects the route with the highest preference.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command in the public network instance or VPN instance.

Example

Select routes according to the longest match in the public network instance.

```
<Huawei> system-view
[Huawei] multicast routing-enable
[Huawei] multicast longest-match
```

10.7.28 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

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

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

NOTICE

The **undo multicast routing-enable** command deletes all multicast configurations of the public network instance or a VPN instance. If multicast services are running in the instance, the multicast services are interrupted when this command is executed. To restore multicast services on the instance, you must re-configure the corresponding commands.

Example

Enable multicast routing in the public network instance.

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

Related Topics

10.1.15 igmp enable

10.3.50 pim dm

10.3.62 pim sm

10.5.12 msdp

10.7.29 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*

Copyright © Huawei Technologies Co., Ltd.

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.
-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.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
-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 information 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.
-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.

Copyright © Huawei Technologies Co., Ltd.

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 router, 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

 Copyright © Huawei Technologies Co., Ltd.

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 GE1/0/0, and detect the OSPF IGP router in the network segment.

```
<Huawei> ping multicast -i gigabitethernet 1/0/0 224.0.0.5
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 gigabitethernet 1/0/0 -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
```

 Copyright © Huawei Technologies Co., Ltd.

Table 10-105 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 Mtrace test is terminated after you press **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.
--- 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.

10.7.30 reset mtrace statistics

Function

The **reset mtrace statistics** command clears statistics about Mtrace packets.

Copyright © Huawei Technologies Co., Ltd.

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
```

Related Topics

10.7.7 display mtrace statistics

10.7.31 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 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-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.	-
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

 Copyright © Huawei Technologies Co., Ltd.

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.

Example

Delete the multicast forwarding entries of the group 225.5.4.3 from the forwarding table in the public network instance.

```
<Huawei> reset multicast forwarding-table 225.5.4.3
```

Related Topics

10.7.10 display multicast forwarding-table

10.7.32 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** } } *

Copyright © Huawei Technologies Co., Ltd.

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 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-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

 Copyright © Huawei Technologies Co., Ltd.

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 of the public network instance.

```
<Huawei> reset multicast routing-table 225.5.4.3
```

Related Topics

10.7.11 display multicast routing-table

10.7.10 display multicast forwarding-table

10.8 Multicast Route Management (IPv6) Commands

10.8.1 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.

Copyright © Huawei Technologies Co., Ltd.

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
 GE1/0/0               FF02::/64
```

Table 10-106 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.

Related Topics

10.8.6 multicast ipv6 boundary

 Copyright © Huawei Technologies Co., Ltd.

10.8.2 display multicast ipv6 boundary policy

Function

The **display multicast ipv6 boundary policy** command displays information about IPv6 multicast boundary policies.

Format

display multicast ipv6 boundary policy [*ipv6-group-address ipv6-source-address* | **interface** *interface-type interface-number*] *

Parameters

Parameter	Description	Value
ipv6-group-address	Specifies an IPv6 multicast group address.	The value ranges from FF00::0 to FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF, in hexadecimal notation.
ipv6-source-address	Specifies an IPv6 multicast source address.	The value is in dotted decimal notation. If the multicast source address is 0::0 in an entry, the entry is a (*, G) entry.
interface *interface-type interface-number*	Specifies the type and number of an interface.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

Deploying a multicast forwarding boundary enhances multicast data security and prevents network congestion caused by forwarding multicast traffic within a large range. Multicast boundary policies can be used to define multicast forwarding boundaries. Multicast boundary policies are classified into inbound multicast boundary policies, outbound multicast boundary policies, and inbound and outbound multicast boundary policies. The **display ipv6 multicast boundary policy** command can be used to view information about multicast boundary policies.

Precautions

When using the **display multicast ipv6 boundary policy** command, note the following points:

 Copyright © Huawei Technologies Co., Ltd.

- If *ipv6-group-address ipv6-source-address* is specified, information about the IPv6 multicast boundary policy that filters packets based on source and group addresses on each interface is displayed.
- If **interface** *interface-type interface-number* is specified, information about the IPv6 multicast boundary on a specific interface is displayed.

Example

Display information about IPv6 multicast boundaries on the router.

```
<Huawei> display multicast ipv6 boundary policy
Direction Flags: I - in, O - out
------------------------------------------------------------------------
IPv6 multicast boundary policy information
Total 1 multicast IPv6 boundary policy
 Interface            Boundary policy     Direction          Result
 GE1/0/0                 2000               I O              --
```

Display information about an IPv6 multicast boundary policy for (2000::2000, ff1e::1) and packet filtering results on the router.

```
<Huawei> display multicast ipv6 boundary policy ff1e::1 2000::2000
Direction Flags: I - in, O - out
IPv6 multicast boundary policy information
Total 1 multicast IPv6 boundary policy
 Interface            Boundary policy     Direction          Result
 GE1/0/0                 2000               I O            Block
```

Table 10-107 Description of the **display multicast ipv6 boundary policy** command output

Item	Description
Direction Flags	Flag indicating the direction in which a multicast boundary policy takes effect: • I: inbound direction • O: outbound direction
IPv6 multicast boundary policy information	Information about an IPv6 multicast boundary policy
Total 1 multicast IPv6 boundary policy	Total number of multicast boundary policies configured on the router
Interface	Interface on which a multicast boundary is configured
Boundary policy	IPv6 multicast boundary policy on an interface
Direction	Flag indicating the direction in which a multicast boundary policy takes effect: • I: inbound direction • O: outbound direction

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Result	Whether a multicast forwarding boundary is configured in a specific direction for a specific multicast source and group on a specific interface: • Block: indicates that a multicast forwarding boundary is configured in a specific direction for a specific multicast source and group on a specific interface. • Unblock: indicates that no multicast forwarding boundary is configured in a specific direction for a specific multicast source and group on a specific interface. • --: indicates that the source and multicast addresses are not identified.

Related Topics

10.8.7 multicast ipv6 boundary policy

10.8.8 multicast ipv6 boundary policy in

10.8.9 multicast ipv6 boundary policy out

10.8.3 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.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
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.	-
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 detailed information about forwarding entries.	-

 Copyright © Huawei Technologies Co., Ltd.

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 router 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: GigabitEthernet1/0/0
    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: GigabitEthernet2/0/0
    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 10-108 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.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
(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.

 Copyright © Huawei Technologies Co., Ltd.

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 LPU. • SACK: indicates that the VPN instance has received the ACK message forwarded by software.

 Copyright © Huawei Technologies Co., Ltd.

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)	Number of multicast packets and bytes that match the (S, G) entry.
Wrong If 0 packets	Number of packets with an incorrect incoming interface.
Forwarded 0 packets(0 bytes)	Number of packets and bytes forwarded by the (S, G) entry.

Related Topics

10.8.10 multicast ipv6 forwarding-table downstream-limit
10.8.11 multicast ipv6 forwarding-table route-limit
10.8.4 display multicast ipv6 routing-table

 Copyright © Huawei Technologies Co., Ltd.

10.8.4 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.	-

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
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.	The value is an integer that ranges from 0 to 2048.

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: GigabitEthernet1/0/0
      List of 1 downstream interface
        1:  GigabitEthernet2/0/0
```

 Copyright © Huawei Technologies Co., Ltd.

Table 10-109 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: GigabitEthernet1/0/0
      List of 2 downstream interfaces

 00002. (FC00::55, FF33::2)
      Uptime: 00:00:05
      Upstream Interface: GigabitEthernet2/0/0
      List of 2 downstream interfaces
```

Table 10-110 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.

Related Topics

10.8.3 display multicast ipv6 forwarding-table

10.8.18 reset multicast ipv6 routing-table

Copyright © Huawei Technologies Co., Ltd.

10.8.5 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.

Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> display multicast ipv6 rpf-info fc00::101
 VPN-Instance: public net
 RPF information about source: FC00::101
    RPF interface: GigabitEthernet1/0/0, RPF neighbor: FE80::208:ACFF:FE10:48
    Referenced route/mask: FC00::/64
    Referenced route type: unicast
    Load splitting rule: disable
```

Table 10-111 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.
RPF neighbor	Indicates the RPF neighbor.
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.

Related Topics

10.8.4 display multicast ipv6 routing-table
10.8.3 display multicast ipv6 forwarding-table

10.8.6 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* }

Copyright © Huawei Technologies Co., Ltd.

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

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 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.

 Copyright © Huawei Technologies Co., Ltd.

Example

Configure GE1/0/0 as the boundary of group FF02::101/16.

```
<Huawei> system-view
[Huawei] multicast ipv6 routing-enable
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] multicast ipv6 boundary FF02::101 16
```

Related Topics

10.8.1 display multicast ipv6 boundary

10.8.7 multicast ipv6 boundary policy

Function

The **multicast ipv6 boundary policy** command configures an IPv6 inbound and outbound multicast boundary policy on a specific interface.

The **undo multicast ipv6 boundary policy** command cancels the configuration.

By default, no IPv6 inbound and outbound multicast boundary policy is configured on an interface.

Format

multicast ipv6 boundary policy *basic-acl6-number*

undo multicast ipv6 boundary policy *basic-acl6-number*

Parameters

Parameter	Description	Value
basic-acl6-number	Specifies the number of a basic IPv6 ACL.	The value is an integer ranging from 2000 to 2999.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Deploying a multicast forwarding boundary enhances multicast data security and prevents network congestion caused by forwarding multicast traffic within a large range. Multicast boundary policies can be used to define multicast boundaries. Multicast boundary policies are classified into inbound multicast boundary policies, outbound multicast boundary policies, and inbound and outbound multicast boundary policies. An inbound and outbound multicast boundary policy

 Copyright © Huawei Technologies Co., Ltd.

has the functions of both an inbound multicast boundary policy and an outbound multicast boundary policy.

Precautions

The **multicast ipv6 boundary policy** command works with the **acl ipv6** command. The **source** parameter in the **rule** command can be run in the ACL6 view to specific a group address range for an inbound and outbound multicast boundary policy.

Example

Configure an inbound and outbound multicast boundary policy for multicast group FF1E::1/128 on GE1/0/0.

```
<Huawei> system-view
[Huawei] multicast ipv6 routing-enable
[Huawei] ipv6
[Huawei] acl ipv6 2000
[Huawei-acl6-basic-2000] rule deny source FF1E::1 128
[Huawei-acl6-basic-2000] quit
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] multicast ipv6 boundary policy 2000
```

Related Topics

10.8.2 display multicast ipv6 boundary policy

10.8.8 multicast ipv6 boundary policy in

Function

The **multicast ipv6 boundary policy in** command configures an IPv6 inbound multicast boundary policy on a specific interface.

The **undo multicast ipv6 boundary policy in** command cancels the configuration.

By default, no IPv6 inbound multicast boundary policy is configured on an interface.

Format

multicast ipv6 boundary policy { **acl6-name** *acl6-name* | *basic-acl6-number* | *advanced-acl6-number* } **in**

undo multicast ipv6 boundary policy { **acl6-name** *acl6-name* | *basic-acl6-number* | *advanced-acl6-number* } **in**

Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
acl6-name *acl6-name*	Specifies the name of a named IPv6 ACL. **NOTE** **acl6-name** *acl6-name* can only be the name of a named advanced ACL.	The value is a string of 1 to 32 case-sensitive characters without spaces. The value must start with a letter (case sensitive).
basic-acl6-number	Specifies the number of a basic IPv6 ACL.	The value is an integer ranging from 2000 to 2999.
advanced-acl6-number	Specifies the number of an advanced IPv6 ACL.	The value is an integer ranging from 3000 to 3999.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Deploying a multicast forwarding boundary enhances multicast data security and prevents network congestion caused by forwarding multicast traffic within a large range. Multicast boundary policies can be used to define multicast boundaries. Multicast boundary policies are classified into inbound multicast boundary policies, outbound multicast boundary policies, and inbound and outbound multicast boundary policies. An inbound multicast boundary policy effectively controls source/group-specific data packets that can enter the local domain. An inbound multicast boundary filters the multicast data packets that an interface can receive and the PIM Join/Prune and MLD Report messages that an interface can send. By filtering these messages, an inbound multicast boundary policy controls the direction in which multicast data is forwarded and received on the protocol control and forwarding planes.

Precautions

- If you run the **multicast ipv6 boundary policy in** command several times, the latest configuration overrides the previous configurations.
- The **multicast ipv6 boundary policy in** command works with the **acl ipv6** command.
  - The parameter **source** in the **rule** command can be run in the view of a numbered basic IPv6 ACL to specify a group address range for an inbound multicast boundary policy.
  - The parameter **source** in the **rule** command in the view of a numbered advanced IPv6 ACL can be used to specify a source address range and the parameter **destination** in this command can be used to specify a group address range for an inbound multicast boundary policy.

 Copyright © Huawei Technologies Co., Ltd.

- A named IPv6 ACL uses the same rules as a numbered advanced IPv6 ACL. The parameter **source** in the **rule** command in the ACL6 view can be used to specify a source address range and the parameter **destination** in this command can be used to specify a group address range for an inbound multicast boundary policy.

Example

Configure an inbound multicast boundary policy for multicast group FF1E::1/128 on GE1/0/0.

```
<Huawei> system-view
[Huawei] multicast ipv6 routing-enable
[Huawei] ipv6
[Huawei] acl ipv6 2000
[Huawei-acl6-basic-2000] rule permit source FF1E::1 128
[Huawei-acl6-basic-2000] quit
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] multicast ipv6 boundary policy 2000 in
```

Use a named IPv6 ACL to configure an inbound multicast boundary policy for the entry (2001::5, FF0E::1) on GE1/0/0.

