Hewlett Packard
Enterprise

HPE FlexFabric 7900 Switch Series

IP Multicast

Command Reference

Part number: 5998-8235
Software version: Release 231x
Document version: 6W101-20151113

Acknowledgments

Contents

IGMP snooping commands

The HPE 7904 (JG682A) or HPE 7904 TAA (JH122A) switch uses one built-in MPU (slot 0) and the HPE 7910 (JG841A) or HPE 7910 TAA (JH123A) switch uses two removable switching fabric modules (slots 10 and 11) for switching and control.

Unless otherwise stated, the term "card" collectively refers to LPUs, switching fabric modules, and MPUs.

display igmp-snooping

Use **display igmp-snooping** to display IGMP snooping status.

Syntax

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

Views

Any view

Predefined user roles

network-admin

network-operator

mdc-admin

mdc-operator

Parameters

global: Displays the global IGMP snooping status.

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

Usage guidelines

If you do not specify any parameters, this command displays the global IGMP snooping status and the IGMP snooping status for all VLANs.

Examples

# Display the global IGMP snooping status and the IGMP snooping status for all VLANs.

```
<Sysname> display igmp-snooping
IGMP snooping information: Global
 IGMP snooping: Enabled
 Drop-unknown: Disabled
 Host-aging-time: 260s
 Router-aging-time: 260s
 Max-response-time: 10s
 Last-member-query-interval: 1s
 Report-aggregation: Enabled

IGMP snooping information: VLAN 1
 IGMP snooping: Enabled
 Drop-unknown: Disabled
 Version: 2
 Host-aging-time: 200s
 Router-aging-time: 260s
 Max-response-time: 10s
 Last-member-query-interval: 2s

IGMP snooping information: VLAN 10
 IGMP snooping: Enabled
 Drop-unknown: Enabled
 Version: 3
 Host-aging-time: 260s
 Router-aging-time: 260s
 Max-response-time: 10s
 Last-member-query-interval: 1s
```

Table 1 Command output

Field	Description
IGMP snooping	IGMP snooping status: - **Enabled**. - **Disabled**.
Drop-unknown	Status of dropping unknown multicast data: - **Enabled**. - **Disabled**.
Version	IGMP snooping version.
Host-aging-time	Aging timer for the dynamic member port.
Router-aging-time	Aging timer for the dynamic router port.
Max-response-time	Maximum response time for IGMP general queries.
Last-member-query-interval	Interval for sending IGMP group-specific queries.
Report-aggregation	Status of IGMP report suppression: - **Enabled**. - **Disabled**.

display igmp-snooping group

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

Syntax

In standalone mode:

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

In IRF mode:

display igmp-snooping group [*group-address* | *source-address*] * [**vlan** *vlan-id*] [**verbose**] [**chassis** *chassis-number* **slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

mdc-admin

mdc-operator

Parameters

group-address: Specifies a multicast group by its IP address in the range of 224.0.1.0 to 239.255.255.255. If you do not specify a multicast group, this command displays dynamic IGMP snooping forwarding entries for all multicast groups.

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

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

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

slot *slot-number*: Specifies a card by its slot number. If you do not specify a card, this command displays dynamic IGMP snooping forwarding entries on the MPU or the switching fabric modules. (In standalone mode.)

chassis *chassis-number* **slot** *slot-number*: Specifies a card on a member device. The *chassis-number* argument specifies an IRF member device ID, and the *slot-number* argument specifies a card by its slot number. If you do not specify a member device, this command displays dynamic IGMP snooping forwarding entries on all MPUs or switching fabric modules in the IRF fabric. (In IRF mode.)

Examples

# Display dynamic IGMP snooping forwarding entries for VLAN 2.

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

VLAN 2: Total 1 entries.
  (0.0.0.0, 224.1.1.1)
    Host slots (1 in total):
      1
    Host ports (1 in total):
      FGE1/0/2
```

Table 2 Command output

Field	Description
Total 1 entries	Total number of dynamic IGMP snooping forwarding entries.
VLAN 2: Total 1 entries	Total number of dynamic IGMP snooping forwarding entries in VLAN 2.
(0.0.0.0, 224.1.1.1)	(S, G) entry, where **0.0.0.0** in the S position means all multicast sources.
Host slots (1 in total)	Total number of cards where member ports reside and the slot IDs of the cards.
Host ports (1 in total)	Total number of member ports and the port list.

Related commands

reset igmp-snooping group

display igmp-snooping router-port

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

Syntax

In standalone mode:

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

In IRF mode:

display igmp-snooping router-port [**vlan** *vlan-id*] [**chassis** *chassis-number* **slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

mdc-admin

mdc-operator

Parameters

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

slot *slot-number*: Specifies a card by its slot number. If you do not specify a card, this command displays dynamic router port information on the MPU or the switching fabric modules. (In standalone mode.)

chassis *chassis-number* **slot** *slot-number*: Specifies a card on a member device. The *chassis-number* argument specifies an IRF member device ID, and the *slot-number* argument specifies a card by its slot number. If you do not specify a member device, this command displays dynamic router port information on all MPUs or switching fabric modules in the IRF fabric. (In IRF mode.)

Examples

# Display dynamic router port information for VLAN 2.

```
<Sysname> display igmp-snooping router-port vlan 2
VLAN 2:
  Router slots (1 in total):
    1
  Router ports (2 in total):
    FGE1/0/1
    FGE1/0/2
```

Table 3 Command output

Field	Description
VLAN 2	VLAN ID.
Router slots (1 in total)	Slot IDs of the cards where dynamic router ports reside and total number of the cards.
Router ports (2 in total)	Dynamic router ports and total number of the dynamic router ports.

Related commands

reset igmp-snooping router-port

display igmp-snooping static-group

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

Syntax

In standalone mode:

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

In IRF mode:

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

Views

Any view

Predefined user roles

network-admin

network-operator

mdc-admin

mdc-operator

Parameters

group-address: Specifies a multicast group by its IP address in the range of 224.0.1.0 to 239.255.255.255. If you do not specify a multicast group, this command displays static IGMP snooping forwarding entries for all multicast groups.

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

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

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

slot *slot-number*: Specifies a card by its slot number. If you do not specify a card, this command displays static IGMP snooping forwarding entries on the MPU or the switching fabric modules. (In standalone mode.)

chassis *chassis-number* **slot** *slot-number*: Specifies a card on a member device. The *chassis-number* argument specifies an IRF member device ID, and the *slot-number* argument specifies a card by its slot number. If you do not specify a member device, this command displays static IGMP snooping forwarding entries on all MPUs or switching fabric modules in the IRF fabric. (In IRF mode.)

Examples

# Display static IGMP snooping forwarding entries for VLAN 2.

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

VLAN 2: Total 1 entries.
  (0.0.0.0, 224.1.1.1)
    Host slots (1 in total):
      1
    Host ports (1 in total):
```

```
    FGE1/0/2
```

Table 4 Command output

Field	Description
Total 1 entries	Total number of static IGMP snooping forwarding entries.
VLAN 2: Total 1 entries	Total number of static IGMP snooping forwarding entries in VLAN 2.
(0.0.0.0, 224.1.1.1)	(S, G) entry, where **0.0.0.0** in the S position means all multicast sources.
Host slots (1 in total)	Slot IDs of the cards where member ports reside and total number of the cards.
Host ports (1 in total)	Member ports and total number of the member ports.

display igmp-snooping static-router-port

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

Syntax

In standalone mode:

display igmp-snooping static-router-port [**vlan** *vlan-id*] [**slot** *slot-number*]

In IRF mode:

display igmp-snooping static-router-port [**vlan** *vlan-id*] [**chassis** *chassis-number* **slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

mdc-admin

mdc-operator

Parameters

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

slot *slot-number*: Specifies a card by its slot number. If you do not specify a card, this command displays static router port information on the MPU or the switching fabric modules. (In standalone mode.)

chassis *chassis-number* **slot** *slot-number*: Specifies a card on a member device. The *chassis-number* argument specifies an IRF member device ID, and the *slot-number* argument specifies a card by its slot number. If you do not specify a member device, this command displays static router port information on all MPUs or switching fabric modules in the IRF fabric. (In IRF mode.)

Examples

# Display static router port information for VLAN 2.

```
<Sysname> display igmp-snooping static-router-port vlan 2
VLAN 2:
  Router slots (1 in total):
    1
  Router ports (2 in total):
    FGE1/0/1
    FGE1/0/2
```

Table 5 Command output

Field	Description
VLAN 2	VLAN ID.
Router slots (1 in total)	Slot IDs of the cards where static router ports reside and total number of the cards.
Router ports (2 in total)	Static router ports and total number of the static router ports.

display igmp-snooping statistics

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

Syntax

display igmp-snooping statistics

Views

Any view

Predefined user roles

network-admin

network-operator

mdc-admin

mdc-operator

Examples

# Display statistics for the IGMP messages learned through IGMP snooping.

```
<Sysname> display igmp-snooping statistics
Received IGMP general queries:  0
Received IGMPv1 reports:  0
Received IGMPv2 reports:  19
Received IGMP leaves:  0
Received IGMPv2 specific queries:  0
Sent     IGMPv2 specific queries:  0
Received IGMPv3 reports:  1
Received IGMPv3 reports with right and wrong records:  0
Received IGMPv3 specific queries:  0
Received IGMPv3 specific sg queries:  0
Sent     IGMPv3 specific queries:  0
Sent     IGMPv3 specific sg queries:  0
Received error IGMP messages:  19
```

Table 6 Command output

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

Field	Description
reports	Number of IGMP reports.
leaves	Number of IGMP leave messages.
reports with right and wrong records	Number of IGMP reports with correct and incorrect records.
specific sg queries	Number of IGMP group-and-source-specific queries.
error IGMP messages	Number of IGMP messages with errors.

Related commands

reset igmp-snooping statistics

display l2-multicast ip

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

Syntax

In standalone mode:

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

In IRF mode:

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

Views

Any view

Predefined user roles

network-admin

network-operator

mdc-admin

mdc-operator

Parameters

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

source *source-address*: Specifies a multicast source by its IP address. If you do not specify a multicast source, this command displays information about Layer 2 IP multicast groups for all multicast sources.

vlan *vlan-id*: Specifies a VLAN by its VLAN ID in the range of 1 to 4094. If you do not specify a VLAN, this command displays information about Layer 2 IP multicast groups for all VLANs.

slot *slot-number*: Specifies a card by its slot number. If you do not specify a card, this command displays information about the Layer 2 IP multicast groups on the MPU or the switching fabric modules. (In standalone mode.)

chassis *chassis-number* **slot** *slot-number*: Specifies a card on a member device. The *chassis-number* argument specifies an IRF member device ID, and the *slot-number* argument specifies a card by its slot number. If you do not specify a member device, this command displays information about Layer 2 IP multicast groups on all MPUs or switching fabric modules in the IRF fabric. (In IRF mode.)

Examples

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

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

VLAN 2: Total 1 IP entries.
  (0.0.0.0, 224.1.1.1)
    Attribute: static, success
    Host slots (1 in total):
      1
    Host ports (1 in total):
      FGE1/0/1                  (S, SUC)
```

Table 7 Command output

Field	Description
Total 1 entries	Total number of Layer 2 IP multicast groups.
VLAN 2: Total 1 IP entries	Total number of Layer 2 IP multicast groups in VLAN 2.
(0.0.0.0, 224.1.1.1)	(S, G) entry, where **0.0.0.0** in the S position means all multicast sources.
Attribute	Entry attribute: • **dynamic**—The entry is created by a dynamic protocol. • **static**—The entry is created by a static protocol. • **pim**—The entry is created by PIM. • **kernel**—The entry is obtained from the kernel. • **success**—Processing succeeds. • **fail**—Processing fails.
Host slots (1 in total)	Slot IDs of the cards where member ports reside and total number of the cards.
Host ports (1 in total)	Member ports and total number of the member ports.
(S, SUC)	Port attribute: • **D**—Dynamic port. • **S**—Static port. • **P**—PIM port. • **K**—Port obtained from the kernel. • **R**—Port learned from (*, *) entries. • **W**—Port learned from (*, G) entries. • **SUC**—Processing succeeds. • **F**—Processing fails.

display l2-multicast ip forwarding

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

Syntax

In standalone mode:

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

In IRF mode:

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

Views

Any view

Predefined user roles

network-admin

network-operator

mdc-admin

mdc-operator

Parameters

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

source *source-address*: Specifies a multicast source by its IP address. If you do not specify a multicast source, this command displays Layer 2 IP multicast group entries for all multicast sources.

vlan *vlan-id*: Specifies a VLAN by its VLAN ID in the range of 1 to 4094. If you do not specify a VLAN, this command displays Layer 2 IP multicast group entries for all VLANs.

slot *slot-number*: Specifies a card by its slot number. If you do not specify a card, this command displays Layer 2 IP multicast group entries on the MPU or the switching fabric modules. (In standalone mode.)

chassis *chassis-number* **slot** *slot-number*: Specifies a card on a member device. The *chassis-number* argument specifies an IRF member device ID, and the *slot-number* argument specifies a card by its slot number. If you do not specify a member device, this command displays Layer 2 IP multicast group entries on all MPUs or switching fabric modules in the IRF fabric. (In IRF mode.)

Examples

# Display Layer 2 IP multicast group entries for VLAN 2.

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

VLAN 2: Total 1 IP entries.
  (0.0.0.0, 224.1.1.1)
    Host slots (1 in total):
      1
    Host ports (3 in total):
      FGE1/0/1
      FGE1/0/2
      FGE1/0/3
```

Table 8 Command output

Field	Description
Total 1 entries	Total number of Layer 2 IP multicast group entries.
VLAN 2: Total 1 IP entries	Total number of Layer 2 IP multicast group entries in VLAN 2.
(0.0.0.0, 224.1.1.1)	(S, G) entry, where **0.0.0.0** in the S position means all multicast sources.
Host slots (1 in total)	Slot IDs of the cards where member ports reside and total number of the cards.

Field	Description
Host ports (3 in total)	Member ports and total number of the member ports.

display l2-multicast mac

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

Syntax

In standalone mode:

display l2-multicast mac [*mac-address*] [**vlan** *vlan-id*] [**slot** *slot-number*]

In IRF mode:

display l2-multicast mac [*mac-address*] [**vlan** *vlan-id*] [**chassis** *chassis-number* **slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

mdc-admin

mdc-operator

Parameters

mac-address: Specifies a MAC multicast group by its MAC address. If you do not specify a MAC multicast group, this command displays information about all Layer 2 MAC multicast groups.

vlan *vlan-id*: Specifies a VLAN by its VLAN ID in the range of 1 to 4094. If you do not specify a VLAN, this command displays information about Layer 2 MAC multicast groups for all VLANs.

slot *slot-number*: Specifies a card by its slot number. If you do not specify a card, this command displays information about the Layer 2 MAC multicast groups on the MPU or the switching fabric modules. (In standalone mode.)

chassis *chassis-number* **slot** *slot-number*: Specifies a card on a member device. The *chassis-number* argument specifies an IRF member device ID, and the *slot-number* argument specifies a card by its slot number. If you do not specify a member device, this command displays information about the Layer 2 MAC multicast groups on all MPUs or switching fabric modules in the IRF fabric. (In IRF mode.)

Examples

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

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

VLAN 2: Total 1 MAC entries.
  MAC group address: 0100-5e01-0101
    Attribute: success
    Host slots (1 in total):
      1
    Host ports (1 in total):
      FGE1/0/1
```

Table 9 Command output

Field	Description
Total 1 MAC entries	Total number of Layer 2 MAC multicast groups.
VLAN 2: Total 1 MAC entries	Total number of Layer 2 MAC multicast groups in VLAN 2.
Attribute	Entry attribute: • **success**—Processing succeeds. • **fail**—Processing fails.
Host slots (1 in total)	Slot IDs of the cards where member ports reside and total number of the cards.
Host ports (1 in total)	Member ports and total number of the member ports.

display l2-multicast mac forwarding

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

Syntax

In standalone mode:

display l2-multicast mac forwarding [*mac-address*] [**vlan** *vlan-id*] [**slot** *slot-number*]

In IRF mode:

display l2-multicast mac forwarding [*mac-address*] [**vlan** *vlan-id*] [**chassis** *chassis-number* **slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

mdc-admin

mdc-operator

Parameters

mac-address: Specifies a MAC multicast group by its MAC address. If you do not specify a MAC multicast group, this commands displays Layer 2 MAC multicast group entries for all MAC multicast groups.

vlan *vlan-id*: Specifies a VLAN by its VLAN ID in the range of 1 to 4094. If you do not specify a VLAN, this command displays Layer 2 MAC multicast group entries for all VLANs.

slot *slot-number*: Specifies a card by its slot number. If you do not specify a card, this command displays Layer 2 MAC multicast group entries on the MPU or the switching fabric modules. (In standalone mode.)

chassis *chassis-number* **slot** *slot-number*: Specifies a card on a member device. The *chassis-number* argument specifies an IRF member device ID, and the *slot-number* argument specifies a card by its slot number. If you do not specify a member device, this command displays Layer 2 MAC multicast group entries on all MPUs or switching fabric modules in the IRF fabric. (In IRF mode.)

Examples

# Display Layer 2 MAC multicast group entries for VLAN 2.

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

VLAN 2: Total 1 MAC entries.
  MAC group address: 0100-5e01-0101
    Host slots (1 in total):
      1
    Host ports (3 in total):
      FGE1/0/1
      FGE1/0/2
      FGE1/0/3
```

Table 10 Command output

Field	Description
Total 1 MAC entries	Total number of Layer 2 MAC multicast group entries.
VLAN 2: Total 1 MAC entries	Total number of Layer 2 MAC multicast group entries in VLAN 2.
MAC group address	Address of the MAC multicast group.
Host slots (1 in total)	Slot IDs of the cards where member ports reside and total number of the cards.
Host ports (3 in total)	Member ports and total number of the member ports.

enable (IGMP-snooping view)

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

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

Syntax

enable vlan *vlan-list*

undo enable vlan *vlan-list*

Default

IGMP snooping is disabled for the VLANs.

Views

IGMP-snooping view

Predefined user roles

network-admin

mdc-admin

Parameters

vlan *vlan-list*: Specifies a space-separated list of up to 10 VLAN items. Each item specifies a VLAN by its ID or a range of VLANs in the form of *start-vlan-id* **to** *end-vlan-id*. The VLAN ID is in the range of 1 to 4094.

Examples

# Enable IGMP snooping globally, and enable IGMP snooping for VLAN 2 through VLAN 10.

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

```
[Sysname-igmp-snooping] enable vlan 2 to 10
```

Related commands

- **igmp-snooping**
- **igmp-snooping enable**

entry-limit (IGMP-snooping view)

Use **entry-limit** to set the global maximum number of IGMP snooping forwarding entries.

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

Syntax

entry-limit *limit*

undo entry-limit

Default

The maximum number of IGMP snooping forwarding entries is 4294967295.

Views

IGMP-snooping view

Predefined user roles

network-admin

mdc-admin

Parameters

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

Examples

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

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

fast-leave (IGMP-snooping view)

Use **fast-leave** to enable fast-leave processing globally.

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

Syntax

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

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

Default

Fast-leave processing is disabled.

Views

IGMP-snooping view

Predefined user roles

network-admin

mdc-admin

Parameters

vlan *vlan-list*: Specifies a space-separated list of up to 10 VLAN items. Each item specifies a VLAN by its ID or a range of VLANs in the form of *start-vlan-id* **to** *end-vlan-id*. The VLAN ID is in the range of 1 to 4094. If you do not specify a VLAN, this command takes effect on all VLANs.

Usage guidelines

This feature enables the switch to immediately remove the port from the forwarding entry for a multicast group when the port receives an IGMP leave message.

The global configuration takes effect on all ports. It has a lower priority than the configuration made on a specific port.

Examples

# Globally enable fast-leave processing for VLAN 2.

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

Related commands

igmp-snooping fast-leave

group-policy (IGMP-snooping view)

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

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

Syntax

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

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

Default

No multicast group policy exists, and hosts can join any multicast groups.

Views

IGMP-snooping view

Predefined user roles

network-admin

mdc-admin

Parameters

acl-number: Specifies an IPv4 basic or advanced ACL by its number, in the range of 2000 to 3999. Receiver hosts can join only the multicast groups that the ACL permits. If the specified ACL does not exist or the ACL does not have valid rules, receiver hosts cannot join any multicast groups.

vlan *vlan-list*: Specifies a space-separated list of up to 10 VLAN items. Each item specifies a VLAN by its ID or a range of VLANs in the form of *start-vlan-id* **to** *end-vlan-id*. The VLAN ID is in the range of 1 to 4094. If you do not specify a VLAN, this command takes effect on all VLANs.

Usage guidelines

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

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

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

  To match the following IGMP reports, set the **source** *source-address source-wildcard* option to 0.0.0.0:

  - IGMPv1 and IGMPv2 reports.
  - IGMPv3 IS_EX and IGMPv3 TO_EX reports that do not carry multicast source addresses.
- Among the other optional parameters, only the **fragment** keyword and the **time-range** *time-range-name* option take effect.

You can configure different ACL rules globally for different VLANs. If you configure multiple ACLs for the same VLAN, the most recent configuration takes effect.

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

The global configuration takes effect on all ports. It has a lower priority than the configuration made on a specific port.

Examples

# Configure a multicast group policy globally for VLAN 2 so that the hosts in this VLAN can join only the multicast group 225.1.1.1.

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

Related commands

igmp-snooping group-policy

host-aging-time (IGMP-snooping view)

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

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

Syntax

host-aging-time *interval*

undo host-aging-time

Default

The default setting is 260 seconds.

Views

IGMP-snooping view

Predefined user roles

network-admin

mdc-admin

Parameters

interval: Specifies an aging timer for dynamic member ports, in the range of 200 to 1000 seconds.

Usage guidelines

The global configuration takes effect on all VLANs. It has a lower priority than the configuration made in a specific VLAN.

Examples

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

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

Related commands

igmp-snooping host-aging-time

igmp-snooping

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

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

Syntax

igmp-snooping

undo igmp-snooping

Default

IGMP snooping is disabled.

Views

System view

Predefined user roles

network-admin

mdc-admin

Examples

# Enable IGMP snooping globally and enter IGMP-snooping view.

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

Related commands

- **enable** (IGMP-snooping view)
- **igmp-snooping enable**

igmp-snooping drop-unknown

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

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

Syntax

igmp-snooping drop-unknown

undo igmp-snooping drop-unknown

Default

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

Views

VLAN view

Predefined user roles

network-admin

mdc-admin

Usage guidelines

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

Examples

# Enable IGMP snooping, and enable dropping unknown multicast data for VLAN 2.

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

Related commands

igmp-snooping enable

igmp-snooping enable

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

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

Syntax

igmp-snooping enable

undo igmp-snooping enable

Default

IGMP snooping is disabled in a VLAN.

Views

VLAN view

Predefined user roles

network-admin

mdc-admin

Usage guidelines

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

Examples

# Enable IGMP snooping globally, and enable IGMP snooping for VLAN 2.

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

```
[Sysname] igmp-snooping
[Sysname-igmp-snooping] quit
[Sysname] vlan 2
[Sysname-vlan2] igmp-snooping enable
```

Related commands

- **enable** (IGMP-snooping view)
- **igmp-snooping**

igmp-snooping fast-leave

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

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

Syntax

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

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

Default

Fast-leave processing is disabled on a port.

Views

Layer 2 Ethernet interface view, Layer 2 aggregate interface view

Predefined user roles

network-admin

mdc-admin

Parameters

vlan *vlan-list*: Specifies a space-separated list of up to 10 VLAN items. Each item specifies a VLAN by its ID or a range of VLANs in the form of *start-vlan-id* **to** *end-vlan-id*. The VLAN ID is in the range of 1 to 4094. If you do not specify a VLAN, this command takes effect on all VLANs.

Usage guidelines

This feature enables the switch to immediately remove a port from the forwarding entry for a multicast group when the port receives a leave message.

The configuration made in interface view is only effective on the current port. It has a higher priority than the global configuration.

Examples

# Enable fast-leave processing for VLAN 2 on FortyGigE 1/0/1.

```
<Sysname> system-view
[Sysname] interface fortygige 1/0/1
[Sysname-FortyGigE1/0/1] igmp-snooping fast-leave vlan 2
```

Related commands

fast-leave (IGMP-snooping view)

igmp-snooping general-query source-ip

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

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

Syntax

igmp-snooping general-query source-ip *ip-address*

undo igmp-snooping general-query source-ip

Default

The source IP address of IGMP general queries is the IP address of the current VLAN interface. If the current VLAN interface does not have an IP address, the source IP address is 0.0.0.0.

Views

VLAN view

Predefined user roles

network-admin

mdc-admin

Parameters

ip-address: Specifies a source IP address for IGMP general queries.

Usage guidelines

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

Examples

# In VLAN 2, enable IGMP snooping, and configure 10.1.1.1 as the source IP address of IGMP general queries.

```
<Sysname> system-view
[Sysname] igmp-snooping
[Sysname-igmp-snooping] quit
[Sysname] vlan 2
[Sysname-vlan2] igmp-snooping enable
[Sysname-vlan2] igmp-snooping general-query source-ip 10.1.1.1
```

Related commands

- **enable** (IGMP-snooping view)
- **igmp-snooping enable**

igmp-snooping group-limit

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

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

Syntax

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

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

Default

The default setting is 4294967295.

Views

Layer 2 Ethernet interface view, Layer 2 aggregate interface view

Predefined user roles

network-admin

mdc-admin

Parameters

limit: Specifies the maximum number of multicast groups that a port can join, in the range of 0 to 4294967295.

vlan *vlan-list*: Specifies a space-separated list of up to 10 VLAN items. Each item specifies a VLAN by its ID or a range of VLANs in the form of *start-vlan-id* **to** *end-vlan-id*. The VLAN ID is in the range of 1 to 4094. If you do not specify a VLAN, this command takes effect on all VLANs.

Usage guidelines

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

Examples

# Set the maximum number of multicast groups that FortyGigE 1/0/1 in VLAN 2 can join to 10.

```
<Sysname> system-view
[Sysname] interface fortygige 1/0/1
[Sysname-FortyGigE1/0/1] igmp-snooping group-limit 10 vlan 2
```

igmp-snooping group-policy

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

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

Syntax

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

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

Default

No multicast group policy exists on a port, and hosts can join any multicast groups.

Views

Layer 2 Ethernet interface view, Layer 2 aggregate interface view

Predefined user roles

network-admin

mdc-admin

Parameters

acl-number: Specifies an IPv4 basic or advanced ACL by its number in the range of 2000 to 3999. Receiver hosts can join only the multicast groups that the ACL permits. If the specified ACL does not exist or the ACL does not have valid rules, receiver hosts cannot join any multicast groups.

vlan *vlan-list*: Specifies a space-separated list of up to 10 VLAN items. Each item specifies a VLAN by its ID or a range of VLANs in the form of *start-vlan-id* **to** *end-vlan-id*. The VLAN ID is in the range of 1 to 4094. If you do not specify a VLAN, this command takes effect on all VLANs.

Usage guidelines

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

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

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

  To match the following IGMP reports, set the **source** *source-address source-wildcard* option to 0.0.0.0:

  - IGMPv1 and IGMPv2 reports.
  - IGMPv3 IS_EX and IGMPv3 TO_EX reports that do not carry multicast source addresses.
- Among the other optional parameters, only the **fragment** keyword and the **time-range** *time-range-name* option take effect.

You can configure different ACLs on a port for different VLANs. If you configure multiple ACLs on a port for the same VLAN, the most recent configuration takes effect.

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

The configuration made in interface view takes effect only on the current port. It has a higher priority than the global configuration.

Examples

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

```
<Sysname> system-view
[Sysname] acl number 2000
[Sysname-acl-basic-2000] rule permit source 225.1.1.1 0
[Sysname-acl-basic-2000] quit
[Sysname] interface fortygige 1/0/1
[Sysname-FortyGigE1/0/1] igmp-snooping group-policy 2000 vlan 2
```

Related commands

group-policy (IGMP-snooping view)

igmp-snooping host-aging-time

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

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

Syntax

igmp-snooping host-aging-time *interval*

undo igmp-snooping host-aging-time

Default

The default setting is 260 seconds.

Views

VLAN view

Predefined user roles

network-admin

mdc-admin

Parameters

interval: Specifies an aging timer for dynamic member ports, in the range of 200 to 1000 seconds.

Usage guidelines

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

The configuration made in VLAN view takes effect only on the current VLAN. It has a higher priority than the global configuration.

Examples

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

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

Related commands

- **host-aging-time** (IGMP-snooping view)
- **igmp-snooping enable**

igmp-snooping host-join

Use **igmp-snooping host-join** to configure a port as a simulated member host for a multicast group.

Use **undo igmp-snooping host-join** to remove the simulated joining configuration.

Syntax

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

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

Default

A port is not configured as a simulated member host for any multicast groups.

Views

Layer 2 Ethernet interface view, Layer 2 aggregate interface view

Predefined user roles

network-admin

mdc-admin

Parameters

group-address: Specifies a multicast group in the range of 224.0.1.0 to 239.255.255.255.

source-ip *source-address*: Specifies a multicast source by its IP address. If you specify a multicast source, this command configures the port as a simulated member host for a multicast source and group. If you do not specify a multicast source, this command configures the port as a simulated member host for a multicast group. This option takes effect on IGMPv3 snooping devices.

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

all: Specifies all multicast groups.

Usage guidelines

The version of IGMP running on a simulated member host is the same as the version of IGMP snooping running on the port. The port ages out in the same way as a dynamic member port.

Examples

# Configure FortyGigE 1/0/1 as a simulated member host of the multicast source and group (1.1.1.1, 232.1.1.1) in VLAN 2.

```
<Sysname> system-view
[Sysname] igmp-snooping
[Sysname-igmp-snooping] quit
[Sysname] vlan 2
[Sysname-vlan2] igmp-snooping enable
[Sysname-vlan2] igmp-snooping version 3
[Sysname-vlan2] quit
[Sysname] interface fortygige 1/0/1
[Sysname-FortyGigE1/0/1] igmp-snooping host-join 232.1.1.1 source-ip 1.1.1.1 vlan 2
```

igmp-snooping last-member-query-interval

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

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

Syntax

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

undo igmp-snooping last-member-query-interval

Default

The default setting is 1 second.

Views

VLAN view

Predefined user roles

network-admin

mdc-admin

Parameters

interval: Specifies the IGMP last member query interval in the range of 1 to 5 seconds.

Usage guidelines

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

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

The configuration made in VLAN view takes effect only on the current VLAN. It has a higher priority than the global configuration.