```
<Huawei> system-view
[Huawei] multicast ipv6 routing-enable
[Huawei] ipv6
[Huawei] acl ipv6 name myacl6
[Huawei-acl6-adv-myacl6] rule permit ipv6 source 2001::5 128 destination FF0E::1 128
[Huawei-acl6-adv-myacl6] quit
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] multicast ipv6 boundary policy acl6-name myacl6 in
```

Related Topics

10.8.2 display multicast ipv6 boundary policy

10.8.9 multicast ipv6 boundary policy out

Function

The **multicast ipv6 boundary policy out** command configures an IPv6 outbound multicast boundary policy on a specific interface.

The **undo multicast ipv6 boundary policy out** command cancels the configuration.

By default, no IPv6 outbound multicast boundary policy is configured on an interface.

Format

multicast ipv6 boundary policy { **acl6-name** *acl6-name* | *basic-acl6-number* | *advanced-acl6-number* } **out**

undo multicast ipv6 boundary policy { **acl6-name** *acl6-name* | *basic-acl6-number* | *advanced-acl6-number* } **out**

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
acl6-name *acl6-name*	Specifies the name of a named IPv6 ACL. **NOTE** **acl6-name** *acl6-name* can only be the name of a named advanced ACL.	The value is a string of 1 to 32 case-sensitive characters without spaces. The value must start with a letter (case sensitive).
basic-acl6-number	Specifies the number of a basic IPv6 ACL.	The value is an integer ranging from 2000 to 2999.
advanced-acl6-number	Specifies the number of an advanced IPv6 ACL.	The value is an integer ranging from 3000 to 3999.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Deploying a multicast forwarding boundary enhances multicast data security and prevents network congestion caused by forwarding multicast traffic within a large range. Multicast boundary policies can be used to define multicast boundaries. Multicast boundary policies are classified into inbound multicast boundary policies, outbound multicast boundary policies, and inbound and outbound multicast boundary policies. Outbound multicast boundary policy effectively controls source/group-specific data packets that can be sent out of the local domain. An interface on which an outbound multicast boundary policy is configured filters the PIM Join/Prune and MLD Report messages that an interface can receive. By filtering these messages, an outbound multicast boundary policy controls the downstream interfaces in the downstream interface list of a multicast forwarding entry.

Configuration Impact

Precautions

- If you run the **multicast ipv6 boundary policy out** command several times, the latest configuration overrides the previous configurations.
- The **multicast ipv6 boundary policy out** command works with the **acl ipv6** command.
  - The parameter **source** in the **rule** command can be run in the view of a numbered basic IPv6 ACL to specify a group address range for an outbound multicast boundary policy.

 Copyright © Huawei Technologies Co., Ltd.

- The parameter **source** in the **rule** command in the view of a numbered advanced IPv6 ACL can be used to specify a source address range and the parameter **destination** in this command can be used to specify a group address range for an outbound multicast boundary policy.
- A named IPv6 ACL uses the same rules as a numbered advanced IPv6 ACL. The parameter **source** in the **rule** command in the ACL6 view can be used to specify a source address range and the parameter **destination** in this command can be used to specify a group address range for an outbound multicast boundary policy.

Example

Use a numbered basic IPv6 ACL to configure an outbound multicast boundary policy for multicast group FF1E::1/128 on GE1/0/0.

```
<Huawei> system-view
[Huawei] multicast ipv6 routing-enable
[Huawei] ipv6
[Huawei] acl ipv6 2000
[Huawei-acl6-basic-2000] rule permit source FF1E::1 128
[Huawei-acl6-basic-2000] quit
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] multicast ipv6 boundary policy 2000 out
```

Use a named IPv6 ACL to configure an outbound multicast boundary policy for the entry (2001::5, FF0E::1) on GE1/0/0.

```
<Huawei> system-view
[Huawei] multicast ipv6 routing-enable
[Huawei] ipv6
[Huawei] acl ipv6 name myacl6
[Huawei-acl6-adv-myacl6] rule permit ipv6 source 2001::5 128 destination FF0E::1 128
[Huawei-acl6-adv-myacl6] quit
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] multicast ipv6 boundary policy acl6-name myacl6 out
```

Related Topics

10.8.2 display multicast ipv6 boundary policy

10.8.10 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

 Copyright © Huawei Technologies Co., Ltd.

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 router receives a multicast packet, it copies the packet for each downstream node in the matching IPv6 multicast forwarding entry. If the router has a large number of IPv6 multicast forwarding entries or each entry has many downstream nodes, many system resources are consumed. To reduce the loads of the router, limit the maximum number of downstream nodes in each IPv6 multicast forwarding entry.

Prerequisites

IPv6 multicast routing has been enabled 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
```

Related Topics

10.8.3 display multicast ipv6 forwarding-table

Copyright © Huawei Technologies Co., Ltd.

10.8.11 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.

By default, the limit on the number of entries in the IPv6 multicast forwarding table varies according to device models:

- AR100&AR120&AR150&AR160&AR200 series: 64
- AR1200 series, AR2201-48FE, AR2202-48FE, AR2204-27GE, AR2204-27GE-P, AR2204-51GE-P, AR2204-51GE-R, AR2204E, AR2204E-D, and AR2204: 128
- AR2220, AR2240C, and AR2220E: 256
- AR2204XE and AR2204XE-DC: 512
- AR2240 and AR3200 series:
  - Configured with SRU40: 256
  - Configured with SRU60: 256
  - Configured with SRU80: 512
  - Configured with SRU100: 512
  - Configured with SRU100E: 512
  - Configured with SRU200: 1024
  - Configured with SRU200E: 1024
  - Configured with SRU400: 2048
- AR3600 series (SRUX5): 1024

Format

multicast ipv6 forwarding-table route-limit *limit*

undo multicast ipv6 forwarding-table route-limit

 Copyright © Huawei Technologies Co., Ltd.

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 64 for the AR100&AR120&AR150&AR160&AR200 series • 0 to 128 for the AR1200 series, AR2201-48FE, AR2202-48FE, AR2204-27GE, AR2204-27GE-P, AR2204-51GE-P, AR2204-51GE-R, AR2204E, AR2204E-D, and AR2204 • 0 to 256 for the AR2220, AR2240C, and AR2220E • 0 to 512 for the AR2204XE and AR2204XE-DC • AR2240 and AR3200 series: – Configured with SRU40: 0 to 256 – Configured with SRU60: 0 to 256 – Configured with SRU80: 0 to 512 – Configured with SRU100: 0 to 512 – Configured with SRU100E: 0 to 512 – Configured with SRU200: 0 to 1024 – Configured with SRU200E: 0 to 1024 – Configured with SRU400: 0 to 2048 • 1 to 1024 for the AR3600 series (SRUX5)

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Excessive IPv6 multicast forwarding entries will exhaust the memory of the router. 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 using the **multicast ipv6 routing-enable** command in the system view.

Precautions

 Copyright © Huawei Technologies Co., Ltd.

NOTICE

If the limit on the number of entries in the IPv6 multicast forwarding table is set after multicast services are deployed on a router, ensure that the limit on the number of entries in the IPv6 multicast forwarding table is equal to or greater than the number of current forwarding entries. Otherwise, faults may occur.

You are recommended to limit the number of entries in the IPv6 multicast forwarding table according to the actual network environment before the router operates multicast services.

If the newly-configured limit on the number of entries are less than the number of existing entries, the excessive entries are not deleted immediately. The configured maximum number of entries 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 run.

Example

Set the limit on the number of the entries in the IPv6 forwarding table to 60.

```
<Huawei> system-view
[Huawei] multicast ipv6 routing-enable
[Huawei] multicast ipv6 forwarding-table route-limit 60
```

Related Topics

10.8.3 display multicast ipv6 forwarding-table

10.8.17 reset multicast ipv6 forwarding-table

10.8.12 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 router.

The **undo multicast ipv6 invalid-packet** command deletes the set maximum number of invalid IPv6 multicast protocol packets that can be stored on the router.

By default, the router 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** }

 Copyright © Huawei Technologies Co., Ltd.

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 router 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 router to 20.

```
<Huawei> system-view
[Huawei] multicast ipv6 invalid-packet mld max-count 20
```

Related Topics

10.2.8 display mld invalid-packet

10.4.25 display pim ipv6 invalid-packet

10.8.13 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.

Copyright © Huawei Technologies Co., Ltd.

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 using the **multicast ipv6 routing-enable** command in the system view.

Follow-up Procedure

 Copyright © Huawei Technologies Co., Ltd.

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 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 router, 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
```

Related Topics

10.8.14 multicast ipv6 load-splitting weight

10.8.15 multicast ipv6 load-splitting-timer

10.8.14 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

Interface view

Copyright © Huawei Technologies Co., Ltd.

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. An interface with a larger weight value has more IPv6 multicast routing entries with it as the upstream interface.

Prerequisites

IPv6 multicast routing has been enabled 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 GE1/0/0 to 10.

```
<Huawei> system-view
[Huawei] multicast ipv6 routing-enable
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] multicast ipv6 load-splitting weight 10
```

Related Topics

10.8.13 multicast ipv6 load-splitting

10.8.15 multicast ipv6 load-splitting-timer

Function

The **multicast ipv6 load-splitting-timer** command sets a load splitting timer.

The **undo multicast ipv6 load-splitting-timer** command restores the default setting.

By default, the value of a load splitting timer is 1800 seconds.

Format

multicast ipv6 load-splitting-timer *interval*

undo multicast ipv6 load-splitting-timer

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
interval	Specifies the value of the 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 relatively stable, such as 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, such as 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 using the **multicast ipv6 routing-enable** command in the system view.

Example

Set a load splitting timer to 100 seconds.

```
<Huawei> system-view
[Huawei] multicast ipv6 routing-enable
[Huawei] multicast ipv6 load-splitting-timer 100
```

Related Topics

10.8.13 multicast ipv6 load-splitting

Copyright © Huawei Technologies Co., Ltd.

10.8.16 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

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.

Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> system-view
[Huawei] multicast ipv6 routing-enable
```

Related Topics

10.2.16 mld enable

10.4.47 pim ipv6 dm

10.4.59 pim ipv6 sm

10.8.17 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.
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.	-

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
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
```

Related Topics

10.8.3 display multicast ipv6 forwarding-table

10.8.18 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** } } *

 Copyright © Huawei Technologies Co., Ltd.

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.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> reset multicast ipv6 routing-table FF02::101
```

Related Topics

10.8.3 display multicast ipv6 forwarding-table

10.8.4 display multicast ipv6 routing-table

10.9 IGMP Snooping Configuration Commands

NOTE

Only AR129CV, AR129CVW, AR129CGVW-L and AR2200&AR3200&AR3600 series support IGMP Snooping.

Only the 8FE1GE, 24GE and 24ES2GP cards support IGMP Snooping.

10.9.1 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

 Copyright © Huawei Technologies Co., Ltd.

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 the VLAN is in Up state (at least one interface in the VLAN is in Up state) and has IGMP snooping enabled. 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 Enable
  IGMP Version is Set to default 2
  IGMP Query Interval is Set to default 60
  IGMP Max Response Interval is Set to default 10
  IGMP Robustness is Set to default 2
  IGMP Last Member Query Interval is Set to default 1
  IGMP Router Port Aging Interval is Set to 180s or holdtime in hello
  IGMP Filter Group-Policy is Set to default : Permit All
  IGMP 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
```

Table 10-112 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 Enable	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	Version of IGMP messages that can be processed in the VLAN. 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.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
IGMP Query Interval is Set to default 60	Interval at which IGMP General Query messages are sent. In this example, the default value (60 seconds) is displayed. This parameter is configured using the **igmp-snoopig query-interval** command.
IGMP Max Response Interval is Set to default 10	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-snoopig 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 1	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-snoopig 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 Set to default : Permit All	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 prompt leave function is disabled for interfaces in the VLAN (default configuration). The prompt leave function can be enabled using the **igmp-snooping prompt-leave** command.
IGMP Router Alert is Not Required	The router does not require that the IGMP messages received from the VLAN contain the Router-Alert option in the IP header (default configuration). The router can be configured to discard IGMP messages without the Router-Alert option using the **igmp-snooping require-router-alert** command.

Copyright © Huawei Technologies Co., Ltd.

Item	Description
IGMP Send Router Alert Enable	The router sends the IGMP messages with the Router-Alert option to the VLAN (default configuration). The router 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 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.

Related Topics

10.9.2 display igmp-snooping configuration
10.9.8 igmp-snooping enable (system view)
10.9.9 igmp-snooping enable (VLAN view)
10.9.12 igmp-snooping group-policy (VLAN view)
10.9.13 igmp-snooping lastmember-queryinterval
10.9.15 igmp-snooping max-response-time
10.9.16 igmp-snooping prompt-leave
10.9.17 igmp-snooping querier enable
10.9.18 igmp-snooping query-interval
10.9.19 igmp-snooping report-suppress
10.9.20 igmp-snooping require-router-alert

 Copyright © Huawei Technologies Co., Ltd.

10.9.21 igmp-snooping robust-count
10.9.22 igmp-snooping router-aging-time
10.9.23 igmp-snooping router-learning (VLAN view)
10.9.26 igmp-snooping send-router-alert
10.9.28 igmp-snooping ssm-mapping enable
10.9.31 igmp-snooping suppress-time
10.9.32 igmp-snooping version

10.9.2 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

 Copyright © Huawei Technologies Co., Ltd.

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
```

Table 10-113 Description of the display igmp-snooping configuration command output

Item	Description
IGMP Snooping Configuration for VLAN 7	The following information displayed is the IGMP snooping configuration in VLAN 7.
igmp-snooping enable	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-snooping version 3	Messages of IGMPv1, IGMPv2, and IGMPv3 can be processed in the VLAN. By default, IGMPv1 and IGMPv2 messages can be processed in a VLAN. This parameter is configured using the **igmp-snooping version** command.
igmp-snooping ssm-mapping enable	IGMP snooping SSM mapping is enabled in the VLAN. By default, IGMP snooping SSM mapping is disabled in a VLAN. IGMP snooping SSM mapping can be enabled using the **igmp-snooping ssm-mapping enable** command.
igmp-snooping ssm-policy 2000	The SSM mapping policy that references ACL 2000 is configured in the VLAN. By default, no SSM group policy is applied to a VLAN. An SSM group policy is configured using the **igmp-snooping ssm-policy** command.

Copyright © Huawei Technologies Co., Ltd.

Item	Description
igmp-snooping ssm-mapping 232.1.1.0 255.255.255.0 10.1.2.1	In the SSM mapping policy, multicast group addresses 232.1.1.0 through 232.1.1.255 are mapped to multicast source 10.1.2.1. By default, group-source mapping is configured in a VLAN. A group-source mapping is configured using the **igmp-snooping ssm-mapping** command.

Related Topics

10.9.1 display igmp-snooping
10.9.8 igmp-snooping enable (system view)
10.9.9 igmp-snooping enable (VLAN view)
10.9.12 igmp-snooping group-policy (VLAN view)
10.9.13 igmp-snooping lastmember-queryinterval
10.9.15 igmp-snooping max-response-time
10.9.16 igmp-snooping prompt-leave
10.9.17 igmp-snooping querier enable
10.9.18 igmp-snooping query-interval
10.9.19 igmp-snooping report-suppress
10.9.20 igmp-snooping require-router-alert
10.9.21 igmp-snooping robust-count
10.9.22 igmp-snooping router-aging-time
10.9.23 igmp-snooping router-learning (VLAN view)
10.9.26 igmp-snooping send-router-alert
10.9.27 igmp-snooping ssm-mapping
10.9.28 igmp-snooping ssm-mapping enable
10.9.29 igmp-snooping ssm-policy
10.9.31 igmp-snooping suppress-time
10.9.32 igmp-snooping version

10.9.3 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**]

 Copyright © Huawei Technologies Co., Ltd.

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 router with IGMP snooping enabled receives IGMP messages exchanged between hosts and a Layer 3 device, the router 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 router have multicast users connected, and control multicast services conveniently.