Examples

# In VLAN 2, enable IGMP snooping, and set the IGMP last member query interval to 3 seconds.

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

```
[Sysname] vlan 2
[Sysname-vlan2] igmp-snooping enable
[Sysname-vlan2] igmp-snooping last-member-query-interval 3
```

Related commands

- **igmp-snooping enable**
- **last-member-query-interval** (IGMP-snooping view)

igmp-snooping leave source-ip

Use **igmp-snooping leave source-ip** to configure the source IP address for IGMP leave messages.

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

Syntax

igmp-snooping leave source-ip *ip-address*

undo igmp-snooping leave source-ip

Default

The source IP address of IGMP leave messages is the IP address of the current VLAN interface. If the current VLAN interface does not have an IP address, the source IP address is 0.0.0.0.

Views

VLAN view

Predefined user roles

network-admin

mdc-admin

Parameters

ip-address: Specifies a source IP address for IGMP leave messages.

Usage guidelines

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

Examples

# In VLAN 2, enable IGMP snooping, and configure the source IP address of IGMP leave messages addressed to 10.1.1.1.

```
<Sysname> system-view
[Sysname] igmp-snooping
[Sysname-igmp-snooping] quit
[Sysname] vlan 2
[Sysname-vlan2] igmp-snooping enable
[Sysname-vlan2] igmp-snooping leave source-ip 10.1.1.1
```

Related commands

- **enable** (IGMP-snooping view)
- **igmp-snooping enable**

igmp-snooping max-response-time

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

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

Syntax

igmp-snooping max-response-time *interval*

undo igmp-snooping max-response-time

Default

The default setting is 10 seconds.

Views

VLAN view

Predefined user roles

network-admin

mdc-admin

Parameters

interval: Specifies the maximum response time for IGMP general queries, in the range of 1 to 25 seconds.

Usage guidelines

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

The configuration made in VLAN view takes effect only on the current VLAN. It has a higher priority than the global configuration.

Examples

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

```
<Sysname> system-view
[Sysname] igmp-snooping
[Sysname-igmp-snooping] quit
[Sysname] vlan 2
[Sysname-vlan2] igmp-snooping enable
[Sysname-vlan2] igmp-snooping max-response-time 5
```

Related commands

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

igmp-snooping overflow-replace

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

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

Syntax

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

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

Default

The multicast group replacement feature is disabled.

Views

Layer 2 Ethernet interface view, Layer 2 aggregate interface view

Predefined user roles

network-admin

mdc-admin

Parameters

vlan *vlan-list*: Specifies a space-separated list of up to 10 VLAN items. Each item specifies a VLAN by its ID or a range of VLANs in the form of *start-vlan-id* **to** *end-vlan-id*. The VLAN ID is in the range of 1 to 4094. If you do not specify a VLAN, this command takes effect on all VLANs.

Usage guidelines

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

The configuration made in interface view takes effect only on the current port. It has a higher priority than the global configuration.

Examples

# Enable the multicast group replacement feature for VLAN 2 on FortyGigE 1/0/1.

```
<Sysname> system-view
[Sysname] interface fortygige 1/0/1
[Sysname-FortyGigE1/0/1] igmp-snooping overflow-replace vlan 2
```

Related commands

overflow-replace (IGMP-snooping view)

igmp-snooping querier

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

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

Syntax

igmp-snooping querier

undo igmp-snooping querier

Default

The IGMP snooping querier is disabled.

Views

VLAN view

Predefined user roles

network-admin

mdc-admin

Usage guidelines

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

Examples

# In VLAN 2, enable IGMP snooping, and enable the IGMP snooping querier.

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

```
[Sysname] vlan 2
[Sysname-vlan2] igmp-snooping enable
[Sysname-vlan2] igmp-snooping querier
```

Related commands

- **enable** (IGMP-snooping view)
- **igmp-snooping enable**

igmp-snooping query-interval

Use **igmp-snooping query-interval** to set the IGMP general query interval for a VLAN.

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

Syntax

igmp-snooping query-interval *interval*

undo igmp-snooping query-interval

Default

The IGMP general query interval for a VLAN is 125 seconds.

Views

VLAN view

Predefined user roles

network-admin

mdc-admin

Parameters

interval: Specifies an IGMP general query interval in the range of 2 to 300 seconds.

Usage guidelines

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

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

Examples

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

```
<Sysname> system-view
[Sysname] igmp-snooping
[Sysname-igmp-snooping] quit
[Sysname] vlan 2
[Sysname-vlan2] igmp-snooping enable
[Sysname-vlan2] igmp-snooping query-interval 20
```

Related commands

- **enable** (IGMP-snooping view)
- **igmp-snooping enable**
- **igmp-snooping max-response-time**
- **igmp-snooping querier**
- **max-response-time**

igmp-snooping report source-ip

Use **igmp-snooping report source-ip** to configure the source IP address for IGMP reports.

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

Syntax

igmp-snooping report source-ip *ip-address*

undo igmp-snooping report source-ip

Default

The source IP address of IGMP reports is the IP address of the current VLAN interface. If the current VLAN interface does not have an IP address, the source IP address is 0.0.0.0.

Views

VLAN view

Predefined user roles

network-admin

mdc-admin

Parameters

ip-address: Specifies a source IP address for IGMP reports.

Usage guidelines

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

Examples

# In VLAN 2, enable IGMP snooping, and configure the source IP address of IGMP reports to 10.1.1.1.

```
<Sysname> system-view
[Sysname] igmp-snooping
[Sysname-igmp-snooping] quit
[Sysname] vlan 2
[Sysname-vlan2] igmp-snooping enable
[Sysname-vlan2] igmp-snooping report source-ip 10.1.1.1
```

Related commands

- **enable** (IGMP-snooping view)
- **igmp-snooping enable**

igmp-snooping router-aging-time

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

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

Syntax

igmp-snooping router-aging-time *interval*

undo igmp-snooping router-aging-time

Default

The default setting is 260 seconds.

Views

VLAN view

Predefined user roles

network-admin

mdc-admin

Parameters

interval: Specifies an aging timer for dynamic router ports in a VLAN, in the range of 1 to 1000 seconds.

Usage guidelines

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

The configuration made in VLAN view takes effect only on the current VLAN. It has a higher priority than the global configuration.

Examples

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

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

Related commands

- **igmp-snooping enable**
- **router-aging-time** (IGMP-snooping view)

igmp-snooping source-deny

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

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

Syntax

igmp-snooping source-deny

undo igmp-snooping source-deny

Default

Multicast source port filtering is disabled.

Views

Layer 2 Ethernet interface view

Predefined user roles

network-admin

mdc-admin

Usage guidelines

This configuration takes effect only on the current port. It has the same priority as the global configuration.

Examples

# Enable source port filtering for multicast data on FortyGigE 1/0/1.

```
<Sysname> system-view
[Sysname] interface fortygige 1/0/1
[Sysname-FortyGigE1/0/1] igmp-snooping source-deny
```

Related commands

source-deny (IGMP-snooping view)

igmp-snooping special-query source-ip

Use **igmp-snooping special-query source-ip** to configure the source IP address for IGMP group-specific queries.

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

Syntax

igmp-snooping special-query source-ip *ip-address*

undo igmp-snooping special-query source-ip

Default

If the IGMP snooping querier has received IGMP general queries, the source IP address of IGMP group-specific queries is the source IP address of IGMP general queries. Otherwise, the source IP address of IGMP group-specific queries is the IP address of the current VLAN interface. If the current VLAN interface does not have an IP address, the source IP address is 0.0.0.0.

Views

VLAN view

Predefined user roles

network-admin

mdc-admin

Parameters

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

Usage guidelines

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

Examples

# In VLAN 2, enable IGMP snooping, and configure the source IP address of IGMP group-specific queries as 10.1.1.1.

```
<Sysname> system-view
[Sysname] igmp-snooping
[Sysname-igmp-snooping] quit
[Sysname] vlan 2
[Sysname-vlan2] igmp-snooping enable
[Sysname-vlan2] igmp-snooping special-query source-ip 10.1.1.1
```

Related commands

- **enable** (IGMP-snooping view)
- **igmp-snooping enable**

igmp-snooping static-group

Use **igmp-snooping static-group** to configure a port as a static member port of a multicast group.

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

Syntax

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

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

Default

A port is not a static member port of any multicast groups.

Views

Layer 2 Ethernet interface view, Layer 2 aggregate interface view

Predefined user roles

network-admin

mdc-admin

Parameters

group-address: Specifies a multicast group by its IP address in the range of 224.0.1.0 to 239.255.255.255.

source-address: Specifies a multicast source by its IP address.

all: Specifies all VLANs.

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

Usage guidelines

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

Examples

# Configure FortyGigE 1/0/1 as a static member port for the multicast source and group (1.1.1.1, 225.0.0.1) in VLAN 2.

```
<Sysname> system-view
[Sysname] igmp-snooping
[Sysname-igmp-snooping] quit
[Sysname] vlan 2
[Sysname-vlan2] igmp-snooping enable
[Sysname-vlan2] igmp-snooping version 3
[Sysname-vlan2] quit
[Sysname] interface fortygige 1/0/1
[Sysname-FortyGigE1/0/1] igmp-snooping static-group 225.0.0.1 source-ip 1.1.1.1 vlan 2
```

igmp-snooping static-router-port

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

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

Syntax

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

undo igmp-snooping static-router-port { **all | vlan** *vlan-id* }

Default

A port is not a static router port.

Views

Layer 2 Ethernet interface view, Layer 2 aggregate interface view

Predefined user roles

network-admin

mdc-admin

Parameters

all: Specifies all VLANs.

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

Examples

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

```
<Sysname> system-view
[Sysname] interface fortygige 1/0/1
[Sysname-FortyGigE1/0/1] igmp-snooping static-router-port vlan 2
```

igmp-snooping version

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

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

Syntax

igmp-snooping version *version-number*

undo igmp-snooping version

Default

The default setting is IGMPv2 snooping.

Views

VLAN view

Predefined user roles

network-admin

mdc-admin

Parameters

version-number: Specifies an IGMP snooping version, 2 or 3.

Usage guidelines

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

Examples

# In VLAN 2, enable IGMP snooping, and specify IGMP snooping version 3.

```
<Sysname> system-view
[Sysname] igmp-snooping
[Sysname-igmp-snooping] quit
[Sysname] vlan 2
[Sysname-vlan2] igmp-snooping enable
[Sysname-vlan2] igmp-snooping version 3
```

Related commands

igmp-snooping enable

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

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

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

Syntax

last-member-query-interval *interval*

undo last-member-query-interval

Default

The default setting is 1 second.

Views

IGMP-snooping view

Predefined user roles

network-admin

mdc-admin

Parameters

interval: Specifies the IGMP last member query interval, in the range of 1 to 5 seconds.

Usage guidelines

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

The global configuration takes effect on all VLANs. It has a lower priority than the configuration made in a specific VLAN.

Examples

# Set the global IGMP last member query interval to 3 seconds.

```
<Sysname> system-view
[Sysname] igmp-snooping
[Sysname-igmp-snooping] last-member-query-interval 3
```

Related commands

igmp-snooping last-member-query-interval

max-response-time (IGMP-snooping view)

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

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

Syntax

max-response-time *interval*

undo max-response-time

Default

The default setting is 10 seconds.

Views

IGMP-snooping view

Predefined user roles

network-admin

mdc-admin

Parameters

interval: Specifies the maximum response time for IGMP general queries, in the range of 1 to 25 seconds.

Usage guidelines

The global configuration takes effect on all VLANs. It has a lower priority than the configuration made in a specific VLAN.

Examples

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

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

Related commands

igmp-snooping max-response-time

overflow-replace (IGMP-snooping view)

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

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

Syntax

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

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

Default

The multicast group replacement feature is disabled globally.

Views

IGMP-snooping view

Predefined user roles

network-admin

mdc-admin

Parameters

vlan *vlan-list*: Specifies a space-separated list of up to 10 VLAN items. Each item specifies a VLAN by its ID or a range of VLANs in the form of *start-vlan-id* **to** *end-vlan-id*. The VLAN ID is in the range of 1 to 4094. If you do not specify a VLAN, this command takes effect on all VLANs.

Usage guidelines

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

The global configuration takes effect on all ports. It has a lower priority than the configuration made on a specific port.

Examples

# Enable the multicast group replacement feature globally for VLAN 2.

```
<Sysname> system-view
[Sysname] igmp-snooping
[Sysname-igmp-snooping] overflow-replace vlan 2
```

Related commands

igmp-snooping overflow-replace

report-aggregation (IGMP-snooping view)

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

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

Syntax

report-aggregation

undo report-aggregation

Default

IGMP report suppression is enabled.

Views

IGMP-snooping view

Predefined user roles

network-admin

mdc-admin

Examples

# Disable IGMP report suppression.

```
<Sysname> system-view
[Sysname] igmp-snooping
[Sysname-igmp-snooping] undo report-aggregation
```

reset igmp-snooping group

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

Syntax

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

Views

User view

Predefined user roles

network-admin

mdc-admin

Parameters

group-address: Specifies a multicast group by its IP address in the range of 224.0.1.0 to 239.255.255.255.

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

all: Specifies all multicast groups.

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

Examples

# Clear dynamic IGMP snooping forwarding entries for all multicast groups.

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

Related commands

display igmp-snooping group

reset igmp-snooping router-port

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

Syntax

reset igmp-snooping router-port { **all** | **vlan** *vlan-id* }

Views

User view

Predefined user roles

network-admin

mdc-admin

Parameters

all: Specifies all VLANs.

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

Examples

# Clear information about all dynamic router ports.

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

Related commands

display igmp-snooping router-port

reset igmp-snooping statistics

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

Syntax

reset igmp-snooping statistics

Views

User view

Predefined user roles

network-admin

mdc-admin

Examples

# Clear the statistics for all IGMP messages learned through IGMP snooping.

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

Related commands

display igmp-snooping statistics

router-aging-time (IGMP-snooping view)

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

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

Syntax

router-aging-time *interval*

undo router-aging-time

Default

The default setting is 260 seconds.

Views

IGMP-snooping view

Predefined user roles

network-admin

mdc-admin

Parameters

interval: Specifies an aging timer for dynamic router ports, in the range of 1 to 1000 seconds.

Usage guidelines

The global configuration takes effect on all VLANs. It has a lower priority than the configuration made in a specific VLAN.

Examples

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

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

Related commands

igmp-snooping router-aging-time

source-deny (IGMP-snooping view)

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

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

Syntax

source-deny port *interface-list*

undo source-deny port *interface-list*

Default

Multicast source port filtering is disabled.

Views

IGMP-snooping view

Predefined user roles

network-admin

mdc-admin

Parameters

port *interface-list*: Specifies a space-separated list of port items. Each item specifies a port by its type and number or a range of ports in the form of *start-interface-type interface-number* **to** *end-interface-type interface-number*.

Usage guidelines

The global configuration takes effect on all specified ports. It has the same priority as the configuration on the current port.

Examples

# Enable multicast source port filtering on ports FortyGigE 1/0/1 through FortyGigE 1/0/4.

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

Related commands

igmp-snooping source-deny

version (IGMP-snooping view)

Use **version** to specify an IGMP snooping version for VLANs.

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

Syntax

version *version-number* **vlan** *vlan-list*

undo version vlan *vlan-list*

Default

The default setting is IGMPv2 snooping.

Views

IGMP-snooping view

Predefined user roles

network-admin

mdc-admin

Parameters

version-number: Specifies an IGMP snooping version, 2 or 3.

vlan *vlan-list*: Specifies a space-separated list of up to 10 VLAN items. Each item specifies a VLAN by its ID or a range of VLANs in the form of *start-vlan-id* **to** *end-vlan-id*. The VLAN ID is in the range of 1 to 4094.

Usage guidelines

You must enable IGMP snooping for the specified VLANs before you execute this command.

Examples

# Enable IGMP snooping for VLAN 2 through VLAN 10, and specify IGMP snooping version 3 for these VLANs.

```
<Sysname> system-view
[Sysname] igmp-snooping
[Sysname-igmp-snooping] enable vlan 2 to 10
[Sysname-igmp-snooping] version 3 vlan 2 to 10
```

Related commands

- **enable** (IGMP-snooping view)
- **igmp-snooping enable**

Multicast routing and forwarding commands

The term "interface" in this chapter collectively refers to VLAN interfaces and Layer 3 Ethernet interfaces. You can set an Ethernet port as a Layer 3 interface by using the **port link-mode route** command (see *Layer 2—LAN Switching Configuration Guide*).

The HPE 7904 (JG682A) or HPE 7904 TAA (JH122A) switch uses one built-in MPU (slot 0) and the HPE 7910 (JG841A) or HPE 7910 TAA (JH123A) switch uses two removable switching fabric modules (slots 10 and 11) for switching and control.

Unless otherwise stated, the term "card" collectively refers to LPUs, switching fabric modules, and MPUs.

delete ip rpf-route-static

Use **delete ip rpf-route-static** to delete all static multicast routes.

Syntax

delete ip rpf-route-static [**vpn-instance** *vpn-instance-name*]

Views

System view

Predefined user roles

network-admin

mdc-admin

Parameters

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, this command deletes all static multicast routes on the public network.

Usage guidelines

This command deletes all static multicast routes, but the **undo ip rpf-route-static** command deletes a specific static multicast route.

Examples

# Delete all static multicast routes on the public network.

```
<Sysname> system-view
[Sysname] delete ip rpf-route-static
This will erase all multicast static routes and their configurations, you must reconfigure
all static routes.
Are you sure?[Y/N]:y
```

Related commands

ip rpf-route-static

display mac-address multicast

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

Syntax

display mac-address [*mac-address* [**vlan** *vlan-id*] | [**multicast**] [**vlan** *vlan-id*] [**count**]]

Views

Any view

Predefined user roles

network-admin

network-operator

mdc-admin

mdc-operator

Parameters

mac-address: Specifies a multicast MAC address. It must be a legal multicast MAC address except 0100-5Exx-xxxx, where "x" represents any hexadecimal number from 0 to F. A multicast MAC address is the MAC address in which the least significant bit of the most significant octet is 1.

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

multicast: Specifies static multicast MAC address entries.

count: Specifies the number of static multicast MAC address entries. If you specify this keyword, the command displays the number of matching static multicast MAC address entries. If you do not specify this keyword, the command displays the contents of the matching entries rather than the entry count.

Usage guidelines

This command displays all MAC address entries, including static multicast and unicast MAC address entries, when one of the following conditions exists:

- You do not specify any parameters.
- You specify either or both of the **vlan** and **count** keywords.

Examples

# Display the static multicast MAC address entries for VLAN 2.

```
<Sysname> display mac-address multicast vlan 2
MAC Address      VLAN ID    State            Port/NickName            Aging
0100-0001-0001   2          Multicast        FGE1/0/1                 N
                                             FGE1/0/2
```

# Display the number of static multicast MAC address entries.

```
<Sysname> display mac-address multicast count
1 mac address(es) found.
```

Table 11 Command output

Field	Description
VLAN ID	ID of the VLAN to which the network device identified by the MAC address belongs.
State	Status of the MAC address. If the multicast MAC address entry is static, this field displays **Multicast**.
Port/NickName	Outgoing ports or nickname of the Egress RB in a TRILL network for the packet that is sent to the MAC address in this MAC address entry. For more information about the nickname, TRILL, and RB, see *TRILL Configuration Guide*.

Field	Description
Aging	Aging time state. If this entry never expires, this field displays **N**.
1 mac address(es) found	One static multicast MAC address entry is found.

Related commands

mac-address multicast

display mrib interface

Use **display mrib interface** to display information about the interfaces maintained by the MRIB.

Syntax

display mrib [**vpn-instance** *vpn-instance-name*] **interface** [*interface-type interface-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

mdc-admin

mdc-operator

Parameters

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, this command displays information about the interfaces maintained by the MRIB on the public network.

interface-type interface-number: Specifies an interface by its type and number. If you do not specify an interface, this command displays information about the interfaces maintained by the MRIB on all interfaces.

Examples

# Display information about the interfaces maintained by the MRIB on all interfaces on the public network.

```
<Sysname> display mrib interface
 Interface: Vlan-interface1
     Index: 0x00000001
     Current state: up
     MTU: 1500
     Type: BROADCAST
     Protocol: PIM-DM
     PIM protocol state: Enabled
     Address list:
          1. Local address : 8.12.0.2/16
             Remote address: 0.0.0.0
             Reference     : 1
             State         : NORMAL
```

Table 12 Command output

Field	Description
Interface	Interface name.
Index	Index number of the interface.
Current state	Current status of the interface: up or down.
MTU	MTU value.
Type	Interface type: • **BROADCAST**—Broadcast link interface. • **LOOP**—Loopback interface. • **REGISTER**—Register interface. • **NBMA**—NBMA interface. This field is empty if the interface is Null 0.
Protocol	Protocol running on the interface: PIM-DM, PIM-SM, IGMP, or MD.
PIM protocol state	Whether PIM is enabled: • **Enabled**. • **Disabled**.
Address list	Interface address list.
Local address	Local IP address.
Remote address	Remote end IP address. This field is displayed when the interface is vlink type.
Reference	Number of times for which the address has been referenced.
State	Status of the interface address: • **NORMAL**. • **DEL**.

display multicast boundary

Use **display multicast boundary** to display multicast boundary information.

Syntax

display multicast [**vpn-instance** *vpn-instance-name*] **boundary** [*group-address* [*mask-length* | *mask*]] [**interface** *interface-type interface-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

mdc-admin

mdc-operator

Parameters

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, this command displays multicast boundary information on the public network.

group-address: Specifies a multicast group address in the range of 224.0.0.0 to 239.255.255.255. If you do not specify a multicast group, this command displays multicast boundary information of all multicast groups.

mask-length: Specifies an address mask length in the range of 4 to 32. The default is 32.

mask: Specifies an address mask. The default is 255.255.255.255.

interface *interface-type interface-number*: Specifies an interface by its type and number. If you do not specify an interface, this command displays multicast boundary information on all interfaces.

Examples

# Display multicast boundary information of all multicast groups on all interfaces on the public network.

```
<Sysname> display multicast boundary
 Boundary            Interface
 224.1.1.0/24        Vlan1
 239.2.2.0/24        Vlan2
```

Table 13 Command output

Field	Description
Boundary	Multicast group that corresponds to the multicast boundary.
Interface	Boundary interface that corresponds to the multicast boundary.

Related commands

multicast boundary

display multicast forwarding event

Use **display multicast forwarding event** to display statistics for multicast forwarding events.

Syntax

In standalone mode:

display multicast [**vpn-instance** *vpn-instance-name*] **forwarding event** [**slot** *slot-number*]

In IRF mode:

display multicast [**vpn-instance** *vpn-instance-name*] **forwarding event** [**chassis** *chassis-number* **slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

mdc-admin

mdc-operator

Parameters

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, this command displays statistics for multicast forwarding events on the public network.

slot *slot-number*: Specifies a card by its slot number. If you do not specify a card, this command displays statistics for multicast forwarding events on the MPU or the switching fabric modules. (In standalone mode.)

chassis *chassis-number* **slot** *slot-number*: Specifies a card on an IRF member device. The *chassis-number* argument specifies the IRF member device ID, and the *slot-number* argument specifies the number of the slot where the card resides. If you do not specify a member device, this command displays statistics for multicast forwarding events on all MPUs or switching fabric modules in the IRF fabric. (In IRF mode.)

Examples

# Display statistics for multicast forwarding events on the public network.

```
<Sysname> display multicast forwarding event
Total entry active event sent: 0
Total entry inactive event sent: 0
Total NoCache event sent: 2
Total NoCache event dropped: 0
Total WrongIF event sent: 0
Total WrongIF event dropped: 0
Total SPT switch event sent: 0
NoCache rate limit: 1024 packets/s
WrongIF rate limit: 1 packets/10s
Total timer of register suppress timeout: 0
```

Table 14 Command output

Field	Description
Total entry active event sent	Number of times for which the entry-active event has been sent.
Total entry inactive event sent	Number of times for which the entry-inactive event has been sent.
Total NoCache event sent	Number of times for which the NoCache event has been sent.
Total NoCache event dropped	Number of times for which the NoCache event has been dropped.
Total WrongIF event sent	Number of times for which the WrongIF event has been sent.
Total WrongIF event dropped	Number of times for which the WrongIF event has been dropped.
Total SPT switch event sent	Number of times for which the SPT-switch event has been sent.
NoCache rate limit	Rate limit for sending the NoCache event, in pps.
WrongIF rate limit	Rate limit for sending the WrongIF event, in packets per 10 seconds.
Total timer of register suppress timeout	Total number of times for which the registration suppression has timed out.

Related commands

reset multicast forwarding event

display multicast forwarding-table

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

Syntax

In standalone mode:

display multicast [**vpn-instance** *vpn-instance-name*] **forwarding-table** [*source-address* [**mask** { *mask-length* | *mask* }] | *group-address* [**mask** { *mask-length* | *mask* }] | **incoming-interface**

interface-type interface-number **| outgoing-interface** { **exclude** **|** **include** **|** **match** } *interface-type interface-number* **| slot** *slot-number***| statistics**] *

In IRF mode:

display multicast [**vpn-instance** *vpn-instance-name*] **forwarding-table** [*source-address* [**mask** { *mask-length* **|** *mask* }] **|** *group-address* [**mask** { *mask-length* **|** *mask* }] **| chassis** *chassis-number* **slot** *slot-number* **| incoming-interface** *interface-type interface-number* **| outgoing-interface** { **exclude | include | match** } *interface-type interface-number* **| statistics**] *

Views

Any view

Predefined user roles

network-admin

network-operator

mdc-admin

mdc-operator

Parameters

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, this command displays multicast forwarding entries on the public network.

source-address: Specifies a multicast source address.

group-address: Specifies a multicast group address in the range of 224.0.0.0 to 239.255.255.255.

mask-length: Specifies an address mask length. The default value is 32. For a multicast group address, the value range for this argument is 4 to 32. For a multicast source address, the value range for this argument is 0 to 32.

mask: Specifies an address mask. The default value is 255.255.255.255.

incoming-interface: Specifies the multicast forwarding entries that contain the specified incoming interface.

interface-type interface-number: Specifies an incoming interface by its type and number.

outgoing-interface: Specifies the multicast forwarding entries that contain the specified outgoing interface.

exclude: Specifies the multicast forwarding entries that do not contain the specified interface in the outgoing interface list.

include: Specifies the multicast forwarding entries that contain the specified interface in the outgoing interface list.

match: Specifies the forwarding entries that contain only the specified interface in the outgoing interface list.

slot *slot-number*: Specifies a card by its slot number. If you do not specify a card, this command displays multicast forwarding entries on the main processing unit (MPU) or the switching fabric modules. (In standalone mode.)

chassis *chassis-number* **slot** *slot-number*: Specifies a card on an IRF member device. The *chassis-number* argument specifies the IRF member device ID, and the *slot-number* argument specifies the number of the slot where the card resides. If you do not specify a member device, this command displays multicast forwarding entries on all MPUs or switching fabric modules in the IRF fabric. (In IRF mode.)

statistics: Displays statistics for the multicast forwarding table.

Examples

# Display multicast forwarding entries on the public network.

```
<Sysname> display multicast forwarding-table
Total 1 entry, 1 matched

00001. (172.168.0.2, 227.0.0.1)
     Flags: 0x0
     Uptime: 00:08:32, Timeout in: 00:03:26
     Incoming interface: Vlan-interface10
     List of 1 outgoing interface:
       1: Vlan-interface20
     Matched 19648 packets(20512512 bytes), Wrong If 0 packet
     Forwarded 19648 packets(20512512 bytes)
```

Table 15 Command output

Field	Description
Total 1 entry, 1 matched	Total number of (S, G) entries and total number of matching (S, G) entries.
00001	Sequence number of the (S, G) entry.
(172.168.0.2,227.0.0.1)	(S, G) entry.
Flags	Entry flag. This field displays one flag or the sum of multiple flags. In this example, the value 0x0 means that the entry has only one flag 0x0. The following entries are available for an entry: • **0x0**—The entry is in correct state. • **0x1**—The entry is in inactive state. • **0x2**—The entry is null. • **0x4**—The entry fails to update. • **0x8**—Outgoing interface information fails to update for the entry. • **0x10**—Data-group information fails to update for the entry. • **0x20**—A register outgoing interface is available. • **0x40**—The entry is to be deleted. • **0x80**—The entry is in registration suppression state. • **0x100**—The entry is being deleted. • **0x200**—The entry is in GR state. • **0x400**—The entry has the VLAN interface of the super VLAN. • **0x800**—The entry has the associated ARP entry for the multicast source address.
Uptime	Length of time for which the (S, G) entry has been up.
Timeout in	Length of time in which the (S, G) entry will expire.
Incoming interface	Incoming interface of the (S, G) entry.
List of 1 outgoing interface:	Outgoing interface list of the (S, G) entry.
Matched 19648 packets(20512512 bytes), Wrong If 0 packet	Number of packets (bytes) that match the (S, G) entry, and number of packets with incoming interface errors.
Forwarded 19648 packets(20512512 bytes)	Number of packets (bytes) that have been forwarded.

Related commands

reset multicast forwarding-table

display multicast routing-table

Use **display multicast routing-table** to display multicast routing entries.

Syntax

display multicast [**vpn-instance** *vpn-instance-name*] **routing-table** [*source-address* [**mask** { *mask-length* | *mask* }] | *group-address* [**mask** { *mask-length* | *mask* }] | **incoming-interface** *interface-type interface-number* | **outgoing-interface** { **exclude** | **include** | **match** } *interface-type interface-number*] *

Views

Any view

Predefined user roles

network-admin

network-operator

mdc-admin

mdc-operator

Parameters

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, this command displays multicast routing entries on the public network.

source-address: Specifies a multicast source address.

group-address: Specifies a multicast group address in the range of 224.0.0.0 to 239.255.255.255.

mask-length: Specifies an address mask length. The default value is 32. For a multicast group address, the value range for this argument is 4 to 32. For a multicast source address, the value range for this argument is 0 to 32.

mask: Specifies an address mask. The default is 255.255.255.255.

incoming-interface: Specifies the multicast routing entries that contain the specified incoming interface.

interface-type interface-number: Specifies an incoming interface by its type and number.

outgoing-interface: Specifies the multicast routing entries that contain the specified outgoing interface.

exclude: Specifies the multicast routing entries that do not contain the specified interface in the outgoing interface list.

include: Specifies the multicast routing entries that contain the specified interface in the outgoing interface list.

match: Specifies the multicast routing entries that contain only the specified interface in the outgoing interface list.

Usage guidelines

Multicast routing tables are the basis of multicast forwarding. You can display the establishment state of an (S, G) entry by examining the multicast routing table.