Precautions

 Copyright © Huawei Technologies Co., Ltd.

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.

Example

Display information about multicast group member ports in VLAN 7.

```
<Huawei> display igmp-snooping port-info vlan 7
----------------------------------------------------------------------
             (Source, Group)    Port                    Flag
----------------------------------------------------------------------
VLAN 7, 5 Entry(s)
                (*,226.1.1.1)   Eth2/0/0                -D-
                                  1 port(s)
          (10.1.1.1,226.1.1.2)  Eth2/0/0                --M
                                  1 port(s)
          (10.1.1.1,226.1.1.3)  Eth2/0/0                --M
                                  1 port(s)
              (*, 227.1.1.2)    Eth2/0/0                S--
                                  1 port(s)
              (*, 227.1.1.3)    Eth2/0/0                S--
                                  1 port(s)
----------------------------------------------------------------------
```

Table 10-114 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.
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 7, 5 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 239.255.255.250 on VLAN 22:
   Time of this group has been up : 00:01:22

 The port information of (10.1.1.2, 239.255.255.250):
   Time of this source has been up : 00:01:22
```

 Copyright © Huawei Technologies Co., Ltd.

```
  Port Table on this source(10.1.1.2):
    No.1
      Port name : Eth2/0/0
      Time of this port has been up as a host-port : 00:01:22
      Remain time of port expire as dynamic host-port : 00:02:58
      Version2-host-present-timer-expiry: 00:04:14
      Host-port flags : Dynamic

The port information of Group 227.1.1.1 on VLAN 200:
  Time of this group has been up : 1d:05h

 The port information of (0.0.0.0, 227.1.1.1):
  Time of this source has been up : 1d:05h
  Port Table on this source(0.0.0.0):
    No.1
      Port name : Eth2/0/0
      Time of this port has been up as a host-port : 1d:05h
      Remain time of port expire as dynamic host-port : NA
      Host-port flags : Static
```

Table 10-115 Description of the display igmp-snooping port-info verbose command output

Item	Description
The port information of Group 239.255.255.250 on VLAN 22	Information about member ports of multicast group 239.255.255.250 in VLAN 22.
Time of this group has been up	Time that elapsed since the multicast group was set up.
The port information of (10.1.1.2, 239.255.255.250)	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.
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).

 Copyright © Huawei Technologies Co., Ltd.

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.
Version2-host-present-timer-expiry	Agile time of the IGMPv2 host.
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

Related Topics

10.9.8 igmp-snooping enable (system view)
10.9.9 igmp-snooping enable (VLAN view)
10.9.15 igmp-snooping max-response-time
10.9.18 igmp-snooping query-interval
10.9.21 igmp-snooping robust-count
10.9.33 l2-multicast static-group

10.9.4 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*]

Copyright © Huawei Technologies Co., Ltd.

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 router to send IGMP Query messages instead 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
```

 Copyright © Huawei Technologies Co., Ltd.

Table 10-116 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.

Related Topics

10.9.17 igmp-snooping querier enable

10.9.5 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.	The value is an integer that ranges from 1 to 4094.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

Copyright © Huawei Technologies Co., Ltd.

A router port connects the router 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)
Eth2/0/0                03:28:16    00:01:20    DYNAMIC
Eth1/0/2                2d:10h      --          STATIC
```

Table 10-117 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

Related Topics

10.9.8 igmp-snooping enable (system view)

10.9.9 igmp-snooping enable (VLAN view)

10.9.22 igmp-snooping router-aging-time

10.9.30 igmp-snooping static-router-port

Copyright © Huawei Technologies Co., Ltd.

10.9.6 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, and 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,

Copyright © Huawei Technologies Co., Ltd.

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      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
 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
    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
    Proxy Send General Query             0
    Proxy Send Group-Specific Query      0
    Proxy Send Group-Source-Specific Query 0
```

 Copyright © Huawei Technologies Co., Ltd.

Table 10-118 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.
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 MSTP interface blocking events.
Recv MSTP Forward Event Times	Number of MSTP forwarding events.
Recv LINK Change Event Times	Number of link status change events.
IGMP Snooping Packets Counter	Statistics on IGMP and PIM 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 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.

 Copyright © Huawei Technologies Co., Ltd.

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.

Related Topics

10.9.9 igmp-snooping enable (VLAN view)
10.9.36 reset igmp-snooping statistics

10.9.7 display l2-multicast forwarding-table

Function

The **display l2-multicast forwarding-table** command displays the Layer 2 multicast forwarding table.

Format

display l2-multicast forwarding-table vlan *vlan-id* [[**source-address** *source-address*] **group-address** { *group-address* | **router-group** }]

Parameters

Parameter	Description	Value
vlan *vlan-id*	Displays Layer 2 multicast forwarding entries in a specified VLAN.	The value is an integer that ranges from 1 to 4094.
source-address *source-address*	Displays the forwarding entries of a specified multicast source.	The value is in dotted decimal notation.
group-address *group-address*	Displays multicast forwarding entries of a specified multicast group.	The value ranges from 224.0.1.0 to 239.255.255.255 in dotted decimal notation.
router-group	Displays multicast forwarding entries of all router ports.	-

Copyright © Huawei Technologies Co., Ltd.

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 dynamic 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 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 l2-multicast forwarding-table vlan 10
VLAN ID : 10, Forwarding Mode : IP
--------------------------------------------------------------------------------
                (Source, Group)     Interface            Out-Vlan
--------------------------------------------------------------------------------
                   Router-port     Ethernet2/0/0            10
                 (*, 225.1.1.6)    Ethernet2/0/0            10
                                   Ethernet1/0/2            10
               (*, 235.80.68.83)   Ethernet2/0/0            10
                                   Ethernet1/0/2            10
--------------------------------------------------------------------------------
Total Group(s): 2
```

Table 10-119 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.
(Source, Group)	(S, G) entry, specifying the multicast source and multicast group. The Router-port field indicates a router port.

Copyright © Huawei Technologies Co., Ltd.

Item	Description
Interface	Outbound interface.
Out-Vlan	VLAN ID of packets.
Total Group(s)	Total number of multicast forwarding entries.

Related Topics

10.9.33 l2-multicast static-group

10.9.8 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 and in a VLAN.

Format

igmp-snooping enable

undo igmp-snooping enable

Parameters

None

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.

Copyright © Huawei Technologies Co., Ltd.

If you run the **igmpsnooping enable vlan** { *vlan-id1* [**to** *vlan-id2*] } &<1-10> command multiple times, all the configurations take effect.

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 configuration is deleted. When you run the **igmp-snooping enable** command to enable IGMP snooping globally again, the router uses the default IGMP snooping configuration.

Example

Enable IGMP snooping globally.

```
<Huawei> system-view
[Huawei] igmp-snooping enable
```

Related Topics

10.9.1 display igmp-snooping

10.9.2 display igmp-snooping configuration

10.9.9 igmp-snooping enable (VLAN view)

10.9.9 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

 Copyright © Huawei Technologies Co., Ltd.

By default, IGMP snooping is disabled in a VLAN after IGMP snooping is 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.

Example

Enable IGMP snooping in VLAN 2.

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

Related Topics

10.9.1 display igmp-snooping

10.9.2 display igmp-snooping configuration

10.9.8 igmp-snooping enable (system view)

10.9.10 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 maximum number of multicast entries that an interface can learn varies according to device models:

- AR2201-48FE, AR2202-48FE, AR2204-27GE, AR2204-27GE-P, AR2204-51GE-P, AR2204-51GE-R, AR2204E, AR2204E-D and AR2204: 128
- AR2220E andAR2220: 1000
- AR2204XE and AR2204XE-DC: 2000
- AR2240C: 1000
- AR2240 and AR3200 series:
  - Configured with SRU40: 1000
  - Configured with SRU60: 1000
  - Configured with SRU80: 2000
  - Configured with SRU100: 2000
  - Configured with SRU100E: 2000

 Copyright © Huawei Technologies Co., Ltd.

  - Configured with SRU200: 2000
  - Configured with SRU200E: 2000
  - Configured with SRU400: 2000
- AR3600 series (SRUX5): 2000

Format

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> }

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
group-limit	Specifies the maximum number of multicast groups that an interface can learn.	The value is an integer ranging from • 1 to 128 for the AR2201-48FE, AR2202-48FE, AR2204-27GE, AR2204-27GE-P, AR2204-51GE-P, AR2204-51GE-R, AR2204E, AR2204E-Dand AR2204 • 1 to 1000 for the AR2220, and AR2220E • AR2204XE and AR2204XE-DC: 1 to 2000 • AR2240C: 1 to 1000 • AR2240 and AR3200 series (depending on the SRU model used on the router): – Configured with SRU40: 1 to 1000 – Configured with SRU60: 1 to 1000 – Configured with SRU80: 1 to 2000 – Configured with SRU100E: 1 to 2000 – Configured with SRU200: 1 to 2000 – Configured with SRU200E: 1 to 2000 – Configured with SRU400: 1 to 2000 • 1 to 2000 for the AR3600 series (SRUX5)
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.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
all	Cancels the limit on the number of multicast groups that interfaces in all VLANs can learn.	-

Views

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 Eth2/0/0 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 ethernet 2/0/0
[Huawei-Ethernet2/0/0] igmp-snooping group-limit 10 vlan 10
```

Configure Eth2/0/0 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 ethernet 2/0/0
[Huawei-Ethernet2/0/0] igmp-snooping group-limit 50 vlan 20 to 30
```

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

10.9.8 igmp-snooping enable (system view)
10.9.9 igmp-snooping enable (VLAN view)

10.9.11 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 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 value is an integer ranging from 2000 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.	-

Copyright © Huawei Technologies Co., Ltd.

Views

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 user VLAN on the interface:

- If so, the Layer 2 device allows the hosts in the VLANs to join the group and forwards the Report messages.
- If not, the Layer 2 device prevents the hosts from joining the group and drops the Report messages.

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)** command.
- The ACL referenced in the policy exists and has filtering rules configured.

This command must reference an ACL. Before using this command, create an ACL and configure rules for the ACL. The ACL referenced in a group policy permits all multicast groups by default. Therefore, to allow interfaces in a VLAN to receive only multicast data sent to specific groups, use a **rule deny source any** rule with **permit** rules in the ACL. For details about ACL configuration commands, see **19.7 ACL Configuration Commands**.

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 VLAN 2 from joining multicast group 225.1.1.123.

```
<Huawei> system-view
[Huawei] acl number 2000
[Huawei-acl-basic-2000] rule deny source 225.1.1.123 0
```

 Copyright © Huawei Technologies Co., Ltd.

```
[Huawei-acl-basic-2000] quit
[Huawei] igmp-snooping enable
[Huawei] vlan 2
[Huawei-vlan2] igmp-snooping enable
[Huawei-vlan2] quit
[Huawei] interface ethernet 2/0/0
[Huawei-Ethernet2/0/0] igmp-snooping group-policy 2000 vlan 2
```

Related Topics

10.9.8 igmp-snooping enable (system view)
10.9.9 igmp-snooping enable (VLAN view)
10.9.12 igmp-snooping group-policy (VLAN view)
10.9.12 igmp-snooping group-policy (VLAN view)

10.9.12 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. A basic or advanced ACL can be used in a multicast group policy.	The value is an integer that ranges from 2000 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

Copyright © Huawei Technologies Co., Ltd.

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 router 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 router receives the message, it checks whether the multicast group matches the multicast group policy applied to the VLAN. If so, the router drops the Report message and prohibits the user from joining the multicast group. If not, the router forwards the message, allowing the user to join the multicast group.

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 VLAN using the **igmp-snooping enable (VLAN view)** command.
- The ACL referenced in the policy exists and has filtering rules configured.

This command must reference an ACL. Before using this command, create an ACL and configure rules for the ACL. The ACL referenced in a group policy permits all multicast groups by default. Therefore, to allow interfaces in a VLAN to receive only multicast data sent to specific groups, use a **rule deny source any** rule with **permit** rules in the ACL. For details about ACL configuration commands, see **19.7 ACL Configuration Commands**.

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
```

 Copyright © Huawei Technologies Co., Ltd.

```
[Huawei-vlan2] igmp-snooping enable
[Huawei-vlan2] igmp-snooping group-policy 2000
```

Related Topics

10.9.1 display igmp-snooping

10.9.2 display igmp-snooping configuration

10.9.8 igmp-snooping enable (system view)

10.9.9 igmp-snooping enable (VLAN view)

10.9.13 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:

Copyright © Huawei Technologies Co., Ltd.

- Configure the router 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 router receives an IGMP Leave message from a host, the router 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 router (querier) receives Report messages from other hosts within the aging time, it continues to maintain memberships of the multicast group. If the router 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 router 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
```

Related Topics

10.9.1 display igmp-snooping

10.9.2 display igmp-snooping configuration

10.9.8 igmp-snooping enable (system view)

10.9.9 igmp-snooping enable (VLAN view)

10.9.17 igmp-snooping querier enable

10.9.21 igmp-snooping robust-count

Copyright © Huawei Technologies Co., Ltd.

10.9.14 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>

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

Interface view

 Copyright © Huawei Technologies Co., Ltd.

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.

Example

Disable learning of group memberships in VLAN 3 and VLAN 4 on Eth2/0/0.

```
<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 ethernet 2/0/0
[Huawei-Ethernet2/0/0] port link-type trunk
[Huawei-Ethernet2/0/0] port trunk allow-pass vlan 3 to 4
[Huawei-Ethernet2/0/0] undo igmp-snooping learning vlan 3 to 4
```

Related Topics

10.9.8 igmp-snooping enable (system view)

10.9.9 igmp-snooping enable (VLAN view)

Copyright © Huawei Technologies Co., Ltd.

10.9.15 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 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 router 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

 Copyright © Huawei Technologies Co., Ltd.

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 router 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 router may 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
```

Related Topics

10.9.1 display igmp-snooping

10.9.2 display igmp-snooping configuration

10.9.8 igmp-snooping enable (system view)

10.9.9 igmp-snooping enable (VLAN view)

10.9.13 igmp-snooping lastmember-queryinterval

10.9.18 igmp-snooping query-interval

10.9.21 igmp-snooping robust-count

Copyright © Huawei Technologies Co., Ltd.

10.9.16 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 router 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

 Copyright © Huawei Technologies Co., Ltd.

resources because the router 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.
- An ACL has been created and has filtering rules configured if a multicast group policy is specified in the command. The default ACL rule of the router permits all multicast groups. Therefore, after configuring a rule that permits a specified multicast group, run the **rule deny source any** command to deny all the other multicast groups. For details about ACL configuration commands, see **19.7 ACL Configuration Commands** in "Security Commands."