Examples

# Display multicast routing entries on the public network.

```
<Sysname> display multicast routing-table
 Total 1 entry

 00001. (172.168.0.2, 227.0.0.1)
       Uptime: 00:00:28
       Upstream Interface: Vlan-interface1
       List of 2 downstream interfaces
           1:  Vlan-interface2
           2:  Vlan-interface3
```

Table 16 Command output

Field	Description
Total 1 entry	Total number of (S, G) entries.
00001	Sequence number of the (S, G) entry.
(172.168.0.2, 227.0.0.1)	(S, G) entry.
Uptime	Length of time for which the (S, G) entry has been up.
Upstream Interface	Incoming interface of the (S, G) entry that multicast packets should arrive at.
List of 2 downstream interfaces	List of downstream interfaces that need to forward multicast packets.

Related commands

reset multicast routing-table

display multicast routing-table static

Use **display multicast routing-table static** to display static multicast routing entries.

Syntax

display multicast [**vpn-instance** *vpn-instance-name*] **routing-table static** [*source-address* { *mask-length* | *mask* }]

Views

Any view

Predefined user roles

network-admin

network-operator

mdc-admin

mdc-operator

Parameters

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, this command displays static multicast routes on the public network.

source-address: Specifies a multicast source address.

mask-length: Specifies an address mask length in the range of 0 to 32.

mask: Specifies an address mask.

Usage guidelines

This command displays only valid static multicast routes.

Examples

# Display static multicast routing entries on the public network.

```
<Sysname> display multicast routing-table static
Destinations : 3        Routes : 4
Destination/Mask   Pre  RPF Neighbor    Interface
1.1.0.0/16         10   7.12.0.1        Vlan12
                        7.11.0.1        Vlan11
2.2.2.0/24         20   7.11.0.1        Vlan11
3.3.3.3/32         50   7.12.0.1        Vlan12
```

Table 17 Command output

Field	Description
Destinations	Number of the multicast destination addresses.
Routes	Number of routes.
Destination/Mask	Destination address and mask length.
Pre	Route preference.
RPF Neighbor	IP address of the RPF neighbor to the reachable destination.
Interface	Outgoing interface to the reachable destination.

display multicast rpf-info

Use **display multicast rpf-info** to display RPF information for a multicast source.

Syntax

display multicast [**vpn-instance** *vpn-instance-name*] **rpf-info** *source-address* [*group-address*]

Views

Any view

Predefined user roles

network-admin

network-operator

mdc-admin

mdc-operator

Parameters

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, this command displays RPF information for a multicast source on the public network.

source-address: Specifies a multicast source address.

group-address: Specifies a multicast group address in the range of 224.0.1.0 to 239.255.255.255.

Examples

# Display RPF information for the multicast source 192.168.1.55 on the public network.

```
<Sysname> display multicast rpf-info 192.168.1.55
```

```
 RPF information about source 192.168.1.55:
     RPF interface: Vlan-interface1, RPF neighbor: 10.1.1.1
     Referenced route/mask: 192.168.1.0/24
     Referenced route type: igp
     Route selection rule: preference-preferred
     Load splitting rule: disable
```

Table 18 Command output

Field	Description
RPF neighbor	IP address of the RPF neighbor.
Referenced route/mask	Referenced route and its mask length.
Referenced route type	Type of the referenced route: • **igp**—IGP unicast route. • **egp**—EGP unicast route. • **unicast (direct)**—Directly connected unicast route. • **unicast**—Other unicast routes, such as static unicast route. • **multicast static**—Static multicast route.
Route selection rule	Rule for RPF route selection: • Route preference. • Longest prefix match.
Load splitting rule	Status of the load splitting rule: • Enabled. • Disabled.

Related commands

- **display multicast forwarding-table**
- **display multicast routing-table**

ip rpf-route-static

Use **ip rpf-route-static** to configure a static multicast route.

Use **undo ip rpf-route-static** to delete a static multicast route.

Syntax

ip rpf-route-static [**vpn-instance** *vpn-instance-name*] *source-address* { *mask-length* | *mask* } { *rpf-nbr-address* | *interface-type interface-number* } [**preference** *preference*]

undo ip rpf-route-static [**vpn-instance** *vpn-instance-name*] *source-address* { *mask-length* | *mask* } { *rpf-nbr-address* | *interface-type interface-number* }

Default

Static multicast routes do not exist.

Views

System view

Predefined user roles

network-admin

mdc-admin

Parameters

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, this command configures a static multicast route on the public network.

source-address: Specifies a multicast source address.

mask-length: Specifies an address mask length in the range of 0 to 32.

mask: Specifies an address mask.

rpf-nbr-address: Specifies an RPF neighbor by its IP address.

interface-type interface-number: Specifies an interface by its type and number. The interface connects the RPF neighbor.

preference: Specifies a route preference in the range of 1 to 255. The default value is 1.

Usage guidelines

In the same multicast source address range, you can configure up to 16 RPF neighbors.

When you configure an RPF neighbor on a Layer 3 interface, which is a Layer 3 Ethernet interface, Loopback interface, or VLAN interface, you must specify the IP address of the neighbor rather than the type and number of the Layer 3 interface.

The configured static multicast route might not take effect due to one of the following reasons:

- The outgoing interface iteration fails.
- The specified interface is not on the public network or the same VPN instance as the current interface.
- The specified interface is not a point-to-point interface.
- The specified interface is in down state.

If multiple static multicast routes within the same multicast source address range are available, only the one with the highest priority can become active. Therefore, after you configure a static multicast route, use the **display multicast routing-table static** command to verify that the configured static multicast route has taken effect.

The **undo ip rpf-route-static** command deletes the specified static multicast route, but the **delete ip rpf-route-static** command deletes all static multicast routes.

Examples

# On the public network, configure a static multicast route to the multicast source groups 10.1.1.1/24, and specify a router with the IP address of 192.168.1.23 as its RPF neighbor.

```
<Sysname> system-view
[Sysname] ip rpf-route-static 10.1.1.1 24 192.168.1.23
```

Related commands

- **delete ip rpf-route-static**
- **display multicast routing-table static**

load-splitting (MRIB view)

Use **load-splitting** to enable load splitting of multicast traffic.

Use **undo load-splitting** to restore the default.

Syntax

load-splitting { **source** | **source-group** }

undo load-splitting

Default

Load splitting of multicast traffic is disabled.

Views

MRIB view

Predefined user roles

network-admin

mdc-admin

Parameters

source: Specifies load splitting on a per-source basis.

source-group: Specifies load splitting both on a per-source basis and on a per-group basis.

Examples

# Enable load splitting of multicast traffic on a per-source basis on the public network.

```
<Sysname> system-view
[Sysname] multicast routing
[Sysname-mrib] load-splitting source
```

longest-match (MRIB view)

Use **longest-match** to specify the longest prefix match principle for RPF route selection.

Use **undo longest-match** to restore the default.

Syntax

longest-match

undo longest-match

Default

Route preference is used for RPF route selection.

Views

MRIB view

Predefined user roles

network-admin

mdc-admin

Examples

# Specify the longest prefix match principle for RPF route selection on the public network.

```
<Sysname> system-view
[Sysname] multicast routing
[Sysname-mrib] multicast longest-match
```

mac-address multicast

Use **mac-address multicast** to configure a static multicast MAC address entry.

Use **undo mac-address multicast** to delete a static multicast MAC address entry.

Syntax

In system view:

mac-address multicast *mac-address* **interface** *interface-list* **vlan** *vlan-id*

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

In Ethernet interface view or Layer 2 aggregate interface view:

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

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

Default

Static multicast MAC address entries do not exist.

Views

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

Predefined user roles

network-admin

mdc-admin

Parameters

mac-address: Specifies a static multicast MAC address, in the format H-H-H. It must be an unused multicast MAC address except 0100-5Exx-xxxx, where "x" represents any hexadecimal number from 0 to F. A multicast MAC address is the MAC address in which the least significant bit of the most significant octet is 1.

interface *interface-list*: Specifies a space-separated list of up to four interface items. Each item specifies an interface or an interface list in the format of *start-interface-type interface-number* **to** *end-interface-type interface-number*. The *interface-type interface-number* argument specifies an interface by its type and number.

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

Usage guidelines

You can configure static multicast MAC address entries on the specified interface in system view or on the current interface in interface view.

You do not need to enable IP multicast routing before you execute this command.

If you do not specify the **multicast** keyword, the **undo mac-address** command deletes all MAC address entries, including static unicast and multicast MAC address entries.

Examples

# Create a multicast entry for 0100-0001-0001 in VLAN 2, and configure FortyGigE 1/0/1 through FortyGigE 1/0/5 in VLAN 2 as outgoing ports.

```
<Sysname> system-view
[Sysname] mac-address multicast 0100-0001-0001 interface fortygige 1/0/1 to fortygige
1/0/5 vlan 2
```

# Configure a multicast entry for 0100-0001-0001 on FortyGigE 1/0/1 in VLAN 2.

```
<Sysname> system-view
[Sysname] interface fortygige 1/0/1
[Sysname-FortyGigE1/0/1] mac-address multicast 0100-0001-0001 vlan 2
```

Related commands

display mac-address multicast

multicast boundary

Use **multicast boundary** to configure a multicast forwarding boundary.

Use **undo multicast boundary** to remove a multicast forwarding boundary.

Syntax

multicast boundary *group-address* { *mask-length* | *mask* }

undo multicast boundary { *group-address* { *mask-length* | *mask* } | **all** }

Default

Multicast forwarding boundaries are not configured.

Views

Interface view

Predefined user roles

network-admin

mdc-admin

Parameters

group-address: Specifies a multicast group address in the range of 224.0.0.0 to 239.255.255.255.

mask-length: Specifies an address mask length in the range of 4 to 32.

mask: Specifies an address mask.

all: Specifies all forwarding boundaries configured on the interface.

Usage guidelines

A multicast forwarding boundary sets the boundary condition for the multicast groups in the specified address range. If the destination address of a multicast packet matches the set boundary condition, the packet is not forwarded.

You do not need to enable IP multicast routing before executing this command.

An interface can act as a forwarding boundary for multiple multicast groups in different address ranges. To achieve this, use this command on the interface for each multicast address range.

Assume that Set A and Set B are multicast forwarding boundary sets with different address ranges, and B is a subset of A. A takes effect on the interface no matter whether A is configured earlier or later than B.

Examples

# Configure VLAN-interface 100 as the forwarding boundary of multicast groups in the range of 239.2.0.0/16.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] multicast boundary 239.2.0.0 16
```

Related commands

display multicast boundary

multicast routing

Use **multicast routing** to enable IP multicast routing and enter MRIB view.

Use **undo multicast routing** to disable IP multicast routing.

Syntax

multicast routing [**vpn-instance** *vpn-instance-name*]

undo multicast routing [**vpn-instance** *vpn-instance-name*]

Default

IP multicast routing is disabled.

Views

System view

Predefined user roles

network-admin

mdc-admin

Parameters

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, this command enables IP multicast routing on the public network.

Usage guidelines

Other Layer 3 multicast commands takes effect only when you enable IP multicast routing on the public network or for a VPN instance.

The switch does not forward any multicast packets before IP multicast routing is enabled.

Examples

# Enable IP multicast routing and enter MRIB view on the public network.

```
<Sysname> system-view
[Sysname] multicast routing
[Sysname-mrib]
```

# Enable IP multicast routing and enter MRIB view in the VPN instance **mvpn**.

```
<Sysname> system-view
[Sysname] multicast routing vpn-instance mvpn
[Sysname-mrib-mvpn]
```

reset multicast forwarding event

Use **reset multicast forwarding event** to clear statistics for multicast forwarding events.

Syntax

reset multicast [**vpn-instance** *vpn-instance-name*] **forwarding event**

Views

User view

Predefined user roles

network-admin

mdc-admin

Parameters

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, this command clears statistics for the multicast forwarding events on the public network.

Examples

# Clear statistics for the multicast forwarding events on the public network.

```
<Sysname> reset multicast forwarding event
```

Related commands

display multicast forwarding event

reset multicast forwarding-table

Use **reset multicast forwarding-table** to clear multicast forwarding entries.

Syntax

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

Views

User view

Predefined user roles

network-admin

mdc-admin

Parameters

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, this command clears multicast forwarding entries on the public network.

source-address: Specifies a multicast source address.

group-address: Specifies a multicast group address in the range of 224.0.0.0 to 239.255.255.255.

mask-length: Specifies an address mask length. The default value is 32. For a multicast group address, the value range for this argument is 4 to 32. For a multicast source address, the value range for this argument is 0 to 32.

mask: Specifies an address mask. The default is 255.255.255.255.

incoming-interface: Specifies the multicast forwarding entries that contain the specified incoming interface.

interface-type interface-number: Specifies an incoming interface by its type and number.

all: Specifies all multicast forwarding entries.

Usage guidelines

When you clear a multicast forwarding entry, the associated multicast routing entry is also cleared.

Examples

# Clear multicast forwarding entries for the multicast group 225.5.4.3 on the public network.

```
<Sysname> reset multicast forwarding-table 225.5.4.3
```

Related commands

display multicast forwarding-table

reset multicast routing-table

Use **reset multicast routing-table** to clear multicast routing entries.

Syntax

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

Views

User view

Predefined user roles

network-admin

mdc-admin

Parameters

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, this command clears the multicast routing entries on the public network.

source-address: Specifies a multicast source address.

group-address: Specifies a multicast group address in the range of 224.0.0.0 to 239.255.255.255.

mask-length: Specifies an address mask length. The default value is 32. For a multicast group address, the value range for this argument is 4 to 32. For a multicast source address, the value range for this argument is 0 to 32.

mask: Specifies an address mask. The default is 255.255.255.255.

incoming-interface: Specifies the routing entries that contain the specified incoming interface.

interface-type interface-number: Specifies an incoming interface by its type and number.

all: Specifies all multicast routing entries.

Usage guidelines

When you clear a multicast routing entry, the associated multicast forwarding entry is also cleared.

Examples

# Clear multicast routing entries for the multicast group 225.5.4.3 on the public network.

```
<Sysname> reset multicast routing-table 225.5.4.3
```

Related commands

display multicast routing-table

IGMP commands

The term "interface" in this chapter collectively refers to VLAN interfaces and Layer 3 Ethernet interfaces. You can set an Ethernet port as a Layer 3 interface by using the **port link-mode route** command (see *Layer 2—LAN Switching Configuration Guide*).

display igmp group

Use **display igmp group** to display information about IGMP multicast groups (the multicast groups that receiver hosts have dynamically joined through IGMP).

Syntax

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

Views

Any view

Predefined user roles

network-admin

network-operator

mdc-admin

mdc-operator

Parameters

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, this command displays information about IGMP multicast groups on the public network.

group-address: Specifies a multicast group by its address in the range of 224.0.1.0 to 239.255.255.255. If you do not specify a multicast group, this command displays information about all IGMP multicast groups.

interface *interface-type interface-number*: Specifies an interface by its type and number. If you do not specify an interface, this command displays information about IGMP multicast groups for all interfaces.

static: Displays information about the multicast groups that interfaces have joined statically. If you do not specify this keyword, the command displays information about IGMP multicast groups.

verbose: Displays detailed information about IGMP multicast groups.

Examples

# Display information about IGMP multicast groups on the public network.