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] rule deny source any
[Huawei-acl-basic-2000] quit
[Huawei] vlan 3
[Huawei-vlan3] igmp-snooping enable
[Huawei-vlan3] igmp-snooping prompt-leave group-policy 2000
```

Related Topics

10.9.1 display igmp-snooping

10.9.2 display igmp-snooping configuration

10.9.8 igmp-snooping enable (system view)

10.9.9 igmp-snooping enable (VLAN view)

Copyright © Huawei Technologies Co., Ltd.

10.9.17 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. You can enable IGMP snooping querier on the downstream Layer 2 device. Then the Layer 2 device can act as a querier to send IGMP Query messages.

On a Layer 2 network without 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.

Copyright © Huawei Technologies Co., Ltd.

- 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.

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
```

Related Topics

10.9.1 display igmp-snooping
10.9.2 display igmp-snooping configuration
10.9.4 display igmp-snooping querier
10.9.8 igmp-snooping enable (system view)
10.9.9 igmp-snooping enable (VLAN view)
10.9.13 igmp-snooping lastmember-queryinterval
10.9.21 igmp-snooping robust-count
10.9.18 igmp-snooping query-interval

10.9.18 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.

Copyright © Huawei Technologies Co., Ltd.

By default, the general query interval is 60 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 router to send IGMP General Query messages at intervals to maintain memberships of interfaces. When a shorter interval is configured, the router 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 router 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.

NOTE

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

Prerequisites

 Copyright © Huawei Technologies Co., Ltd.

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 router may 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
```

Related Topics

10.9.1 display igmp-snooping
10.9.2 display igmp-snooping configuration
10.9.8 igmp-snooping enable (system view)
10.9.9 igmp-snooping enable (VLAN view)
10.9.15 igmp-snooping max-response-time
10.9.17 igmp-snooping querier enable
10.9.21 igmp-snooping robust-count

10.9.19 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

Copyright © Huawei Technologies Co., Ltd.

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 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.
- 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 device can suppress duplicate Report messages even when IGMP message suppression is disabled. The default suppression time is 10 seconds. To change

 Copyright © Huawei Technologies Co., Ltd.

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.

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
```

Related Topics

10.9.1 display igmp-snooping

10.9.8 igmp-snooping enable (system view)

10.9.9 igmp-snooping enable (VLAN view)

10.9.17 igmp-snooping querier enable

10.9.31 igmp-snooping suppress-time

10.9.20 igmp-snooping require-router-alert

Function

The **igmp-snooping require-router-alert** command configures the router 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 router 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

Copyright © Huawei Technologies Co., Ltd.

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 router does not check whether IGMP messages contain the Router-Alert option and sends all the IGMP messages to the upper-layer routing protocol. Discarding IGMP messages without the Router-Alert option improves device performance, reduces cost, and enhances security of the upper-layer routing protocol. After the **igmp-snooping require-router-alert** command is executed, the router checks each IGMP message for the Router-Alert option and discards those IGMP messages without this option.

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 router 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
```

Related Topics

10.9.1 display igmp-snooping

10.9.2 display igmp-snooping configuration

10.9.8 igmp-snooping enable (system view)

10.9.9 igmp-snooping enable (VLAN view)

10.9.21 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.

Copyright © Huawei Technologies Co., Ltd.

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 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 router sends a Group-Specific Query message certain 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 router 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.

 Copyright © Huawei Technologies Co., Ltd.

- 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
```

Related Topics

10.9.1 display igmp-snooping
10.9.2 display igmp-snooping configuration
10.9.8 igmp-snooping enable (system view)
10.9.9 igmp-snooping enable (VLAN view)
10.9.13 igmp-snooping lastmember-queryinterval
10.9.15 igmp-snooping max-response-time
10.9.18 igmp-snooping query-interval

10.9.22 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

Copyright © Huawei Technologies Co., Ltd.

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 router. If a router port on the router ages in this period, the router 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 on an unstable network.

When a dynamic router port on the router receives an IGMP Query message or a PIM Hello message, the router resets the aging time of the router port.

- If the router port receives an IGMP Query message, the router sets the remaining aging time of the interface to the configured value.
- If the router port receives a PIM Hello message and the holdtime value in the Hello message is larger than the remaining aging time of the router port, the router sets the aging time of the interface to the holdtime value. If the holdtime value is smaller than the remaining aging time of the router port, the router does not change the aging time of the router port.

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.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> system-view
[Huawei] igmp-snooping enable
[Huawei] vlan 3
[Huawei-vlan3] igmp-snooping enable
[Huawei-vlan3] igmp-snooping router-aging-time 300
```

Related Topics

10.9.1 display igmp-snooping

10.9.2 display igmp-snooping configuration

10.9.8 igmp-snooping enable (system view)

10.9.9 igmp-snooping enable (VLAN view)

10.9.23 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 router 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 router 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:

Copyright © Huawei Technologies Co., Ltd.

- 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 router does not listen on IGMP Query 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.

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
```

Related Topics

10.9.1 display igmp-snooping
10.9.2 display igmp-snooping configuration
10.9.8 igmp-snooping enable (system view)
10.9.9 igmp-snooping enable (VLAN view)
10.9.30 igmp-snooping static-router-port

10.9.24 igmp-snooping send-query enable

Function

The **igmp-snooping send-query enable** command enables the router 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 router from sending IGMP General Query messages to non-router ports.

By default, the router does not send IGMP General Query messages to non-router ports when receiving topology change events.

 Copyright © Huawei Technologies Co., Ltd.

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 router receives a topology change event. By default, the router does not send IGMP General Query messages in this case. A network topology change triggers recalculation of the Multiple Spanning Tree Protocol (MSTP), 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 router 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 router 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 set the source IP address to 0.0.0.0.

Precautions

Use this command only when MSTP is enabled on the network.

Example

Configure the router to send IGMP General Query messages upon topology changes.

```
<Huawei> system-view
[Huawei] igmp-snooping enable
[Huawei] igmp-snooping send-query enable
```

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

10.9.6 display igmp-snooping statistics
10.9.8 igmp-snooping enable (system view)
10.9.25 igmp-snooping send-query source-address

10.9.25 igmp-snooping send-query source-address

Function

The **igmp-snooping send-query source-address** command sets the source IP address of IGMP General Query messages.

The **undo igmp-snooping send-query source-address** command restores the default source IP address of IGMP General Query messages.

By default, the source IP address of IGMP General 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 General Query messages.	The value is in dotted decimal notation.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

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 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 General 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

 Copyright © Huawei Technologies Co., Ltd.

the network, run the **igmp-snooping send-query source-address** command to change the source IP address of IGMP General 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.

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 router to 192.168.0.2.

```
<Huawei> system-view
[Huawei] igmp-snooping enable
[Huawei] igmp-snooping send-query source-address 192.168.0.2
```

Related Topics

10.9.8 igmp-snooping enable (system view)

10.9.17 igmp-snooping querier enable

10.9.24 igmp-snooping send-query enable

10.9.26 igmp-snooping send-router-alert

Function

The **igmp-snooping send-router-alert** command configures the router 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 router to send IGMP messages without the Router-Alert option in the IP header to a VLAN.

By default, the router 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

 Copyright © Huawei Technologies Co., Ltd.

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 router sends IGMP messages with the Router-Alert option. If some devices in the same VLAN as the router can process only the IGMP messages without the Router-Alert option, use the **undo igmp-snooping send-router-alert** command to configure the router to send IGMP messages without the Router-Alert option.

The router 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 router 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
```

Related Topics

10.9.1 display igmp-snooping

10.9.2 display igmp-snooping configuration

10.9.8 igmp-snooping enable (system view)

10.9.9 igmp-snooping enable (VLAN view)

10.9.27 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.

Copyright © Huawei Technologies Co., Ltd.

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.
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

 Copyright © Huawei Technologies Co., Ltd.

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
```

Related Topics

10.9.8 igmp-snooping enable (system view)

10.9.9 igmp-snooping enable (VLAN view)

10.9.28 igmp-snooping ssm-mapping enable

10.9.29 igmp-snooping ssm-policy

10.9.32 igmp-snooping version

10.9.28 igmp-snooping ssm-mapping enable

Function

The **igmp-snooping ssm-mapping enable** command enables Source-Specific Multicast (SSM) mapping in a VLAN.

Copyright © Huawei Technologies Co., Ltd.

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.

 Copyright © Huawei Technologies Co., Ltd.

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
```

Related Topics

10.9.8 igmp-snooping enable (system view)
10.9.9 igmp-snooping enable (VLAN view)
10.9.27 igmp-snooping ssm-mapping
10.9.29 igmp-snooping ssm-policy
10.9.32 igmp-snooping version

10.9.29 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

Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

Usage Scenario

SSM allows multicast group addresses in the range of 232.0.0.0 to 232.255.255.255. If hosts 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.

Follow-up Procedure

Enable SSM mapping and configure SSM mapping in the VLAN. The multicast group in the SSM mapping must be in the SSM group range.

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.

This command must reference an ACL. Before using this command, create an ACL and configure 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 **19.7 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-policy 2000
```

Related Topics

10.9.8 igmp-snooping enable (system view)

10.9.9 igmp-snooping enable (VLAN view)

10.9.27 igmp-snooping ssm-mapping

10.9.28 igmp-snooping ssm-mapping enable

10.9.30 igmp-snooping static-router-port

Function

The **igmp-snooping static-router-port** command configures an interface as a static router port in specified VLANs.

Copyright © Huawei Technologies Co., Ltd.

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.
all	Cancels the static router port configuration in all VLANs on the interface.	-

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When an interface needs to forward IGMP Report/Leave messages for a long time, configure the interface as a static router port.

Prerequisites

 Copyright © Huawei Technologies Co., Ltd.

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.

Example

Configure Eth2/0/0 as a static router port in VLAN 2.

```
<Huawei> system-view
[Huawei] igmp-snooping enable
[Huawei] interface ethernet 2/0/0
[Huawei-Ethernet2/0/0] igmp-snooping static-router-port vlan 2
```

Related Topics

10.9.5 display igmp-snooping router-port

10.9.8 igmp-snooping enable (system view)

10.9.31 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

Copyright © Huawei Technologies Co., Ltd.

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 protects 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 receiving 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
```

Related Topics

10.9.1 display igmp-snooping
10.9.2 display igmp-snooping configuration
10.9.8 igmp-snooping enable (system view)
10.9.9 igmp-snooping enable (VLAN view)

 Copyright © Huawei Technologies Co., Ltd.

10.9.15 igmp-snooping max-response-time

10.9.32 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, IGMP snooping can process IGMPv1 and IGMPv2 messages in a VLAN.

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 VLAN.	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

VLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

 Copyright © Huawei Technologies Co., Ltd.

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.

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 message version is changed from IGMPv3 to IGMPv2, the system deletes all the dynamic IGMP snooping entries when the aging time is reached and processes static IGMP snooping entries as follows:

- Does not delete static entries that have only multicast groups but not 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 VLAN 2.

```
<Huawei> system-view
[Huawei] igmp-snooping enable
[Huawei] vlan 2
[Huawei-vlan2] igmp-snooping enable
[Huawei-vlan2] igmp-snooping version 1
```

Related Topics

10.9.1 display igmp-snooping
10.9.2 display igmp-snooping configuration
10.9.8 igmp-snooping enable (system view)
10.9.9 igmp-snooping enable (VLAN view)

10.9.33 l2-multicast static-group

Function

The **l2-multicast static-group** command configures static group memberships on an interface.

 Copyright © Huawei Technologies Co., Ltd.

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.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
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).
vlan *vlan-id*	Specifies the VLANs that the interface belongs to.	The values of *vlan-id* are integers that range from 1 to 4094.

Views

Interface view

 Copyright © Huawei Technologies Co., Ltd.

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In addition to dynamic multicast forwarding entries generated by Layer 2 multicast protocol 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 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

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 reserved group address cannot be used as the static multicast group address.

Example

Configure a static multicast group 224.1.1.1 on Eth2/0/0 in VLAN 2.

```
<Huawei> system-view
[Huawei] igmp-snooping enable
[Huawei] interface ethernet 2/0/0
[Huawei-Ethernet2/0/0] port link-type trunk
[Huawei-Ethernet2/0/0] port trunk allow-pass vlan 2
[Huawei-Ethernet2/0/0] 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 Eth2/0/0 in VLAN 2.

```
<Huawei> system-view
[Huawei] igmp-snooping enable
[Huawei] interface ethernet 2/0/0
[Huawei-Ethernet2/0/0] port link-type trunk
[Huawei-Ethernet2/0/0] port trunk allow-pass vlan 2
[Huawei-Ethernet2/0/0] 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 Eth2/0/0 in all VLANs.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> system-view
[Huawei] interface ethernet 2/0/0
[Huawei-Ethernet2/0/0] undo l2-multicast static-group group-address 224.1.1.1 vlan all
```

Related Topics

10.9.3 display igmp-snooping port-info
10.9.7 display l2-multicast forwarding-table
10.9.8 igmp-snooping enable (system view)
10.9.9 igmp-snooping enable (VLAN view)
10.9.32 igmp-snooping version

10.9.34 multicast drop-unknown

Function

The **multicast drop-unknown** command configures the router to drop unknown multicast flows in a VLAN.

The **undo multicast drop-unknown** command restores the default measure taken for unknown multicast flows.

By default, the router broadcasts unknown multicast flows in a VLAN.

NOTE

AR129CV, AR129CVW, AR129CGVW-L, AR2204-24GE, AR2204-27GE, AR2204-27GE-P, AR2204E-D-27GE, AR2204-48GE-P, AR2204-51GE, AR2204-51GE-P, AR2204-51GE-R, AR2204E, AR2204E-D, AR2204XE, AR2204XE-DC, AR2220L, AR2220E and AR2240C do not support this command.

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 multicast data flows that match no entry in the multicast forwarding table. By default, the router broadcasts unknown multicast

 Copyright © Huawei Technologies Co., Ltd.

flows in the corresponding VLAN. You can use the **multicast drop-unknown** command to configure the router to drop unknown multicast flows, which reduces instant bandwidth usage compared with the broadcast mode.

Configuration Impact

After the **multicast drop-unknown** command is executed, all unknown multicast packets are dropped, including the protocol packets that are transparently transmitted within the VLAN and use the reserved multicast address.

Example

Drop unknown multicast flows in VLAN 10.

```
<Huawei> system-view
[Huawei] vlan 10
[Huawei-vlan10] multicast drop-unknown
```

10.9.35 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* } }

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.

Views

User view

Default Level

3: Management level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

Usage Scenario

When multicast groups on a network change, the router generates new Layer 2 multicast forwarding entries until the aging time of member ports expire. To enable the router 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 router 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
```

Related Topics

10.9.3 display igmp-snooping port-info

10.9.36 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.	-

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
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

3: Management 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
```

Related Topics

10.9.6 display igmp-snooping statistics

10.10 MLD Snooping Configuration Commands

NOTE

Only AR2200&AR3200&AR3600 series support MLD Snooping.