```
<Sysname> display igmp group
IGMP groups in total: 3
 Vlan-interface1(10.10.1.20):
  IGMP groups reported in total: 3
   Group address   Last reporter   Uptime      Expires
   225.1.1.1       10.10.1.10      00:02:04    00:01:15
   225.1.1.2       10.10.1.10      00:02:04    00:01:15
   225.1.1.3       10.10.1.10      00:02:04    00:01:17
```

Table 19 Command output

Field	Description
IGMP groups in total	Total number of IGMP multicast groups.
IGMP groups reported in total	Total number of IGMP multicast groups that the interface joins dynamically.
Group address	Multicast group address.
Last reporter	Address of the last receiver host that reported its membership to the multicast group.
Uptime	Length of time since the multicast group was reported.
Expire	Remaining time for the multicast group, where **Off** means that the timer is disabled.

# Display detailed information about the IGMP multicast group 225.1.1.1 on the public network. In this example, the switch runs IGMPv3.

```
<Sysname> display igmp group 225.1.1.1 verbose
 Vlan-interface1(10.10.1.20):
  IGMP groups reported in total: 1
   Group: 225.1.1.1
     Uptime: 00:00:34
     Exclude expires: 00:04:16
     Last reporter: 10.10.1.10
     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: 00:00:55
     Source list (sources in total: 1):
       Source: 10.1.1.1
          Uptime: 00:00:03
          V3 expires: 00:04:16
          Last-member-query-counter: 0
          Last-member-query-timer-expiry: Off
```

Table 20 Command output

Field	Description
IGMP groups reported in total	Total number of IGMP multicast groups that the interface joins dynamically.
Group	Multicast group address.
Uptime	Length of time since the multicast group was reported.
Exclude expires	Remaining time for the multicast group in Exclude mode, where **Off** means that the timer is disabled.
Last reporter	Address of the last receiver host that reported its membership to this multicast group.
Last-member-query-counter	Number of IGMP group-specific queries or IGMP source-and-group-specific queries sent for the multicast group.
Last-member-query-timer-expiry	Remaining time for the last member query timer for the multicast group, where **Off** means that the timer is disabled.

Field	Description
Group mode	Multicast source filtering mode: - **Include**—Include mode. - **Exclude**—Exclude mode.
Version1-host-present-timer-expiry	Remaining time for the IGMPv1 host present timer, where **Off** means that the timer is disabled. This field is displayed only when the switch runs IGMPv2 or IGMPv3.
Version2-host-present-timer-expiry	Remaining time for the IGMPv2 host present timer, where **Off** means that the timer is disabled. This field is displayed only when the switch runs IGMPv3.
Source list (sources in total: 1)	List of multicast sources and total number of multicast sources. This field is displayed only when the switch runs IGMPv3.
Source	Multicast source address. This field is displayed only when the switch runs IGMPv3.
Uptime	Length of time since the multicast source was reported. This field is displayed only when the switch runs IGMPv3.
V3 expires	Remaining time for the multicast source when the switch runs IGMPv3, where **Off** means that the timer is disabled. This field is displayed only when the switch runs IGMPv3.
Last-member-query-counter	Number of IGMP group-specific queries or IGMP group-and-source-specific queries sent for the multicast source and group. This field is displayed only when the switch runs IGMPv3.
Last-member-query-timer-expiry	Remaining time for the last member query timer for the multicast source and group, where **Off** means that the timer is disabled. This field is displayed only when the switch runs IGMPv3.

Related commands

reset igmp group

display igmp interface

Use **display igmp interface** to display IGMP information for interfaces.

Syntax

display igmp [**vpn-instance** *vpn-instance-name*] **interface** [*interface-type interface-number*] [**host**] [**verbose**]

Views

Any view

Predefined user roles

network-admin

network-operator

mdc-admin

mdc-operator

Parameters

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, this command displays IGMP information for interfaces on the public network.

interface-type interface-number: Specifies an interface by its type and number. If you do not specify an interface, this command displays IGMP information for all interfaces.

host: Displays information about the interfaces enabled with the IGMP host feature. If you do not specify this keyword, the command displays IGMP information for interfaces enabled with IGMP and those enabled with the IGMP host feature. For more information about the IGMP host feature, see *VXLAN Configuration Guide*.

verbose: Displays detailed IGMP information.

Examples

# Display detailed IGMP information for VLAN-interface 1 on the public network.

```
<Sysname> display igmp interface vlan-interface 1 verbose
 Vlan-interface1(10.10.1.20):
   IGMP is enabled.
   IGMP version: 2
   Query interval for IGMP: 125s
   Other querier present time for IGMP: 255s
   Maximum query response time for IGMP: 10s
   Last member query interval: 1s
   Last member query count: 2
   Startup query interval: 31s
   Startup query count: 2
   General query timer expiry (hh:mm:ss): 00:00:54
   Querier for IGMP: 10.10.1.20 (This router)
   IGMP activity: 1 join(s), 0 leave(s)
   Multicast routing on this interface: Enabled
   Robustness: 2
   Require-router-alert: Disabled
   Fast-leave: Disabled
   Startup-query: Off
   Other-querier-present-timer-expiry (hh:mm:ss): --:--:--
  IGMP groups reported in total: 1
```

# Display detailed IGMP information for all interfaces enabled with the IGMP host feature on the public network.

```
<Sysname> display igmp interface host verbose
 Vlan-interface2(20.10.1.20):
   IGMP host is enabled.
   IGMP version: 2
   Multicast routing on this interface: Enabled
   Require-router-alert: Disabled
   Version1-querier-present-timer-expiry (hh:mm:ss): --:--:--
```

Table 21 Command output

Field	Description
Vlan-interface1(10.10.1.20)	Interface (IP address).

Field	Description
Query interval for IGMP	IGMP general query interval, in seconds.
Other querier present time for IGMP	Other querier present interval, in seconds.
Maximum query response time for IGMP	Maximum response time for IGMP general queries, in seconds.
Last member query interval	IGMP last member query interval, in seconds.
Last member query count	Number of IGMP group-specific queries or IGMP group-and-source-specific queries sent for the multicast group.
Startup query interval	IGMP startup query interval, in seconds.
Startup query count	Number of IGMP general queries that the switch sends on startup.
General query timer expiry	Remaining time for the IGMP general query timer. If the timer never expires, the field displays **Off**.
Querier for IGMP	IP address of the IGMP querier. If the switch is configured with IGMPv1 and it is not the IGMP querier, this field is not displayed.
No querier elected	No querier is elected. This field is displayed only when the switch runs IGMPv1 and it is not the IGMP querier. NOTE: In IGMPv1, the PIM DR acts as the IGMP querier. You can use the **display pim interface** command to display IGMP querier information.
IGMP activity: 1 join(s), 0 leave(s)	Statistics of IGMP activities: • **join(s)**—Total number of multicast groups that this interface has joined. • **leave(s)**—Total number of multicast groups that this interface has left.
Multicast routing on this interface	Whether the multicast routing and forwarding is enabled.
Robustness	Robustness variable of the IGMP querier.
Require-router-alert	Whether the function of dropping of IGMP messages without Router-Alert is enabled.
Fast-leave	Whether the fast-leave processing is enabled.
Startup-query	Whether the IGMP querier sends IGMP general queries at the startup query interval on startup: • **On**—The IGMP querier performs the above action. • **Off**—The IGMP querier does not perform the above action.
Other-querier-present-timer-expiry	Remaining time for the other querier present timer. If the timer never expires, the field displays **Off**.
IGMP groups reported in total	Total number of multicast groups that the interface has dynamically joined. This field is not displayed if the interface does not join any multicast groups.
IGMP host is enabled	The IGMP host feature is enabled.
Version1-querier-present-timer-expiry	Remaining time for IGMPv1 querier present timer.
Version2-querier-present-timer-expiry	Remaining time for IGMPv2 querier present timer.

igmp enable

Use **igmp enable** to enable IGMP on an interface.

Use **undo igmp enable** to disable IGMP on an interface.

Syntax

igmp enable

undo igmp enable

Default

IGMP is disabled on all interfaces.

Views

Interface view

Predefined user roles

network-admin

mdc-admin

Usage guidelines

This command takes effect only when IP multicast routing is enabled on the public network or for a VPN instance to which the interface belongs.

You must enable IGMP on an interface to make the IGMP configurations on this interface take effect.

Examples

# Enable IP multicast routing, and enable IGMP on VLAN-interface 100 on the public network.

```
<Sysname> system-view
[Sysname] multicast routing
[Sysname-mrib] quit
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] igmp enable
```

Related commands

multicast routing

igmp fast-leave

Use **igmp fast-leave** to enable fast-leave processing on an interface.

Use **undo igmp fast-leave** to disable fast-leave processing on an interface.

Syntax

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

undo igmp fast-leave

Default

Fast-leave processing is disabled. The IGMP querier sends IGMP group-specific queries or IGMP group-and-source-specific queries after receiving an IGMP leave message from a host, instead of sending a leave notification directly to the upstream.

Views

Interface view

Predefined user roles

network-admin

mdc-admin

Parameters

acl-number: Specifies an IPv4 basic ACL by its number in the range of 2000 to 2999. If you specify an ACL, this command takes effect only on the multicast groups that the ACL permits. The command takes effect on all multicast groups when one of the following conditions exists:

- You do not specify an ACL.
- The specified ACL does not exist.
- The specified ACL does not contain any valid rules.

Usage guidelines

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

- For the rule to take effect, do not specify the **vpn-instance** *vpn-instance* option.
- The **source** *source-address source-wildcard* option specifies a multicast group address.
- Among the other optional parameters, only the **fragment** keyword and the **time-range** *time-range-name* option take effect.

Examples

# Enable fast-leave processing on VLAN-interface 100.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] igmp fast-leave
```

igmp group-policy

Use **igmp group-policy** to configure a multicast group policy for an interface to control the multicast groups that the receiver hosts on an interface can join.

Use **undo igmp group-policy** to remove the multicast group policy.

Syntax

igmp group-policy *acl-number* [*version-number*]

undo igmp group-policy

Default

An interface is not configured with a multicast group policy, and receiver hosts attached to the interface can join any multicast groups.

Views

Interface view

Predefined user roles

network-admin

mdc-admin

Parameters

acl-number: Specifies an IPv4 basic or advanced ACL by its number in the range of 2000 to 3999. Receiver hosts can join only the multicast groups that the ACL permits. If the specified ACL does not exist or the ACL does not have valid rules, receiver hosts cannot join any multicast groups.

version-number: Specifies an IGMP version in the range of 1 to 3. By default, the configured group policy applies to IGMP reports of all versions.

Usage guidelines

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

- For the rule to take effect, do not specify the **vpn-instance** *vpn-instance* option.
- In a basic ACL, the **source** *source-address source-wildcard* option specifies a multicast group address.
- In an advanced ACL, the **source** *source-address source-wildcard* option specifies a multicast source address. The **destination** *dest-address dest-wildcard* option specifies a multicast group address.

  To match the following IGMP reports, set the **source** *source-address source-wildcard* option to 0.0.0.0:
  - IGMPv1 and IGMPv2 reports.
  - IGMPv3 IS_EX and IGMPv3 TO_EX reports that do not carry multicast source addresses.
- Among the other optional parameters, only the **fragment** keyword and the **time-range** *time-range-name* option take effect.

This command does not take effect on static member interfaces because static member interfaces do not send IGMP reports.

Examples

# Configure a multicast group policy so that receiver hosts attached to VLAN-interface 100 can join only the multicast group 225.1.1.1.

```
<Sysname> system-view
[Sysname] acl number 2005
[Sysname-acl-basic-2005] rule permit source 225.1.1.1 0
[Sysname-acl-basic-2005] quit
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] igmp group-policy 2005
```

igmp static-group

Use **igmp static-group** to configure an interface as a static member of a multicast group.

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

Syntax

igmp static-group *group-address* [**source** *source-address*]

undo igmp static-group { **all |** *group-address* [**source** *source-address*] }

Default

An interface is not a static member of any multicast groups.

Views

Interface view

Predefined user roles

network-admin

mdc-admin

Parameters

group-address: Specifies a multicast group by its address in the range of 224.0.1.0 to 239.255.255.255.

source-address: Specifies a multicast source address. If you do not specify a multicast source, this command configures an interface as a static member of the multicast groups with all multicast source addresses.

all: Specifies all multicast groups that the interface has statically joined.

Usage guidelines

If the specified multicast address is in the SSM multicast address range, you must specify a multicast source address at the same time. Otherwise, IGMP routing entries cannot be established. No such a restriction exists if the specified multicast group address is not in the SSM multicast address range.

Examples

# Configure VLAN-interface 100 as a static member of the multicast group 224.1.1.1.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] igmp static-group 224.1.1.1
```

# Configure VLAN-interface 100 as a static member of the multicast source and group (192.168.1.1, 232.1.1.1).

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] igmp static-group 232.1.1.1 source 192.168.1.1
```

igmp version

Use **igmp version** to specify an IGMP version for an interface.

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

Syntax

igmp version *version-number*

undo igmp version

Default

The default IGMP version is 2.

Views

Interface view

Predefined user roles

network-admin

mdc-admin

Parameters

version-number: Specifies an IGMP version in the range of 1 to 3.

Examples

# Specify IGMPv1 for VLAN-interface 100.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] igmp version 1
```

reset igmp group

Use **reset igmp group** to clear dynamic entries for IGMP multicast groups.

Syntax

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

Views

User view

Predefined user roles

network-admin

mdc-admin

Parameters

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, this command clears dynamic IGMP multicast group entries on the public network.

all: Specifies all interfaces (the first **all**), or all IGMP multicast groups (the second **all**).

interface-type interface-number: Specifies an interface by its type and number.

group-address: Specifies a multicast group by its address in the range of 224.0.0.0 to 239.255.255.255.

source-address: Specifies a multicast source address. If you do not specify a multicast source, this command clears dynamic IGMP multicast group entries for all multicast sources.

mask: Specifies an address mask. The default is 255.255.255.255.

mask-length: Specifies an address mask length. The default is 32. For a multicast group address, the value range for this argument is 4 to 32. For a multicast source address, the value range for this argument is 0 to 32.

Usage guidelines

This command might interrupt the multicast information transmission.

Examples

# Clear dynamic IGMP multicast group entries for all interfaces on the public network.

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

# Clear dynamic IGMP multicast group entries for VLAN-interface 100 on the public network.

```
<Sysname> reset igmp group interface vlan-interface 100 all
```

# Clear the dynamic IGMP multicast group entry of the group 225.0.0.1 for VLAN-interface 100 on the public network.

```
<Sysname> reset igmp group interface vlan-interface 100 225.0.0.1
```

Related commands

display igmp group

PIM commands

The term "interface" in this chapter collectively refers to VLAN interfaces and Layer 3 Ethernet interfaces. You can set an Ethernet port as a Layer 3 interface by using the **port link-mode route** command (see *Layer 2—LAN Switching Configuration Guide*).

auto-rp enable (PIM view)

Use **auto-rp enable** to enable Auto-RP listening.

Use **undo auto-rp enable** to disable Auto-RP listening.

Syntax

auto-rp enable

undo auto-rp enable

Default

Auto-RP listening is disabled.

Views

PIM view

Predefined user roles

network-admin

mdc-admin

Usage guidelines

This command is available in Release 2137 and later versions.

Examples

# Enable Auto-RP listening on the public network.

```
<Sysname> system-view
[Sysname] pim
[Sysname-pim] auto-rp enable
```

bsm-fragment enable (PIM view)

Use **bsm-fragment enable** to enable bootstrap message (BSM) semantic fragmentation.

Use **undo bsm-fragment enable** to disable BSM semantic fragmentation.

Syntax

bsm-fragment enable

undo bsm-fragment enable

Default

BSM semantic fragmentation is enabled.

Views

PIM view

Predefined user roles

network-admin

mdc-admin

Usage guidelines

Disable BSM semantic fragmentation if the PIM-SM domain contains a device that does not support this feature.

Examples

# Disable BSM semantic fragmentation on the public network.