Only the 8FE1GE, 24GE and 24ES2GP cards support MLD Snooping.

Copyright © Huawei Technologies Co., Ltd.

10.10.1 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 the VLAN is in Up state (at least one interface in the VLAN is in Up state) and has MLD snooping enabled.

Copyright © Huawei Technologies Co., Ltd.

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 60
  MLD Max Response Interval is Set to default 10
  MLD Robustness is Set to default 2
  MLD Last Member Query Interval is Set to default 1
  MLD Router Port Aging Interval is Set to 180s or holdtime in hello
  MLD Filter Group-Policy is Set to default : Permit All
  MLD Prompt Leave Disable
  MLD Router Alert is Not Required
  MLD Send Router Alert Enable
  MLD Snooping Querier Disable
```

Table 10-120 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 60	Interval at which MLD General Query messages are sent. In this example, the default value (60 seconds) is displayed. This parameter is configured using the **mld-snooping query-interval** command.
MLD Max Response Interval is Set to default 10	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.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
MLD Last Member Query Interval is Set to default 1	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.
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 Set to default : Permit All	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 prompt leave function is disabled for interfaces in the VLAN (default configuration). The prompt leave function can be enabled using the **mld-snooping prompt-leave** command.
MLD Router Alert is Not Required	The router does not require that MLD messages received from the VLAN contain the Router-Alert option in the IP header (default configuration). The router 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 router sends MLD messages with the Router-Alert option to the VLAN (default configuration). The router can be configured to send MLD messages with the Router-Alert option using the **mld-snooping send-router-alert** command.
MLD Snooping Querier Disable	MLD snooping querier is disabled (default configuration). MLD snooping querier can be enabled using the **mld-snooping querier enable** command.

Related Topics

10.10.6 mld-snooping enable
10.10.8 mld-snooping group-policy (VLAN view)
10.10.9 mld-snooping last-listener-query-interval
10.10.10 mld-snooping max-response-time

 Copyright © Huawei Technologies Co., Ltd.

10.10.11 mld-snooping prompt-leave
10.10.12 mld-snooping querier enable
10.10.14 mld-snooping require-router-alert
10.10.15 mld-snooping robust-count
10.10.16 mld-snooping router-aging-time
10.10.19 mld-snooping send-router-alert
10.10.24 mld-snooping version

10.10.2 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

 Copyright © Huawei Technologies Co., Ltd.

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 10-121 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.

Related Topics

10.10.6 mld-snooping enable
10.10.8 mld-snooping group-policy (VLAN view)
10.10.9 mld-snooping last-listener-query-interval
10.10.10 mld-snooping max-response-time
10.10.11 mld-snooping prompt-leave
10.10.14 mld-snooping require-router-alert
10.10.15 mld-snooping robust-count
10.10.16 mld-snooping router-aging-time
10.10.19 mld-snooping send-router-alert
10.10.24 mld-snooping version

10.10.3 display mld-snooping port-info

Copyright © Huawei Technologies Co., Ltd.

Function

The **display mld-snooping port-info** command displays information about multicast group ports.

Format

display mld-snooping port-info [**vlan** *vlan-id* [**group** *ipv6-group-address* [**source-address** *ipv6-source-address*]]] [**verbose**]

Parameters

Parameter	Description	Value
vlan *vlan-id*	Displays multicast group ports in a specified VLAN. If this parameter is not specified, the system displays multicast group ports in all VLANs.	The value is an integer that ranges from 1 to 4094.
group *ipv6-group-address*	Displays member ports of a specified multicast group. If this parameter is not specified, the system displays 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.
source-address *ipv6-source-address*	Displays member ports of a specified multicast source.	The value is an IPv6 multicast address, which is a 32-digit hexadecimal number in X:X:X:X:X:X:X:X format.
verbose	Displays detailed information about multicast group ports. If this parameter is not specified, the system displays the summary of multicast group ports.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

 Copyright © Huawei Technologies Co., Ltd.

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 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 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 multicast group ports.

```
<Huawei> display mld-snooping port-info
 ------------------------------------------------------------------------------
                  (Source, Group)  Port                      Flag
 ------------------------------------------------------------------------------
VLAN 10, 1 Entry(s)
(             *, ff13:0:0:0:0:0:0:2)Eth2/0/0                 S--
                                    1 port(s)
 ------------------------------------------------------------------------------
```

Table 10-122 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 port.

Related Topics

10.10.6 mld-snooping enable

10.10.20 mld-snooping static-group

10.10.4 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*]

Copyright © Huawei Technologies Co., Ltd.

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 router 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
   Eth2/0/0             00:00:06       --             STATIC
```

 Copyright © Huawei Technologies Co., Ltd.

Table 10-123 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 does not age.
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

Related Topics

10.10.6 mld-snooping enable

10.10.21 mld-snooping static-router-port

10.10.5 display mld-snooping statistics

Function

The **display mld-snooping statistics** command displays MLD snooping statistics.

Format

display mld-snooping statistics [**vlan** *vlan-id*]

Copyright © Huawei Technologies Co., Ltd.

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, and 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
```

 Copyright © Huawei Technologies Co., Ltd.

```
  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
```

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
```

Table 10-124 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 MSTP blocking events.
Recv MSTP Forward Event Times	Number of MSTP forwarding events.
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.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
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.
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 ::.

Related Topics

10.10.6 mld-snooping enable

10.10.27 reset mld-snooping statistics

10.10.6 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

Copyright © Huawei Technologies Co., Ltd.

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*.
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 you run the **undo mld-snooping enable** command to disable global MLD snooping, all MLD snooping configurations on the router are deleted. After you run the **mld-snooping enable** command to enable global MLD snooping again, the router uses the default MLD snooping configuration.

Example

Enable global MLD snooping.

 Copyright © Huawei Technologies Co., Ltd.

```
<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
```

Related Topics

10.10.1 display mld-snooping

10.10.2 display mld-snooping configuration

10.10.7 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* [*mld-version*]

undo mld-snooping group-policy vlan *vlan-id* [*mld-version*]

Parameters

Parameter	Description	Value
acl6-number	Specifies the number of an IPv6 ACL that defines a range of multicast groups. A basic or advanced ACL can be used in an IPv6 multicast group policy.	The value is an integer that ranges from 2000 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.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
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

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 so, the Layer 2 device drops the Report message and prohibits the user from joining the multicast group. If not, the Layer 2 device forwards the message, allowing the user to join the multicast group.

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.

When configuring the ACL for a multicast group policy in a VLAN, set the action in the ACL rule to deny. That is, the policy only prohibits hosts in the VLAN from joining all or specified multicast groups. For details about ACL configuration commands, see **19.7 ACL Configuration Commands** in "Security Commands."

 Copyright © Huawei Technologies Co., Ltd.

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 Eth2/0/0 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 ethernet 2/0/0
[Huawei-Ethernet2/0/0] port link-type trunk
[Huawei-Ethernet2/0/0] port trunk allow-pass vlan 10
[Huawei-Ethernet2/0/0] mld-snooping group-policy 2000 vlan 10
```

Related Topics

10.10.1 display mld-snooping

10.10.2 display mld-snooping configuration

10.10.6 mld-snooping enable

10.10.8 mld-snooping group-policy (VLAN view)

10.10.8 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* [*mld-version*]

undo mld-snooping group-policy

Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
acl6-number	Specifies the number of an IPv6 ACL that defines a range of multicast groups. A basic or advanced ACL can be used in an IPv6 multicast group policy.	The value is an integer that ranges from 2000 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 so, the Layer 2 device drops the Report message and prohibits the user from joining the multicast group. If not, the Layer 2 device forwards the message, allowing the user to join the multicast group.

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.

 Copyright © Huawei Technologies Co., Ltd.

- The ACL specified in the command has been created and had filtering rules configured.

When configuring the ACL for a multicast group policy in a VLAN, set the action in the ACL rule to deny. That is, the policy only prohibits hosts in the VLAN from joining all or specified multicast groups. For details about ACL configuration commands, see **19.7 ACL Configuration Commands** in "Security Commands."

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
```

Related Topics

10.10.1 display mld-snooping

10.10.2 display mld-snooping configuration

10.10.6 mld-snooping enable

10.10.7 mld-snooping group-policy (interface view)

10.10.9 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

 Copyright © Huawei Technologies Co., Ltd.

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:

 Copyright © Huawei Technologies Co., Ltd.

- 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** 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
```

Related Topics

10.10.1 display mld-snooping

10.10.2 display mld-snooping configuration

10.10.6 mld-snooping enable

10.10.12 mld-snooping querier enable

10.10.15 mld-snooping robust-count

10.10.10 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.

Copyright © Huawei Technologies Co., Ltd.

Views

VLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Setting MLD snooping parameters helps improve multicast forwarding performance on the router. 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 router 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 router 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 router may delete multicast memberships that should not be deleted.

 Copyright © Huawei Technologies Co., Ltd.

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
```

Related Topics

10.10.1 display mld-snooping
10.10.2 display mld-snooping configuration
10.10.6 mld-snooping enable
10.10.9 mld-snooping last-listener-query-interval
10.10.13 mld-snooping query-interval
10.10.15 mld-snooping robust-count

10.10.11 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.

Copyright © Huawei Technologies Co., Ltd.

Views

VLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The fast leave function enables the router 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 router 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.
- An ACL has been created and has filtering rules configured if a multicast group policy is specified in the command. The default ACL rule permits all multicast groups. Therefore, after configuring a rule that permits a specified multicast group, run the **rule deny source any** command to deny all the other multicast groups. For details about ACL configuration commands, see **19.7 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] rule deny source any
[Huawei-acl6-basic-2000] quit
[Huawei] vlan 3
[Huawei-vlan3] mld-snooping enable
[Huawei-vlan3] mld-snooping prompt-leave group-policy 2000
```

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

10.10.1 display mld-snooping
10.10.2 display mld-snooping configuration
10.10.6 mld-snooping enable

10.10.12 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. Then the Layer 2 device can act as a querier to send MLD Query messages.

On a Layer 2 network without 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.

Copyright © Huawei Technologies Co., Ltd.

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.

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
```

Related Topics

10.10.1 display mld-snooping
10.10.2 display mld-snooping configuration
10.10.6 mld-snooping enable
10.10.9 mld-snooping last-listener-query-interval
10.10.13 mld-snooping query-interval
10.10.15 mld-snooping robust-count

10.10.13 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 60 seconds.

Copyright © Huawei Technologies Co., Ltd.

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. However, more bandwidth and resources are consumed in this case.
- Change the aging time of member ports.

  When receiving an MLD Report message from a host, the router 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.

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.

Copyright © Huawei Technologies Co., Ltd.

Use this command only when the router can send MLD Query message. The router can send MLD Query messages only 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 router may 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
```

Related Topics

10.10.1 display mld-snooping
10.10.2 display mld-snooping configuration
10.10.6 mld-snooping enable
10.10.10 mld-snooping max-response-time
10.10.12 mld-snooping querier enable
10.10.15 mld-snooping robust-count

10.10.14 mld-snooping require-router-alert

Function

The **mld-snooping require-router-alert** command configures the router 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 router 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

 Copyright © Huawei Technologies Co., Ltd.

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 router does not check whether MLD messages contain the Router-Alert option and sends all the MLD messages to the upper-layer routing protocol. Discarding MLD messages without the Router-Alert option improves device performance, reduces cost, and enhances security of the upper-layer routing protocol. After the **mld-snooping require-router-alert** command is executed, the router checks each MLD message for the Router-Alert option and discards those MLD messages without this option.

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 router 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
```

Related Topics

10.10.1 display mld-snooping

10.10.2 display mld-snooping configuration

10.10.6 mld-snooping enable

10.10.15 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.

Copyright © Huawei Technologies Co., Ltd.

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 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 certain 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 router 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.

 Copyright © Huawei Technologies Co., Ltd.

- 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
```

Related Topics

10.10.1 display mld-snooping
10.10.2 display mld-snooping configuration
10.10.6 mld-snooping enable
10.10.9 mld-snooping last-listener-query-interval
10.10.10 mld-snooping max-response-time
10.10.13 mld-snooping query-interval

10.10.16 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

Copyright © Huawei Technologies Co., Ltd.

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 on an unstable network.

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 and the Holdtime value in the Hello packet is larger than the remaining aging time of the router port, the Layer 2 device sets the aging time of the router port to the Holdtime value contained in the PIM Hello packet. If the Holdtime value in the Hello packet is smaller than the remaining aging time of the router port, the Layer 2 device does not reset the aging time of the router port.

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.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> system-view
[Huawei] mld-snooping enable
[Huawei] vlan 3
[Huawei-vlan3] mld-snooping enable
[Huawei-vlan3] mld-snooping router-aging-time 300
```

Related Topics

10.10.1 display mld-snooping

10.10.2 display mld-snooping configuration

10.10.6 mld-snooping enable

10.10.17 mld-snooping send-query enable

Function

The **mld-snooping send-query enable** command enables the router 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 router from sending MLD General Query messages when receiving Layer 2 topology change events.

By default, the router 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 router receives a topology change event. By default, the router does not send MLD General Query messages in this case. The network topology change triggers recalculation of the Multiple Spanning Tree Protocol (MSTP). If the router 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 router to

Copyright © Huawei Technologies Co., Ltd.

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 router sends MLD General Query messages with source IPv6 address FE80::0. 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 MSTP is enabled on the network.

Example

Enable the router 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
```

Related Topics

10.10.6 mld-snooping enable

10.10.18 mld-snooping send-query source-address

10.10.18 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

Copyright © Huawei Technologies Co., Ltd.

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, 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 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.

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
```

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

10.10.6 mld-snooping enable

10.10.12 mld-snooping querier enable

10.10.17 mld-snooping send-query enable

10.10.19 mld-snooping send-router-alert

Function

The **mld-snooping send-router-alert** command configures the router to send MLD messages with the Router-Alert option in the IP header to a VLAN.

The **undo mld-snooping send-router-alert** command configures the router to send MLD messages without the Router-Alert option to a VLAN.

By default, the MLD messages sent by the router 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 router sends MLD messages with the Router-Alert option. If some devices in the same VLAN as the router can process only the MLD messages without the Router-Alert option, use the **undo igmp-snooping send-router-alert** command to configure the router to send MLD messages without the Router-Alert option.

The router 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

 Copyright © Huawei Technologies Co., Ltd.

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 router to send MLD messages that do not contain the Router-Alert option in the IP 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
```

Related Topics

10.10.1 display mld-snooping

10.10.2 display mld-snooping configuration

10.10.6 mld-snooping enable

10.10.20 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.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
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

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 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.

 Copyright © Huawei Technologies Co., Ltd.

- The specified VLAN has been created and the interface has been added to the VLAN.

Example

Statically bind Eth2/0/0 in VLAN 2 to multicast group ff1a::1.

```
<Huawei> system-view
[Huawei] mld-snooping enable
[Huawei] interface ethernet 2/0/0
[Huawei-Ethernet2/0/0] port link-type trunk
[Huawei-Ethernet2/0/0] port trunk allow-pass vlan 2
[Huawei-Ethernet2/0/0] mld-snooping static-group ff1a::1 vlan 2
```

Related Topics

10.10.1 display mld-snooping
10.10.2 display mld-snooping configuration
10.10.6 mld-snooping enable
10.10.24 mld-snooping version

10.10.21 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.	-

Copyright © Huawei Technologies Co., Ltd.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When an interface needs to receive or forward multicast data packets in 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 Eth2/0/0 as a router port in VLAN 2.

```
<Huawei> system-view
[Huawei] mld-snooping enable
[Huawei] interface ethernet 2/0/0
[Huawei-Ethernet2/0/0] mld-snooping static-router-port vlan 2
```

Related Topics

10.10.4 display mld-snooping router-port

10.10.6 mld-snooping enable

10.10.22 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

Copyright © Huawei Technologies Co., Ltd.

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 loads 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 receiving 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.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> system-view
[Huawei] mld-snooping enable
[Huawei] mld-snooping suppression-time 15
```

Related Topics

10.10.1 display mld-snooping

10.10.2 display mld-snooping configuration

10.10.6 mld-snooping enable

10.10.23 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 maximum number of multicast entries that an interface can learn varies according to device models:

- AR2201-48FE, AR2202-48FE, AR2204-27GE, AR2204-27GE-P, AR2204-51GE-P, AR2204-51GE-R, AR2204E, AR2204E-D, and AR2204: 128
- AR2220, AR2240C, and AR2220E: 1000
- AR2204XE and AR2204XE-DC: 2000
- AR2240 and AR3200 series:
  - Configured with SRU40: 1000
  - Configured with SRU60: 1000
  - Configured with SRU80: 2000
  - Configured with SRU100E: 2000
  - Configured with SRU200: 2000
  - Configured with SRU200E: 2000
  - Configured with SRU400: 2000
- AR3600 series (SRUX5): 2000

Format

mld-snooping table limit *limit* **vlan** *vlan-id*

undo mld-snooping table limit vlan *vlan-id*

Copyright © Huawei Technologies Co., Ltd.

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 ranging from • 1 to 128 for the AR2201-48FE, AR2202-48FE, AR2204-27GE, AR2204-27GE-P, AR2204-51GE-P, AR2204-51GE-R, AR2204E, AR2204E-D, and AR2204 • 1 to 1000 for the AR2220, AR2240C, and AR2220E • AR2204XE and AR2204XE-DC: 1 to 2000 • AR2240 and AR3200 series (depending on the SRU model used on the router): – Configured with SRU40: 1 to 1000 – Configured with SRU60: 1 to 1000 – Configured with SRU80: 1 to 2000 – Configured with SRU100: 1 to 2000 – Configured with SRU100E: 1 to 2000 – Configured with SRU200: 1 to 2000 – Configured with SRU200E: 1 to 2000 – Configured with SRU400: 1 to 2000 • 1 to 2000 for the AR3600 series (SRUX5)
vlan *vlan-id*	Specifies a VLAN ID.	The value is an integer ranging from 1 to 4094.

 Copyright © Huawei Technologies Co., Ltd.

Views

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

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 **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 Eth2/0/0 in VLAN 5 to 100. (Eth2/0/0 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 ethernet 2/0/0
[Huawei-Ethernet2/0/0] mld-snooping table limit 100 vlan 5
```

Related Topics

10.10.6 mld-snooping enable

10.10.24 mld-snooping version

Copyright © Huawei Technologies Co., Ltd.

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

 Copyright © Huawei Technologies Co., Ltd.

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

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
```

Related Topics

10.10.1 display mld-snooping

10.10.2 display mld-snooping configuration

10.10.6 mld-snooping enable

10.10.25 multicast drop-unknown

Function

The **multicast drop-unknown** command configures the router to drop unknown multicast flows in a VLAN.

The **undo multicast drop-unknown** command restores the default measure taken for unknown multicast flows.

By default, the router broadcasts unknown multicast flows in a VLAN.

NOTE

AR2204-24GE, AR2204-27GE, AR2204-27GE-P, AR2204E-D-27GE, AR2204-48GE-P, AR2204-51GE, AR2204-51GE-P, AR2204-51GE-R, AR2204E, AR2204E-D, AR2204XE, AR2204XE-DC, AR2220L, AR2220E and AR2240C do not support this command.

Format

multicast drop-unknown

undo multicast drop-unknown

Parameters

None

Views

VLAN view

Copyright © Huawei Technologies Co., Ltd.

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Unknown multicast flows are multicast data flows that match no entry in the multicast forwarding table. By default, the router broadcasts unknown multicast flows in the corresponding VLAN. You can use the **multicast drop-unknown** command to configure the router to drop unknown multicast flows, which reduces instant bandwidth usage compared with the broadcast mode.

Configuration Impact

After the **multicast drop-unknown** command is executed, all unknown multicast packets are dropped, including the protocol packets that are transparently transmitted within the VLAN and use the reserved multicast address.

Example

Drop unknown multicast flows in VLAN 10.

```
<Huawei> system-view
[Huawei] vlan 10
[Huawei-vlan10] multicast drop-unknown
```

10.10.26 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* }

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.

Views

User view

 Copyright © Huawei Technologies Co., Ltd.

Default Level

3: Management level

Usage Guidelines

Usage Scenario

When multicast groups change on a network, the router generates new Layer 2 multicast forwarding entries until the aging time of member ports expire. To enable the router 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 router 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
```

Related Topics

10.10.3 display mld-snooping port-info

10.10.27 reset mld-snooping statistics

Function

The **reset mld-snooping statistics** command clears MLD snooping statistics.

Format

reset mld-snooping statistics [**vlan** *vlan-id*]

Copyright © Huawei Technologies Co., Ltd.

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

3: Management 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
```

Related Topics

10.10.5 display mld-snooping statistics

10.11 Multicast Network Management Commands

10.11.1 display pim mib-control-message

Function

The **display pim mib-control-message counters** command displays the number of neighbor loss events, the number of times for DR election, the number of

Copyright © Huawei Technologies Co., Ltd.

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 invalid Join/Prune message that is received at the last time.

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 invalid Register message that is received at the last time.

Format

display pim mib-control-message { **counters** | **join-prune** | **assert** | **register** }

Parameters

Parameter	Description	Value
counters	Indicates related PIM counters.	-
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

None

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 changes, 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
```

 Copyright © Huawei Technologies Co., Ltd.

```
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 GigabitEthernet1/0/0
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 10-125 Description of the **display pim mib-control-message** command output

Item	Description
pim mib-control-message counters	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 changes, and the number of received and sent Assert messages.
The last invalid join-prune message received information	Display the invalid Join/Prune message that is received at the last time
The last assert message received or sent on GigabitEthernet1/0/0	Display the Assert message that is sent or received at the last time
The last invalid register message received information	Display the invalid Register message that is received at the last time
Neighbor-loss(times)	The number of neighbor loss events
DR-Election (times)	The number of times for DR election
Invalid-join-prune(times)	The number of invalid Join/Prune messages
RP-Mapping(times)	The number of RP-mapping changes

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Invalid-register(times)	The number of invalid Register messages
Assert-received(times)	The number of received Assert messages
Assert-send(times)	The number of sent Assert messages
Group address	Multicast group address
Source address	Multicast source address
RP address	RP address

10.11.2 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

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
```


Copyright © Huawei Technologies Co., Ltd.

```
New-neighbor notification interval      : 0 s
Mrt-limit notification interval         : never
```

Table 10-126 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.

10.11.3 display snmp-agent trap feature-name igmp all

Function

The **display snmp-agent trap feature-name igmp all** command displays whether the trap function is enabled for the IGMP module.

Format

display snmp-agent trap feature-name igmp all

Parameters

None

Views

All views

 Copyright © Huawei Technologies Co., Ltd.

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display snmp-agent trap feature-name igmp all** command to view the status of all IGMP traps when you want to monitor the current status of IGMP protocol events but are not sure whether the IGMP trap function is enabled.

Example

Display whether the trap function is enabled for the IGMP module.

```
<Huawei> display snmp-agent trap feature-name igmp all
------------------------------------------------------------------------------
Feature name: IGMP
Trap number : 18
------------------------------------------------------------------------------
Trap name                      Default switch status   Current switch status
IFLIMIT                       off                     off
IFLIMITCLR                     off                     off
INSLIMIT                      off                     off
GLBLIMIT                       off                     off
HWMGMDGMPGLOBALLIMITCLEAR      off                     off
HWMGMDGMPTOTALLIMITCLEAR       off                     off
JOINGRP                        off                     off
LEAVEGRP                       off                     off

hwMgmdTotalLimitThresholdExceed
                               off                     off
hwMgmdTotalLimitThresholdExceedClear
                               off                     off
hwMgmdHostStarGThresholdExceed  off                     off
hwMgmdHostStarGThresholdExceedClear
                               off                     off
hwMgmdHostStarGExceed          off                     off
hwMgmdHostStarGExceedClear     off                     off
hwMgmdHostSGThresholdExceed    off                     off
hwMgmdHostSGThresholdExceedClear
                               off                     off
hwMgmdHostSGExceed             off                     off
hwMgmdHostSGExceedClear        off                     off
```

Table 10-127 Description of the **display snmp-agent trap feature-name igmp all** command output

Item	Description
Feature name	Name of the module.
Trap number	Number of trap event types.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Trap name	Trap event type. The following types of trap events are defined: • IFLIMIT: The number of IGMP entries on an interface reaches the limit. • IFLIMITCLR: The number of IGMP entries on an interface falls below the limit. • INSLIMIT: The number of IGMP entries in an instance reaches the limit. • GLBLIMIT: The total number of the entries in all instances reaches the limit. • HWMGMDGMPGLOBALLIMITCLEAR: The number of IGMP entries in a single instance falls below the limit. • HWMGMDGMPTOTALLIMITCLEAR: The number of IGMP entries in all instances falls below the limit. • JOINGRP: An IGMP Join message is received. • LEAVEGRP: An IGMP Leave message is received or the group timer expires. • hwMgmdTotalLimitThresholdExceed: a trap message indicating that the proportion of global IGMP/MLD entries created to the maximum global IGMP/MLD entries allowed reaches the upper alarm threshold. • hwMgmdTotalLimitThresholdExceed-Clear: a trap message indicating that the proportion of global IGMP/MLD entries created to the maximum global IGMP/MLD entries allowed falls below the lower alarm threshold. • hwMgmdHostStarGThresholdExceed: a trap message indicating that the total number of (*, G) entries of all instances reaches the specified upper alarm threshold. • hwMgmdHostStarGThresholdExceed-Clear: a trap message indicating that the total number of (*, G) entries of all instances falls below the specified lower alarm threshold. • hwMgmdHostStarGExceed: a trap message indicating that the total

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
	number of (*, G) entries of all instances exceeds the maximum number allowed on the user-side IGMP/MLD device. • hwMgmdHostStarGExceedClear: a trap message indicating that the total number of (*, G) entries of all instances falls below the maximum number allowed on the user-side IGMP/MLD device. • hwMgmdHostSGThresholdExceed: a trap message indicating that the total number of (S, G) entries of all instances reaches the specified upper alarm threshold. • hwMgmdHostSGThresholdExceed-Clear: a trap message indicating that the total number of (S, G) entries of all instances falls below the specified lower alarm threshold. • hwMgmdHostSGExceed: a trap message indicating that the total number of (S, G) entries of all instances exceeded the maximum number allowed on the user-side IGMP/MLD device. • hwMgmdHostSGExceedClear: a trap message indicating that the total number of (S, G) entries of all instances falls below the maximum number allowed on the user-side IGMP/MLD device.
Default switch status	Default status of a trap function: • on: indicates that the trap function is enabled by default. • off: indicates that the trap function is disabled by default.
Current switch status	Current status of a trap function: • on: indicates that the trap function is enabled. • off: indicates that the trap function is disabled.

Related Topics

10.11.17 snmp-agent trap enable feature-name igmp

 Copyright © Huawei Technologies Co., Ltd.

10.11.4 display snmp-agent trap feature-name mld all

Function

The **display snmp-agent trap feature-name mld all** command displays whether the trap function is enabled for the MLD module.

Format

display snmp-agent trap feature-name mld all

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

You can run the **display snmp-agent trap feature-name mld all** command to view the status of all MLD traps when you want to monitor the current status of MLD protocol events but are not sure whether the MLD trap function is enabled.

Example

Display whether the trap function is enabled for the MLD module.

```
<Huawei> display snmp-agent trap feature-name mld all
------------------------------------------------------------------------------
Feature name: MLD
Trap number : 8
------------------------------------------------------------------------------
Trap name                      Default switch status   Current switch status
IFLIMIT                        off                     off
IFLIMITCLR                     off                     off
INSLIMIT                       off                     off
GLBLIMIT                       off                     off
HWMGMDGMPGLOBALLIMITCLEAR      off                     off
HWMGMDGMPTOTALLIMITCLEAR       off                     off
JOINGRP                        off                     off
LEAVEGRP                       off                     off
```

Table 10-128 Description of the **display snmp-agent trap feature-name mld all** command output

Item	Description
Feature name	Name of the module

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Trap number	Number of trap messages of a specific type
Trap name	Types of trap messages: • IFLIMIT: a trap message indicating that the number of MLD entries on the interface reaches the limit value. • IFLIMITCLR: the number of MLD entries on an interface falls below the limit value. • INSLIMIT: a trap message indicating that the number of MLD entries in the instance reaches the limit value. • GLBLIMIT: a trap message indicating that the total number of MLD entries of all instances reaches the limit value. • HWMGMDGMPGLOBALLIMITCLEAR: a trap message indicates that the number of MLD entries in an instance has fallen below the limit. • HWMGMDGMPTOTALLIMITCLEAR: a trap message indicating that the total number of MLD entries in all instances has fallen below the limit. • JOINGRP: a trap message indicating that a MLD Join message is received • LEAVEGRP: a trap message indicating that a MLD Leave message is received or the group timer expires
Default switch status	Status of the default trap switch: • on: indicates that the trap function is enabled. • off: indicates that the trap function is disabled.
Current switch status	Status of the current trap switch: • on: indicates that the trap function is enabled. • off: indicates that the trap function is disabled.

Related Topics

10.11.18 snmp-agent trap enable feature-name mld

 Copyright © Huawei Technologies Co., Ltd.

10.11.5 display snmp-agent trap feature-name mrm all

Function

The **display snmp-agent trap feature-name mrm all** command displays whether the trap function is enabled for the MRM module.

Format

display snmp-agent trap feature-name mrm all

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display snmp-agent trap feature-name mrm all** command to view the status of all MRM traps when you want to monitor the current status of MRM protocol events but are not sure whether the MRM trap function is enabled.

Example

Display whether the trap function is enabled for the MRM module.