```
<Sysname> system-view
[Sysname] pim
[Sysname-pim] undo bsm-fragment enable
```

bsr-policy (PIM view)

Use **bsr-policy** to configure a BSR policy to define the legal BSR address range.

Use **undo bsr-policy** to remove the configuration.

Syntax

bsr-policy *acl-number*

undo bsr-policy

Default

No BSR policy exists, and all bootstrap messages are regarded as legal.

Views

PIM view

Predefined user roles

network-admin

mdc-admin

Parameters

acl-number: Specifies an IPv4 basic ACL by its number in the range of 2000 to 2999.

Usage guidelines

You can use this command to guard against BSR spoofing.

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

- For the rule to take effect, do not specify the **vpn-instance** *vpn-instance* option.
- The **source** *source-address source-wildcard* option specifies a BSR address.
- Among the other optional parameters, only the **fragment** keyword and the **time-range** *time-range-name* option take effect.

Examples

# On the public network, configure a BSR policy so that only the devices on the subnet 10.1.1.0/24 can act as the BSR.

```
<Sysname> system-view
[Sysname] acl number 2000
[Sysname-acl-basic-2000] rule permit source 10.1.1.0 0.0.0.255
[Sysname-acl-basic-2000] quit
[Sysname] pim
[Sysname-pim] bsr-policy 2000
```

Related commands

c-bsr (PIM view)

c-bsr (PIM view)

Use **c-bsr** to configure a candidate-BSR (C-BSR).

Use **undo c-bsr** to remove a C-BSR.

Syntax

c-bsr *ip-address* [**scope** *group-address* { *mask-length* | *mask* }] [**hash-length** *hash-length* | **priority** *priority*] *

undo c-bsr *ip-address* [**scope** *group-address* { *mask-length* | *mask* }]

Default

No C-BSRs exist.

Views

PIM view

Predefined user roles

network-admin

mdc-admin

Parameters

ip-address: Specifies the IP address of a C-BSR.

scope *group-address*: Specifies a multicast group by its IP address in the range of 239.0.0.0 to 239.255.255.255. If you do not specify a multicast group, the C-BSR is used for the global-scoped zone.

mask-length: Specifies an address mask length in the range of 8 to 32.

mask: Specifies an address mask.

hash-length *hash-length*: Specifies a hash mask length in the range of 0 to 32. The default setting is 30.

priority *priority*: Specifies a priority for the C-BSR, in the range of 0 to 255. The default setting is 64. The greater the value, the higher the priority.

Usage guidelines

The IP address of a C-BSR must be the IP address of a local PIM enabled interface on the C-BSR. Otherwise, the configuration does not take effect.

If you execute this command for a zone multiple times, the most recent configuration takes effect.

You can configure the same C-BSR for different zones.

Examples

# Configure the interface with the IP address of 1.1.1.1 as the C-BSR for the global-scoped zone on the public network.

```
<Sysname> system-view
[Sysname] pim
[Sysname-pim] c-bsr 1.1.1.1
```

c-rp (PIM view)

Use **c-rp** to configure a candidate-RP (C-RP).

Use **undo c-rp** to remove the configuration of a C-RP.

Syntax

c-rp *ip-address* [**advertisement-interval** *adv-interval* | **group-policy** *acl-number* | **holdtime** *hold-time* | **priority** *priority*] *

undo c-rp *ip-address*

Default

No C-RPs exist.

Views

PIM view

Predefined user roles

network-admin

mdc-admin

Parameters

ip-address: Specifies the IP address of a C-RP.

advertisement-interval *adv-interval*: Specifies a C-RP-Adv interval in the range of 1 to 65535 seconds. The default value is 60 seconds.

group-policy *acl-number*: Specifies an IPv4 basic ACL number in the range of 2000 to 2999. If you specify an ACL, this command designates the C-RP to only the multicast groups that the ACL permits. The command designates the C-RP to all multicast groups (224.0.0.0/24) when one of the following conditions exists:

- You do not specify an ACL.
- The specified ACL does not exist.
- The specified ACL does not contain any valid rules.

holdtime *hold-time*: Specifies a C-RP lifetime in the range of 1 to 65535 seconds. The default value is 150 seconds.

priority *priority*: Specifies a C-RP priority in the range of 0 to 255. The default setting is 192. A larger value represents a lower priority.

Usage guidelines

The IP address of a C-RP must be the IP address of a local PIM enabled interface on the C-RP. Otherwise, the configuration does not take effect.

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

- For the rule to take effect, do not specify the **vpn-instance** *vpn-instance* option.
- The **source** *source-address source-wildcard* option specifies a multicast group range.
- Among the other optional parameters, only the **fragment** keyword and the **time-range** *time-range-name* option take effect.

To designate a C-RP to multiple multicast group ranges, create multiple rules that specify different multicast group ranges in the ACL.

If you execute this command using the same C-RP IP address multiple times, the most recent configuration takes effect.

Examples

# On the public network, configure the interface with the IP address of 1.1.1.1 as the C-RP for multicast group ranges 225.1.0.0/16 and 226.2.0.0/16, and set its priority to 10.

```
<Sysname> system-view
[Sysname] acl number 2000
[Sysname-acl-basic-2000] rule permit source 225.1.0.0 0.0.255.255
[Sysname-acl-basic-2000] rule permit source 226.2.0.0 0.0.255.255
[Sysname-acl-basic-2000] quit
[Sysname] pim
[Sysname-pim] c-rp 1.1.1.1 group-policy 2000 priority 10
```

crp-policy (PIM view)

Use **crp-policy** to configure a C-RP policy to define the legal C-RP address range and the multicast group range to which the C-RP is designated.

Use **undo crp-policy** to remove the configuration.

Syntax

crp-policy *acl-number*

undo crp-policy

Default

No C-RP policy exists, and all C-RP messages are regarded as legal.

Views

PIM view

Predefined user roles

network-admin

mdc-admin

Parameters

acl-number: Specifies an IPv4 advanced ACL number in the range of 3000 to 3999.

Usage guidelines

You can use this command to guard against C-RP spoofing.

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

- For the rule to take effect, do not specify the **vpn-instance** *vpn-instance* option.
- The **source** *source-address source-wildcard* option specifies an RP address.
- The **destination** *dest-address dest-wildcard* option specifies a multicast group address.
- Among the other optional parameters, only the **fragment** keyword and the **time-range** *time-range-name* option take effect.

The switch uses only the prefixes of the multicast group ranges in advertisement messages to match the destination field in ACL rules. For example, the multicast group range in an advertisement message is 224.1.0.0/16. If the prefix 224.1.0.0 is in the range specified by the destination field of an ACL rule, the specified C-RPs are designated to this multicast group range.

Examples

# On the public network, configure a C-RP policy so that only devices in the address range of 1.1.1.1/24 can be C-RPs for the multicast group range 225.1.1.0/24.

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

```
[Sysname] acl number 3000
[Sysname-acl-adv-3000] rule permit ip source 1.1.1.1 0.0.0.255 destination 225.1.1.0
0.0.0.255
[Sysname-acl-adv-3000] quit
[Sysname] pim
[Sysname-pim] crp-policy 3000
```

Related commands

c-rp (PIM view)

display interface register-tunnel

Use **display interface register-tunnel** to display register-tunnel interface information.

Syntax

display interface [**register-tunnel** [*interface-number*]] [**brief** [**description** | **down**]]

Views

Any view

Predefined user roles

network-admin

network-operator

mdc-admin

mdc-operator

Parameters

register-tunnel: Displays information about the register-tunnel interface. If you do not specify this keyword, the command displays information about all interfaces on the switch.

interface-number: Specifies a register-tunnel interface by its number. The switch has only one register-tunnel interface, and the value for this argument is fixed at 0. The command always displays information about Register-Tunnel 0 when you specify the **register-tunnel** keyword, regardless of whether you specify an interface number.

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

description: Displays the full interface description. If you do not specify this keyword, the command displays only the first 27 characters of the interface description.

down: Displays information about the interfaces in down state and the causes. If you do not specify this keyword, the command displays information about interfaces in all states.

Usage guidelines

The register-tunnel interface is a virtual interface that is automatically created by the system. You cannot configure it or delete it, but you can display the interface information by using this command. The physical state and link state of the register-tunnel interface are always down.

In the initial stage of multicast source registration, the register-tunnel interface is used to establish a channel between the source-side DR and the RP for transmitting multicast register messages. The process of initial source registration is as follows:

1. After receiving the first multicast data from the source, the source-side DR encapsulates the multicast data into a register message. Then, it forwards the message to the RP through the register-tunnel interface.

2. The register message arrives at the register-tunnel interface on the RP. The RP decapsulates the register message and forwards the multicast data to the receiver hosts. At the same time, the RP learns the IP address of the multicast source.
3. The RP sends a join message to the multicast source to build an SPT.
4. After the SPT is built, the multicast data travels to the RP along the SPT rather than through the register-tunnel interface.

Examples

# Display detailed information about Register-Tunnel 0.

```
<Sysname> display interface register-tunnel 0
Register-Tunnel0
Current state: UP
Line protocol state: DOWN
Description: Register-Tunnel0 Interface
Bandwidth: 0kbps
Maximum Transmit Unit: 1536
Internet protocol processing: disabled
Physical: Unknown
Last 300 seconds input rate: 0 bytes/sec, 0 bits/sec, 0 packets/sec
Last 300 seconds output rate: 0 bytes/sec, 0 bits/sec, 0 packets/sec
Input: 0 packets, 0 bytes, 0 drops
Output: 0 packets, 0 bytes, 0 drops
```

# Display brief information about Register-Tunnel 0.

```
<Sysname> display interface register-tunnel 0 brief
Brief information on interface(s) under route mode:
Link: ADM - administratively down; Stby - standby
Protocol: (s) - spoofing
Interface            Link Protocol Main IP         Description
REG0                 UP   --       --
```

Table 22 Command output

Field	Description
Current state	Physical state of the register-tunnel interface. This field always displays **UP**.
Line protocol state	Link state of the register-tunnel interface. This field always displays **DOWN**.
Description	Description of the register-tunnel interface. It is not configurable.
Bandwidth	Expected bandwidth of the register-tunnel interface. It is not configurable.
Maximum Transmit Unit	MTU of the register-tunnel interface. It is not configurable.
Internet protocol processing	IP protocol processing capability. This field always displays **disabled**.
Physical	Physical type of the register-tunnel interface. This field always displays **Unknown**.
Last 300 seconds input rate	Average incoming rate in the last 300 seconds. This field always displays **0**.
Last 300 seconds output rate	Average outgoing rate in the last 300 seconds. This field always displays **0**.
Input	Number of incoming packets, incoming bytes, and discarded packets. This field always displays **0**.

Field	Description
Output	Number of outgoing packets, outgoing bytes, and discarded packets. This field always displays **0**.
Brief information on interface(s) under route mode	Brief information about Layer 3 interfaces.
Link: ADM - administratively down; Stby - standby	Physical link state of the interface: • **UP**—The link is up. • **DOWN**—The link is physically down. • **ADM**—The link has been administratively shut down. To recover its physical state, use the **undo shutdown** command. • **Stby**—The link is a backup link. To display information about the primary interface, use the **display interface-backup** command.
Protocol: (s) - spoofing	If the Protocol field of the interface contains "(s)", it means one of the following conditions: • The data link protocol state of the interface is up, but no link is present on the interface. • The link is not permanent. Instead, it is created on demand. Typically, null interfaces or loopback interfaces have this attribute.
Protocol	Protocol connection state of the interface. This field always displays double hyphens (--).
Main IP	IP address of the interface. This field always displays double hyphens (--).
Cause	Causes why the physical state of the interface is down. This field always displays **Not connected**.

display pim bsr-info

Use **display pim bsr-info** to display BSR information in the PIM-SM domain.

Syntax

display pim [**vpn-instance** *vpn-instance-name*] **bsr-info**

Views

Any view

Predefined user roles

network-admin

network-operator

mdc-admin

mdc-operator

Parameters

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, this command displays BSR information on the public network.

Examples

# Display BSR information in the PIM-SM domain on the public network.

```
<Sysname> display pim bsr-info
 Scope: non-scoped
     State: Accept Preferred
     Bootstrap timer: 00:01:44
     Elected BSR address: 12.12.12.1
       Priority: 64
       Hash mask length: 30
       Uptime: 00:21:56

 Scope: 239.4.0.0/16
     State: Accept Any
     Scope-zone expiry timer: 00:21:12

 Scope: 239.1.0.0/16
     State: Elected
     Bootstrap timer: 00:00:26
     Elected BSR address: 17.1.11.1
       Priority: 64
       Hash mask length: 30
       Uptime: 02:53:37
     Candidate BSR address: 17.1.11.1
       Priority: 64
       Hash mask length: 30

 Scope: 239.2.2.0/24
     State: Candidate
     Bootstrap timer: 00:01:56
     Elected BSR address: 61.2.37.1
       Priority: 64
       Hash mask length: 30
       Uptime: 02:53:32
     Candidate BSR address: 17.1.12.1
       Priority: 64
       Hash mask length: 30

 Scope: 239.3.3.0/24
     State: Pending
     Bootstrap timer: 00:00:07
     Candidate BSR address: 17.1.13.1
       Priority: 64
       Hash mask length: 30
```

Table 23 Command output

Field	Description
Scope-zone expiry timer	Scoped zone aging timer.
Elected BSR address	Address of the elected BSR.
Candidate BSR address	Address of the candidate BSR.
Priority	BSR priority.
Uptime	Length of time the BSR has been up.

display pim claimed-route

Use **display pim claimed-route** to display information about all routes that PIM uses.

Syntax

display pim [**vpn-instance** *vpn-instance-name*] **claimed-route** [*source-address*]

Views

Any view

Predefined user roles

network-admin

network-operator

mdc-admin

mdc-operator

Parameters

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, this command displays information about all routes that PIM uses on the public network.

source-address: Specifies a multicast source by its IP address. If you do not specify a multicast source, this command displays information about all routes that PIM uses.

Examples

# Display information about all routes that PIM uses on the public network.

```
<Sysname> display pim claimed-route
 RPF-route selecting rule: longest-match

 Route/mask: 7.11.0.0/16 (unicast (direct))
     RPF interface: Vlan-interface2, RPF neighbor: 8.0.0.2
     Total number of (S,G) or (*,G) dependent on this route entry: 4
     (7.11.0.10, 225.1.1.1)
     (7.11.0.10, 226.1.1.1)
     (7.11.0.10, 227.1.1.1)
     (*, 228.1.1.1)
 Route/mask: 7.12.0.0/16 (multicast static)
     RPF interface: Vlan-interface2, RPF neighbor: 8.0.0.3,
     Config NextHop: 8.0.0.5
     Total number of (S,G) or (*,G) dependent on this route entry: 2
     (7.12.0.10, 226.1.1.1)
     (7.12.0.10, 225.1.1.1)
```

Table 24 Command output

Field	Description
Route/mask	Route entry. Route types in parentheses include: • **igp**—IGP unicast route. • **egp**—EGP unicast route. • **unicast (direct)**—Direct unicast route. • **unicast**—Other unicast route, such as static unicast route.

Field	Description
	- **multicast static**—Static multicast route.
RPF interface	Name of the RPF interface.
RPF neighbor	IP address of the RPF neighbor.
Config NextHop	Address of the configured next hop. This field is displayed only when the static multicast route is configured with a next hop.
Total number of (S,G) or (*,G) dependent on this route entry	Total number (S, G) or (*, G) entries dependent on the RPF route and their details.

display pim c-rp

Use **display pim c-rp** to display C-RP information in the PIM-SM domain.

Syntax

display pim [**vpn-instance** *vpn-instance-name*] **c-rp** [**local**]

Views

Any view

Predefined user roles

network-admin

network-operator

mdc-admin

mdc-operator

Parameters

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, this command displays information about learned C-RPs on the public network.

local: Specifies local C-RPs. If you do not specify this keyword, the command displays information about all C-RPs.

Usage guidelines

You can view information about learned C-RPs on only the BSR. On other devices, you can view information about the locally configured C-RPs.

Examples

# Display information about learnt C-RPs on the public network.