```
<Huawei> display snmp-agent trap feature-name mrm all
------------------------------------------------------------------------------
Feature name: MRM
Trap number : 4
------------------------------------------------------------------------------
Trap name                     Default switch status   Current switch status
hwIpMcastSGThresholdExceed      off                       off
hwIpMcastSGThresholdExceedClear
                              off                     off
hwIpMcastSGExceed             off                   off
hwIpMcastSGExceedClear          off                     off
```

Table 10-129 Description of the **display snmp-agent trap feature-name mrm all** command output

Item	Description
Feature name	Name of the module.
Trap number	Number of trap event types.

Copyright © Huawei Technologies Co., Ltd.

Item	Description
Trap name	Trap event type. The following types of trap events are defined: • hwIpMcastSGThresholdExceed: The proportion of (S, G) multicast forwarding entries created to the maximum (S, G) multicast forwarding entries allowed exceeds the upper alarm threshold. • hwIpMcastSGThresholdExceedClear: The proportion of (S, G) multicast forwarding entries created to the maximum (S, G) multicast forwarding entries allowed falls below the lower alarm threshold. • hwIpMcastSGExceed: The number of (S, G) multicast forwarding entries created exceeds the maximum number of (S, G) multicast forwarding entries allowed. • hwIpMcastSGExceedClear: The number of (S, G) multicast forwarding entries created falls below the maximum number of (S, G) multicast forwarding entries allowed.
Default switch status	Default status of a trap function: • on: indicates that the trap function is enabled by default. • off: indicates that the trap function is disabled by default.
Current switch status	Current status of a trap function: • on: indicates that the trap function is enabled. • off: indicates that the trap function is disabled.

Related Topics

10.11.19 snmp-agent trap enable feature-name mrm

10.11.6 display snmp-agent trap feature-name msdp all

Function

The **display snmp-agent trap feature-name msdp all** command displays the status of all MSDP traps.

Format

display snmp-agent trap feature-name msdp all

Copyright © Huawei Technologies Co., Ltd.

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

You can run the **display snmp-agent trap feature-name msdp all** command to view the status of all MSDP traps when you want to monitor the current status of MSDP protocol events but are not sure whether the MSDP trap function is enabled.

Example

Display whether the trap function is enabled for the MSDP module.

```
<Huawei> display snmp-agent trap feature-name msdp all
------------------------------------------------------------------------------
Feature name: MSDP
Trap number : 2
------------------------------------------------------------------------------
Trap name                Default switch status   Current switch status
establish                off                     off
backward                 off                     off
```

Table 10-130 Description of the display snmp-agent trap feature-name msdp all command output

Item	Description
Feature name	Indicates the name of the module.
Trap number	Indicates the type number of a trap.
Trap name	Indicates the event type. The event types are as follows: • establish: indicates that an MSDP peer is established. • backward: indicates that an MSDP peer is removed.
Default switch status	Status of the default trap switch: • on: indicates that the trap function is enabled. • off: indicates that the trap function is disabled.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Current switch status	Status of the current trap switch: • on: indicates that the trap function is enabled. • off: indicates that the trap function is disabled.

Related Topics

10.11.20 snmp-agent trap enable feature-name msdp

10.11.7 display snmp-agent trap feature-name pim all

Function

The **display snmp-agent trap feature-name pim all** command displays the status of all PIM traps.

Format

display snmp-agent trap feature-name pim all

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display snmp-agent trap feature-name pim all** command to view the status of all PIM traps when you want to monitor the current status of PIM protocol events but are not sure whether the PIM trap function is enabled.

Example

Display whether the trap function is enabled for the PIM module.

```
<Huawei> display snmp-agent trap feature-name pim all
------------------------------------------------------------------------------
Feature name: PIM
Trap number : 16
------------------------------------------------------------------------------
Trap name                     Default switch status   Current switch status
neighbor-loss                 off                     on
```

 Copyright © Huawei Technologies Co., Ltd.

```
invalid-register                off                    on
invalid-join-prune              off                    on
rp-mapping-change               off                    on
interface-election              off                    on
new-neighbor                    off                    on
mrt-limit                       off                    on
HWPIMMRTLIMITCLEAR              off                    on
hwPimStarGThresholdExceed       off                    on
hwPimSGThresholdExceed          off                    on
hwPimStarGExceed                off                    on
hwPimSGExceed                   off                    on
hwPimStarGThresholdExceedClear  off                    on
hwPimSGThresholdExceedClear     off                    on
hwPimStarGExceedClear           off                    on
hwPimSGExceedClear              off                    on
```

Table 10-131 Description of the **display snmp-agent trap feature-name pim all** command output

Item	Description
Feature name	Name of the module.
Trap number	Number of trap event types.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Trap name	Trap event type. The following types of trap events are defined: • neighbor-loss: A neighbor is lost. • invalid-register: An invalid Register message is received. • invalid-join-prune: An invalid Join/Prune message is received. • rp-mapping-change: The RP-mapping changes. • interface-election: An interface is elected as the DR. • new-neighbor: A new neighbor appears. • mrt-limit: The number of PIM entries exceeds the limit for the multicast routing table (MRT). • HWPIMMRTLIMITCLEAR: The total number of PIM entries falls below the limit. • hwPimStarGThresholdExceed: The proportion of PIM (*, G) entries created to the maximum PIM (*, G) entries allowed exceeds the upper alarm threshold. • hwPimSGThresholdExceed: The proportion of PIM (S, G) entries created to the maximum PIM (S, G) entries allowed exceeds the upper alarm threshold. • hwPimStarGExceed: The number of PIM (*, G) entries created exceeds the maximum number of PIM (*, G) entries allowed. • hwPimSGExceed: The number of PIM (S, G) entries created exceeds the maximum number of PIM (S, G) entries allowed. • hwPimStarGThresholdExceedClear: The proportion of PIM (*, G) entries created to the maximum PIM (*, G) entries allowed falls below the lower alarm threshold. • hwPimSGThresholdExceedClear: The proportion of PIM (S, G) entries created to the maximum PIM (S, G)

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
	entries allowed falls below the lower alarm threshold. • hwPimStarGExceedClear: The number of PIM (*, G) entries created falls below the maximum number of PIM (*, G) entries allowed. • hwPimSGExceedClear: The number of PIM (S, G) entries created falls below the maximum number of PIM (S, G) entries allowed.
Default switch status	Default status of a trap function: • on: indicates that the trap function is enabled by default. • off: indicates that the trap function is disabled by default.
Current switch status	Current status of a trap function: • on: indicates that the trap function is enabled. • off: indicates that the trap function is disabled.

Related Topics

10.11.21 snmp-agent trap enable feature-name pim

10.11.8 display snmp-agent trap feature-name pim-std all

Function

The **display snmp-agent trap feature-name pim-std all** command displays the status of all PIM-STD traps.

Format

display snmp-agent trap feature-name pim-std all

Parameters

None

Views

All views

Copyright © Huawei Technologies Co., Ltd.

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

You can run the **display snmp-agent trap feature-name pim-std all** command to view the status of all PIM-STD MIB traps when you want to monitor the current status of the public PIM protocol events but are not sure whether the PIM-STD MIB trap function is enabled.

Example

View the status of all PIM-STD MIB traps.

```
<Huawei> display snmp-agent trap feature-name pim-std all
------------------------------------------------------------------------------
Feature name: pim-std
Trap number : 5
------------------------------------------------------------------------------
Trap name                     Default switch status   Current switch status
pimneighborloss                 off                       on
piminvalidregister              off                       on
piminvalidjoinprune             off                       on
pimrpmappingchange                off                       on
piminterfaceelection            off                       on
```

Table 10-132 Description of the display snmp-agent trap feature-name pim-std all command output

Item	Description
Feature name	Feature name
Trap number	Number of trap message types
Trap name	Types of trap messages: • pimneighborloss: A neighbor relationship is lost. • piminvalidregister: An invalid Register message is received. • piminvalidjoinprune: An invalid Join or Prune message is received. • pimrpmappingchange: RP-Mapping changes. • piminterfaceelection: The interface is elected as the DR.
Default switch status	Default status of the trap function: • on: The trap function is enabled. • off: The trap function is disabled.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Current switch status	Current status of the trap function: • on: The trap function is enabled. • off: The trap function is disabled.

Related Topics

10.11.22 snmp-agent trap enable feature-name pim-std

10.11.9 igmp trap-interval limit

Function

The **igmp trap-interval limit** command configures the interval for sending trap messages of the failure of IGMP joining because the number of the IGMP entries exceeds the limit.

The **undo igmp trap-interval limit** command deletes the interval for sending trap messages of the failure of IGMP joining because the number of the IGMP entries exceeds the limit. When the joining failure event occurs, a trap message is sent immediately.

By default, the interval for sending trap messages of the failure of IGMP joining because the number of the IGMP entries exceeds the limit is not limited

Format

igmp trap-interval limit *min-interval*

undo igmp trap-interval limit

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

Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

When the interval is configured to 0 by using the **igmp trap-interval limit** command, the interval for IGMP to send trap messages of the failure of IGMP joining because the number of the IGMP entries exceeds the limit is not limited; otherwise, the interval for sending trap messages of the failure of IGMP joining because the number of the IGMP entries exceeds the limit should be equal to or longer than the configured one.

Example

Set the interval for sending trap messages of the failure of IGMP joining 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
```

10.11.10 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

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

Copyright © Huawei Technologies Co., Ltd.

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 help you learn IGMP/MLD entry usage in a timely manner. 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
```

10.11.11 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.

 Copyright © Huawei Technologies Co., Ltd.

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**

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 facilitate 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 run:

- 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

 Copyright © Huawei Technologies Co., Ltd.

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 one configures the upper and lower alarm thresholds, while the latter one 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
```

10.11.12 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

 Copyright © Huawei Technologies Co., Ltd.

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 operation and maintenance, configure the upper and lower alarm thresholds for multicast forwarding entries. Multicast forwarding entry alarms and clear alarms help you learn IGMP/MLD entry usage in a timely manner. 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

 Copyright © Huawei Technologies Co., Ltd.

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
```

10.11.13 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

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

None

 Copyright © Huawei Technologies Co., Ltd.

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
```

10.11.14 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

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

In 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.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> system-view
[Huawei] multicast-mib
[Huawei-mcast-mib]
```

10.11.15 pim mib-notification interval

Function

The **pim mib-notification interval** command sets the interval for PIM to send trap messages about various events.

The **undo pim mib-notification interval** command restores the default interval for PIM to send various trap messages.

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** }

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.
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.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
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.
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, if the period since the last time for sending the trap message is shorter than the configured interval, the system does not send any trap message.

- If the default interval is 0, it indicates that a trap message is sent immediately after an event occurs.
- If the default interval is 65535, it indicates that no trap message is sent after an event occurs. Then 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
```

 Copyright © Huawei Technologies Co., Ltd.

10.11.16 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**

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 operation and maintenance, configure the upper and lower alarm thresholds for PIM entries.

Copyright © Huawei Technologies Co., Ltd.

PIM entry alarms and clear alarms help you learn PIM entry usage in a timely manner. The **pim threshold-alarm** command allows you to flexibly 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
```

10.11.17 snmp-agent trap enable feature-name igmp

Function

The **snmp-agent trap enable feature-name igmp** command enables the trap function for the IGMP module.

The **undo snmp-agent trap enable feature-name igmp** command disables the trap function for the IGMP module.

By default, the trap function for IGMP events is disabled.

Format

snmp-agent trap enable feature-name igmp [**trap-name** { **glblimit** | **iflimit** | **iflimitclr** | **inslimit** | **joingrp** | **leavegrp** | **hwmgmdgmptotallimitclear** | **hwmgmdgmpgloballimitclear** | **hwmgmdtotallimitthresholdexceed** | **hwmgmdtotallimitthresholdexceedclear** | **hwmgmdhoststargthresholdexceed** | **hwmgmdhoststargthresholdexceedclear** | **hwmgmdhoststargexceed** | **hwmgmdhoststargexceedclear** | **hwmgmdhostsgthresholdexceed** |

 Copyright © Huawei Technologies Co., Ltd.

hwmgmdhostsgthresholdexceedclear | **hwmgmdhostsgexceed** | **hwmgmdhostsgexceedclear** }]

undo snmp-agent trap enable feature-name igmp [**trap-name** { **glblimit** | **iflimit** | **iflimitclr** | **inslimit** | **joingrp** | **leavegrp** | **hwmgmdgmptotallimitclear** | **hwmgmdgmpgloballimitclear** | **hwmgmdtotallimitthresholdexceed** | **hwmgmdtotallimitthresholdexceedclear** | **hwmgmdhoststargthresholdexceed** | **hwmgmdhoststargthresholdexceedclear** | **hwmgmdhoststargexceed** | **hwmgmdhoststargexceedclear** | **hwmgmdhostsgthresholdexceed** | **hwmgmdhostsgthresholdexceedclear** | **hwmgmdhostsgexceed** | **hwmgmdhostsgexceedclear** }]

Parameters

Parameter	Description	Value
trap-name	Enables the trap for a specified type of IGMP event.	-
glblimit	Enables the trap for the event indicating that the total number of the IGMP entries of all instances reaches the limit.	-
iflimit	Enables the trap for the event indicating that the number of IGMP entries on an interface reaches the limit.	-
iflimitclr	Enables the trap for the event indicating that the number of IGMP entries on an interface falls below the limit.	-
inslimit	Enables the trap for the event indicating that the number of IGMP entries in an instance reaches the limit.	-
joingrp	Enables the trap for the event indicating that an IGMP Join message is received.	-
leavegrp	Enables the trap for the event indicating that an IGMP Leave message is received or the group timer expires.	-
hwmgmdgmptotallimitclear	Enables the trap for the event indicating that the number of IGMP entries in all instances falls below the upper threshold.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
hwmgmdgmpgloballimitclear	Enables the trap for the event indicating that the number of IGMP entries a single instance falls below the upper threshold.	-
hwmgmdtotallimitthresholdexceed	Generates an alarm when the proportion of global IGMP/MLD entries created to the maximum global IGMP/MLD entries allowed reaches the upper alarm threshold.	-
hwmgmdtotallimitthresholdexceedclear	Generates a clear alarm when the proportion of global IGMP/MLD entries created to the maximum global IGMP/MLD entries allowed falls below the lower alarm threshold.	-
hwmgmdhoststargthresholdexceed	Generates an alarm when the (*, G) entry usage of all instances reaches the specified upper alarm threshold on the user-side IGMP/MLD device.	-
hwmgmdhoststargthresholdexceedclear	Generates a clear alarm when the (*, G) entry usage of all instances falls below the specified lower alarm threshold on the user-side IGMP/MLD device.	-
hwmgmdhoststargexceed	Generates an alarm when the number of (*, G) entries of all instances exceeds the maximum number allowed on the user-side IGMP/MLD device.	-
hwmgmdhoststargexceedclear	Generates a clear alarm when the number of (*, G) entries of all instances falls below the maximum number allowed on the user-side IGMP/MLD device.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
hwmgmdhostsgthresholdexceed	Generates an alarm when the (S, G) entry usage of all instances reaches the specified upper alarm threshold on the user-side IGMP/MLD device.	-
hwmgmdhostsgthresholdexceedclear	Generates a clear alarm when the (S, G) entry usage of all instances falls below the specified lower alarm threshold on the user-side IGMP/MLD device.	-
hwmgmdhostsgexceed	Generates an alarm when the number of (S, G) entries of all instances exceeds the maximum number allowed on the user-side IGMP/MLD device.	-
hwmgmdhostsgexceedclear	Generates a clear alarm when the number of (S, G) entries of all instances falls below the maximum number allowed on the user-side IGMP/MLD device.	-

Views

System view

Default Level

3: Management level

Usage Guidelines

To enable the trap function for a specific type of event, specify **trap-name**. To enable the trap function for multiple types of events, run this command multiple times.

Example

Enable the trap for the event indicating that an IGMP Join message is received.

```
<Huawei> system-view
[Huawei] snmp-agent trap enable feature-name igmp trap-name joingrp
```

Disable the trap for the event indicating that an IGMP Join message is received.

```
<Huawei> system-view
[Huawei] undo snmp-agent trap enable feature-name igmp trap-name joingrp
```

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

10.11.3 display snmp-agent trap feature-name igmp all

10.11.18 snmp-agent trap enable feature-name mld

Function

The **snmp-agent trap enable feature-name mld** command enables the trap function for the MLD module.

The **undo snmp-agent trap enable feature-name mld** command disables the trap function for the MLD module.

By default, the trap function for MLD events is disabled.

Format

snmp-agent trap enable feature-name mld [**trap-name** { **glblimit** | **iflimit** | **iflimitclr** | **inslimit** | **joingrp** | **leavegrp** | **hwmgmdgmptotallimitclear** | **hwmgmdgmpgloballimitclear** }]

undo snmp-agent trap enable feature-name mld [**trap-name** { **glblimit** | **iflimit** | **iflimitclr** | **inslimit** | **joingrp** | **leavegrp** | **hwmgmdgmptotallimitclear** | **hwmgmdgmpgloballimitclear** }]

Parameters

Parameter	Description	Value
trap-name	Enables the trap of MLD events of specified types.	-
glblimit	Enables the trap that the total number of the MLD entries of all instances reaches the limit value.	-
iflimit	Enables the trap that the number of MLD entries on an interface reaches the limit value.	-
iflimitclr	Enables the trap that the number of MLD entries on an interface falls below the limit value.	-
inslimit	Enables the trap that the number of MLD entries in an instance reaches the limit value.	-
joingrp	Enables the trap of the event that an MLD Join message is received.	-
leavegrp	Enables the trap of the event that an MLD Leave message is received or the group timer expires.	-

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
hwmgmdgmptotallimitclear	Generates an alarm when the number of MLD entries in all instances falls below the upper threshold.	-
hwmgmdgmpgloballimitclear	Generates an alarm when the number of MLD entries in a single instance falls below the upper threshold.	-

Views

System view

Default Level

3: Management level

Usage Guidelines

To enable the trap function of one or more types of trap messages, specify **trap-name**.

Example

Enable the trap of the event that an MLD Join message is received.

```
<Huawei> system-view
[Huawei] snmp-agent trap enable feature-name mld trap-name joingrp
```

Disable the trap of the event that an MLD Join message is received.

```
<Huawei> system-view
[Huawei] undo snmp-agent trap enable feature-name mld trap-name joingrp
```

Related Topics

10.11.4 display snmp-agent trap feature-name mld all

10.11.19 snmp-agent trap enable feature-name mrm

Function

The **snmp-agent trap enable feature-name mrm** command enables the trap function for the Multicast Routing Management (MRM) module.

The **undo snmp-agent trap enable feature-name mrm** command disables the trap function for the MRM module.

By default, the trap function for MRM events is disabled.

Format

snmp-agent trap enable feature-name mrm [**trap-name** { **hwipmcastsgexceed** | **hwipmcastsgexceedclear** | **hwipmcastsgthresholdexceed** | **hwipmcastsgthresholdexceedclear** }]

Copyright © Huawei Technologies Co., Ltd.

undo snmp-agent trap enable feature-name mrm [**trap-name** { **hwipmcastsgexceed** | **hwipmcastsgexceedclear** | **hwipmcastsgthresholdexceed** | **hwipmcastsgthresholdexceedclear** }]

Parameters

Parameter	Description	Value
trap-name	Enables the trap for a specified type of MRM event.	-
hwipmcastsgexceed	Enables the trap for the event indicating that the number of (S, G) multicast forwarding entries created exceeds the maximum number of (S, G) multicast forwarding entries allowed.	-
hwipmcastsgexceedclear	Enables the trap for the event indicating that the number of (S, G) multicast forwarding entries created falls below the maximum number of (S, G) multicast forwarding entries allowed.	-
hwipmcastsgthresholdexceed	Enables the trap for the event indicating that the proportion of (S, G) multicast forwarding entries created to the maximum (S, G) multicast forwarding entries allowed exceeds the upper alarm threshold.	-
hwipmcastsgthresholdexceedclear	Enables the trap for the event indicating that the proportion of (S, G) multicast forwarding entries created to the maximum (S, G) multicast forwarding entries allowed falls below the lower alarm threshold.	-

Views

System view

Default Level

3: Management level

Usage Guidelines

To enable the trap function for a specific type of event, specify **trap-name**. To enable the trap function for multiple types of events, run this command multiple times.

 Copyright © Huawei Technologies Co., Ltd.

Example

Enables the trap for the event indicating that the number of (S, G) multicast forwarding entries created exceeds the maximum number of (S, G) multicast forwarding entries allowed.

```
<Huawei> system-view
[Huawei] snmp-agent trap enable feature-name mrm trap-name hwipmcastsgexceed
```

Disable the trap for the event indicating that the number of (S, G) multicast forwarding entries created exceeds the maximum number of (S, G) multicast forwarding entries allowed.

```
<Huawei> system-view
[Huawei] undo snmp-agent trap enable feature-name mrm trap-name hwipmcastsgexceed
```

Related Topics

10.11.5 display snmp-agent trap feature-name mrm all

10.11.20 snmp-agent trap enable feature-name msdp

Function

The **snmp-agent trap enable feature-name msdp** command enables the traps function for the MSDP module.

The **undo snmp-agent trap enable feature-name msdp** command disables the traps function for the MSDP module.

By default, the trap function for MSDP events is disabled.

Format

snmp-agent trap enable feature-name msdp [**trap-name** { **establish** | **backward** }]

undo snmp-agent trap enable feature-name msdp [**trap-name** { **establish** | **backward** }]

Parameters

Parameter	Description	Value
trap-name	Enables the traps of MSDP events of specified types.	-
establish	Enables the trap of the setup of the MSDP peer relationship.	-
backward	Enables the trap of the deletion of the MSDP peer relationship.	-

Views

System view

Copyright © Huawei Technologies Co., Ltd.

Default Level

3: Management level

Usage Guidelines

To enable the traps of one or more events, you can specify **trap-name**.

Example

Enable the trap of the setup of the MSDP peer relationship in the system view.

```
<Huawei> system-view
[Huawei] snmp-agent trap enable feature-name msdp trap-name establish
```

Disable the trap of the setup of the MSDP peer relationship in the system view.

```
<Huawei> system-view
[Huawei] undo snmp-agent trap enable feature-name msdp trap-name establish
```

Related Topics

10.11.6 display snmp-agent trap feature-name msdp all

10.11.21 snmp-agent trap enable feature-name pim

Function

The **snmp-agent trap enable feature-name pim** command enables the trap function for PIM events.

The **undo snmp-agent trap enable feature-name pim** command disables the trap function for PIM events.

By default, the trap function for PIM events is disabled.

Format

snmp-agent trap enable feature-name pim [**trap-name** { **neighbor-loss** | **invalid-join-prune** | **rp-mapping-change** | **interface-election** | **invalid-register** | **new-neighbor** | **mrt-limit** | **hwpimmrtlimitclear** | **hwpimsgexceed** | **hwpimsgexceedclear** | **hwpimsgthresholdexceed** | **hwpimsgthresholdexceedclear** | **hwpimstargexceed** | **hwpimstargexceedclear** | **hwpimstargthresholdexceed** | **hwpimstargthresholdexceedclear** }]

undo snmp-agent trap enable feature-name pim [**trap-name** { **neighbor-loss** | **invalid-join-prune** | **rp-mapping-change** | **interface-election** | **invalid-register** | **new-neighbor** | **mrt-limit** | **hwpimmrtlimitclear** | **hwpimsgexceed** | **hwpimsgexceedclear** | **hwpimsgthresholdexceed** | **hwpimsgthresholdexceedclear** | **hwpimstargexceed** | **hwpimstargexceedclear** | **hwpimstargthresholdexceed** | **hwpimstargthresholdexceedclear** }]

Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
trap-name	Enables the trap for a specified type of PIM event.	-
neighbor-loss	Enables the trap for the PIM neighbor loss event.	-
invalid-join-prune	Enables the trap for the event indicating that an invalid Join/Prune message is received.	-
rp-mapping-change	Enables the trap for the PIM RP-mapping change event.	-
interface-election	Enables the trap for the event indicating that a PIM interface is elected as the DR.	-
invalid-register	Enables the trap for the event indicating that an invalid Register message is received.	-
new-neighbor	Enables the trap for the event indicating that a new PIM neighbor appears.	-
mrt-limit	Enables the trap for the event indicating that the number of PIM entries exceeds the limit.	-
hwpimmrtlimitclear	Enables the trap for the event indicating that the total number of PIM entries falls below the limit.	-
hwpimsgexceed	Enables the trap for the event indicating that the number of PIM (S, G) entries created exceeds the maximum number of PIM (S, G) entries allowed.	-
hwpimsgexceedclear	Enables the trap for the event indicating that the number of PIM (S, G) entries created falls below the maximum number of PIM (S, G) entries allowed.	-
hwpimsgthresholdexceed	Enables the trap for the event indicating that the proportion of PIM (S, G) entries created to the maximum PIM (S, G) entries allowed exceeds the upper alarm threshold.	-

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
hwpimsgthresholdexceedclear	Enables the trap for the event indicating that the proportion of PIM (S, G) entries created to the maximum PIM (S, G) entries allowed falls below the lower alarm threshold.	-
hwpimstargexceed	Enables the trap for the event indicating that the number of PIM (*, G) entries created exceeds the maximum number of PIM (*, G) entries allowed.	-
hwpimstargexceedclear	Enables the trap for the event indicating that the number of PIM (*, G) entries created falls below the maximum number of PIM (*, G) entries allowed.	-
hwpimstargthresholdexceed	Enables the trap for the event indicating that the proportion of PIM (*, G) entries created to the maximum PIM (*, G) entries allowed exceeds the upper alarm threshold.	-
hwpimstargthresholdexceedclear	Enables the trap for the event indicating that the proportion of PIM (*, G) entries created to the maximum PIM (*, G) entries allowed falls below the lower alarm threshold.	-

Views

System view

Default Level

3: Management level

Usage Guidelines

To enable the trap function for a specific type of event, specify **trap-name**. To enable the trap function for multiple types of events, run this command multiple times.

Example

Enable the trap for the PIM neighbor loss event in the system view.

```
<Huawei> system-view
[Huawei] snmp-agent trap enable feature-name pim trap-name neighbor-loss
```

Disable the trap for the PIM neighbor loss event in the system view.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> system-view
[Huawei] undo snmp-agent trap enable feature-name pim trap-name neighbor-loss
```

Related Topics

10.11.7 display snmp-agent trap feature-name pim all

10.11.15 pim mib-notification interval

10.11.22 snmp-agent trap enable feature-name pim-std

Function

The **snmp-agent trap enable feature-name pim-std** command enables PIM-STD traps.

The **undo snmp-agent trap enable feature-name pim-std** command disables related PIM-STD traps.

By default, the trap function for PIM-STD MIB events is disabled.

Format

snmp-agent trap enable feature-name pim-std [**trap-name** { **pimneighborloss** | **piminvalidregister** | **piminvalidjoinprune** | **pimrpmappingchange** | **piminterfaceelection** }]

undo snmp-agent trap enable feature-name pim-std [**trap-name** { **pimneighborloss** | **piminvalidregister** | **piminvalidjoinprune** | **pimrpmappingchange** | **piminterfaceelection** }]

Parameters

Parameter	Description	Value
trap-name	Enables the trap function for specific events.	-
pimneighborloss	Enables the trap function for the PIM-STD MIB events of neighbor loss.	-
piminvalidregister	Enables the trap function for the PIM-STD MIB events of invalid Register messages.	-
piminvalidjoinprune	Enables the trap function for the PIM-STD MIB events of invalid Join/Prune messages.	-
pimrpmappingchange	Enables the trap function for the PIM-STD MIB events of RP-Mapping change.	-
piminterfaceelection	Enables the trap function for the PIM-STD MIB events of interface election.	-

Views

System view

Copyright © Huawei Technologies Co., Ltd.

Default Level

3: Management level

Usage Guidelines

Usage Scenario

At present, the defined public PIM-STD MIB traps events include neighbor loss, invalid Join/Prune messages, RP-mapping change, interface election, and invalid Register messages. You can run the **snmp-agent trap enable feature-name pim-std** command to enable the trap function for PIM-STD MIB events when you need to monitor the current status of PIM protocol events.

Precautions

When using the **snmp-agent trap enable feature-name pim-std**, note the following points:

- Run the **snmp-agent trap enable feature-name pim-std** command directly to enable the trap function for all PIM-STD MIB events.
- Specify **trap-name** to enable the trap function for a specified type of PIM-STD MIB events.

Example

Enable the trap function for the PIM-STD MIB events of neighbor loss.

```
<Huawei> system-view
[Huawei] snmp-agent trap enable feature-name pim-std trap-name pimneighborloss
```

Enable the trap function for all PIM-STD MIB events.

```
<Huawei> system-view
[Huawei] snmp-agent trap enable feature-name pim-std
```

Disable the trap function for the PIM-STD MIB events of neighbor loss.

```
<Huawei> system-view
[Huawei] undo snmp-agent trap enable feature-name pim-std trap-name pimneighborloss
```

Related Topics

10.11.8 display snmp-agent trap feature-name pim-std all

Copyright © Huawei Technologies Co., Ltd.