```
<Sysname> display pim c-rp
 Scope: non-scoped
     Group/MaskLen: 224.0.0.0/4
       C-RP address             Priority  HoldTime  Uptime    Expires
       1.1.1.1 (local)          192       150       03:01:36  00:02:29
       2.2.2.2                  192       150       1d:13h    00:02:02
     Group/MaskLen: 226.1.1.0/24 Expires: 00:00:33
     Group/MaskLen: 225.1.0.0/16
       C-RP Address             Priority  HoldTime  Uptime    Expires
       3.3.3.3                  192       150       12w:5d    00:02:05
```

# Display information about the locally configured C-RPs.

```
<Sysname> display pim c-rp local
 Candidate RP: 12.12.12.9(Loop1)
     Priority: 192
     HoldTime: 150
     Advertisement interval: 60
     Next advertisement scheduled at: 00:00:48
```

Table 25 Command output

Field	Description
Group/MaskLen	Multicast group to which the C-RP is designated.
(local)	Local address. This field is not displayed if the IP address of the C-RP is not a local address.
HoldTime	C-RP lifetime.
Uptime	Length of time the C-RP has been up: • **w**—weeks. • **d**—days. • **h**—hours.
Expires	Remaining lifetime for the C-RP or multicast group.
Candidate RP	IP address of the locally configured C-RP.
Advertisement interval	Interval between two advertisement messages sent by the locally configured C-RP.
Next advertisement scheduled at	Remaining time for the locally configured C-RP to send the next advertisement message.

display pim interface

Use **display pim interface** to display PIM information on an interface.

Syntax

display pim [**vpn-instance** *vpn-instance-name*] **interface** [*interface-type interface-number*] [**verbose**]

Views

Any view

Predefined user roles

network-admin

network-operator

mdc-admin

mdc-operator

Parameters

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, this command displays PIM information on the public network.

interface-type interface-number: Specifies an interface by its type and number. If you do not specify an interface, this command displays PIM information on all interfaces.

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

Examples

# Display brief PIM information on all interfaces on the public network.

```
<Sysname> display pim interface
 Interface          NbrCnt  HelloInt  DR-Pri     DR-Address
 Vlan1              1       30        1          10.1.1.2
 Vlan2              0       30        1          172.168.0.2    (local)
 Vlan3              1       30        1          20.1.1.2
```

Table 26 Command output

Field	Description
NbrCnt	Number of PIM neighbors.
HelloInt	PIM hello interval.
DR-Pri	DR priority.

# Display detailed PIM information on VLAN-interface 1 on the public network.

```
<Sysname> display pim interface vlan-interface 1 verbose
 Interface: Vlan-interface1, 10.1.1.1
     PIM version: 2
     PIM mode: Sparse
     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 override interval (negotiated): 2500 ms
     PIM override interval (configured): 2500 ms
     PIM neighbor tracking (negotiated): disabled
     PIM neighbor tracking (configured): disabled
     PIM generation ID: 0xF5712241
     PIM require generation ID: 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 passive: disabled
     Number of routers on network not using DR priority: 0
     Number of routers on network not using LAN delay: 0
     Number of routers on network not using neighbor tracking: 2
```

Table 27 Command output

Field	Description
PIM mode	PIM mode: dense or sparse.
PIM DR	IP address of the DR.
PIM DR Priority (configured)	Configured DR priority.
PIM neighbor count	Total number of PIM neighbors.
PIM hello interval	Interval for sending hello messages.
PIM LAN delay (negotiated)	Negotiated PIM message propagation delay.
PIM LAN delay (configured)	Configured PIM message propagation delay.
PIM override interval (negotiated)	Negotiated interval for overriding prune messages.
PIM override interval (configured)	Configured interval for overriding prune messages.
PIM neighbor tracking (negotiated)	Negotiated neighbor tracking status: enabled or disabled.
PIM neighbor tracking (configured)	Configured neighbor tracking status: enabled or disabled.
PIM require generation ID	Whether the function of discarding hello messages without Generation_ID is enabled.
PIM hello hold interval	PIM neighbor lifetime.
PIM assert hold interval	Assert holdtime timer.
PIM triggered hello delay	Maximum delay for sending hello messages.
PIM J/P interval	Interval for sending join/prune messages.
PIM J/P hold interval	Joined/pruned state holdtime timer.
PIM BSR domain border	Whether a PIM domain border is configured.
PIM BFD	Whether PIM is enabled to work with BFD.
PIM passive	Whether PIM passive mode is enabled.
Number of routers on network not using DR priority	Number of routers that do not use the DR priority field on the subnet where the interface resides.
Number of routers on network not using LAN delay	Number of routers that do not use the LAN delay field on the subnet where the interface resides.
Number of routers on network not using neighbor tracking	Number of routers that are not enabled with neighbor tracking on the subnet where the interface resides.

display pim neighbor

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

Syntax

display pim [**vpn-instance** *vpn-instance-name*] **neighbor** [*neighbor-address* **| interface** *interface-type interface-number* **| verbose**] *

Views

Any view

Predefined user roles

network-admin

network-operator

mdc-admin

mdc-operator

Parameters

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, this command displays information about all PIM neighbors on the public network.

neighbor-address: Specifies a PIM neighbor by its IP address. If you do not specify a PIM neighbor, this command displays information about all PIM neighbors.

interface *interface-type interface-number*: Specifies an interface by its type and number. If you do not specify an interface, this command displays information about PIM neighbors on all interfaces.

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

Examples

# Display brief information about all PIM neighbors on the public network.

```
<Sysname> display pim neighbor
 Total Number of Neighbors = 2

 Neighbor        Interface           Uptime   Expires  DR-Priority Mode
 10.1.1.2        Vlan1               02:50:49 00:01:31 1
 20.1.1.2        Vlan2               02:49:39 00:01:42 1
```

# Display detailed information about the PIM neighbor with the IP address 11.110.0.20 on the public network.

```
<Sysname> display pim neighbor 11.110.0.20 verbose
 Neighbor: 11.110.0.20
     Interface: Vlan-interface3
     Uptime: 00:00:10
     Expiry time: 00:00:30
     DR Priority: 1
     Generation ID: 0x2ACEFE15
     Holdtime: 105 s
     LAN delay: 500 ms
     Override interval: 2500 ms
     State refresh interval: 60 s
     Neighbor tracking: Disabled
     Bidirectional PIM: Disabled
```

Table 28 Command output

Field	Description
Neighbor	IP address of the PIM neighbor.
Interface	Interface that connects to the PIM neighbor.
Uptime	Length of time the PIM neighbor has been up.
Expires/Expiry time	Remaining lifetime for the PIM neighbor. If the PIM neighbor is always up and reachable, this field displays **never**.
DR-Priority/DR Priority	Priority of the PIM neighbor.
Mode	PIM mode.

Field	Description
Generation ID	Generation ID of the PIM neighbor. (A random value represents a status change of the PIM neighbor.)
Holdtime	Lifetime of the PIM neighbor. If the PIM neighbor is always up and reachable, this field displays **forever**.
LAN delay	Delay for sending prune messages.
Override interval	Interval for overriding prune messages.
State refresh interval	Interval for refreshing state. This field is displayed only when the PIM neighbor operates in PIM-DM mode and the state refresh capability is enabled.
Neighbor tracking	Neighbor tracking status: • **Enabled**. • **Disabled**.
Bidirectional PIM	Whether BIDIR-PIM is enabled.

display pim routing-table

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

Syntax

display pim [**vpn-instance** *vpn-instance-name*] **routing-table** [*group-address* [**mask** { *mask-length* | *mask* }] | *source-address* [**mask** { *mask-length* | *mask* }] | **flags** *flag-value* | **fsm** | **incoming-interface** *interface-type interface-number* | **mode** *mode-type* | **outgoing-interface** { **exclude** | **include** | **match** } *interface-type interface-number*] *

Views

Any view

Predefined user roles

network-admin

network-operator

mdc-admin

mdc-operator

Parameters

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, this command displays PIM routing entries on the public network.

group-address: Specifies a multicast group by its IP address in the range of 224.0.0.0 to 239.255.255.255. If you do not specify a multicast group, this command displays PIM routing entries for all multicast groups.

source-address: Specifies a multicast source by its IP address.

mask-length: Specifies an address mask length in the range of 0 to 32. The default value is 32.

mask: Specifies an address mask. The default value is 255.255.255.255.

flags *flag-value*: Specifies a flag. If you do not specify a flag, this command displays PIM routing entries that contain all flags. The following lists the values of the *flag-value* argument and their meanings:

- **act**: Specifies PIM routing entries that have been used for routing data.

- **del**: Specifies PIM routing entries to be deleted.
- **exprune**: Specifies PIM routing entries containing outgoing interfaces pruned by other multicast routing protocols.
- **ext**: Specifies PIM routing entries containing outgoing interfaces provided by other multicast routing protocols.
- **loc**: Specifies PIM routing entries on the devices that reside on the same subnet as the multicast source.
- **niif**: Specifies PIM routing entries containing unknown incoming interfaces.
- **nonbr**: Specifies PIM routing entries with PIM neighbor lookup failure.
- **rpt**: Specifies PIM routing entries on the RPT branches where (S, G) prunes have been sent to the RP.
- **spt**: Specifies PIM routing entries on the SPT.
- **swt**: Specifies PIM routing entries in the process of RPT-to-SPT switchover.
- **wc**: Specifies PIM routing entries with wildcards.

fsm: Displays detailed information about the finite state machine.

incoming-interface *interface-type interface-number*: Specifies an incoming interface. If you do not specify an incoming interface, this command displays PIM routing entries that contain all incoming interfaces.

mode *mode-type*: Specifies a PIM mode. If you do not specify a PIM mode, this command displays PIM routing entries in all PIM modes. The available PIM modes include:

- **dm**: Specifies PIM-DM.
- **sm**: Specifies PIM-SM.
- **ssm**: Specifies PIM-SSM.

outgoing-interface { **exclude** | **include** | **match** } *interface-type interface-number*: Specifies an outgoing interface. If you do not specify an outgoing interface, this command displays PIM routing entries that contain all outgoing interfaces. Whether the specified outgoing interface is contained in the PIM routing table depends on the following conditions:

- If you specify an excluded interface, this command displays PIM routing entries that do not contain the specified outgoing interface.
- If you specify an included interface, this command displays PIM routing entries that contain the specified outgoing interface.
- If you specify a matching interface, this command displays PIM routing entries that contain only the specified outgoing interface.

Examples

# Display PIM routing entries on the public network.

```
<Sysname> display pim routing-table
 Total 0 (*, G) entry; 1 (S, G) entry

 (172.168.0.12, 227.0.0.1)
     RP: 2.2.2.2
     Protocol: pim-sm, Flag: SPT LOC ACT
     UpTime: 02:54:43
     Upstream interface: Vlan-interface1
         Upstream neighbor: NULL
         RPF prime neighbor: NULL
     Downstream interface(s) information:
     Total number of downstreams: 1
```

```
        1: Vlan-interface2
            Protocol: pim-sm, UpTime: 02:54:43, Expires: 00:02:47
```

Table 29 Command output

Field	Description
Total 0 (*, G) entry; 1 (S, G) entry	Total number of (S, G) entries and (*, G) entries.
(172.168.0.12, 227.0.0.1)	(S, G) entry.
Protocol	PIM mode.
Flag	Flag of the (S, G) entry or (*, G) entry: • **ACT**—The entry has been used for routing data. • **DEL**—The entry will be removed. • **EXPRUNE**—Some outgoing interfaces are pruned by other multicast routing protocols. • **EXT**—The entry contains outgoing interfaces provided by other multicast routing protocols. • **LOC**—The entry is on a router directly connected to the same subnet with the multicast source. • **NIIF**—The entry contains unknown incoming interfaces. • **NONBR**—The entry has a PIM neighbor lookup failure. • **RPT**—The entry is on an RPT branch where (S, G) prunes have been sent to the RP. • **SPT**—The entry is on the SPT. • **SWT**—The entry is in the process of RPT-to-SPT switchover. • **WC**—The entry contains a wildcard.
Uptime	Length of time since the (S, G) entry or (*, G) entry was installed.
Upstream interface	Upstream (incoming) interface of the (S, G) entry or (*, G) entry.
Upstream neighbor	Upstream neighbor of the (S, G) entry or (*, G) entry.
RPF prime neighbor	RPF neighbor of the (S, G) or (*, G) entry: • For a (*, G) entry, if the RPF neighbor is the RP, the field displays **NULL**. • For an (S, G) entry, if the RPF neighbor is a router that directly connects to the multicast source, this field displays **NULL**.
Downstream interface(s) information	Information about the downstream interfaces: • Total number of downstream interfaces. • Names of the downstream interfaces. • Protocol type on the downstream interfaces. • Uptime of the downstream interfaces. • Expiration time of the downstream interfaces.

display pim rp-info

Use **display pim rp-info** to display RP information in the PIM-SM domain.

Syntax

display pim [**vpn-instance** *vpn-instance-name*] **rp-info** [*group-address*]

Views

Any view

Predefined user roles

network-admin

network-operator

mdc-admin

mdc-operator

Parameters

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, this command displays RP information on the public network.

group-address: Specifies a multicast group by its IP address in the range of 224.0.1.0 to 239.255.255.255. If you do not specify a multicast group, this command displays RP information for all multicast groups.

Examples

# Display RP information for the multicast group 224.0.1.1 on the public network.

```
<Sysname> display pim rp-info 224.0.1.1
 BSR RP address is: 2.2.2.2
     Priority: 192
     HoldTime: 150
     Uptime: 03:01:10
     Expires: 00:02:30

 Static RP address is: 3.3.3.5
     Preferred: Yes
     Configured ACL: 2003

 RP mapping for this group is: 3.3.3.5
```

# Display RP information for all multicast groups on the public network.

```
<Sysname> display pim rp-info
 BSR RP information:
   Scope: non-scoped
     Group/MaskLen: 224.0.0.0/4
       RP address               Priority  HoldTime  Uptime    Expires
       1.1.1.1 (local)          192       150       03:01:36  00:02:29
       2.2.2.2                  192       150       1d:13h    00:02:02
     Group/MaskLen: 225.1.0.0/16
       RP address               Priority  HoldTime  Uptime    Expires
       3.3.3.3                  192       150       12w:5d    00:02:05

 Static RP information:
       RP address               ACL   Mode    Preferred
       3.3.3.1                  2000  pim-sm  No
       3.3.3.3                  2002  pim-sm  No
       3.3.3.4                        pim-sm  No
       3.3.3.5                  2002  pim-sm  Yes
```

Table 30 Command output

Field	Description
Group/MaskLen	Multicast group to which the RP is designated.
(local)	Local address. This field is not displayed if the IP address is not a local address.
Priority	Priority of the RP.
HoldTime	RP lifetime.
Uptime	Length of time the RP has been up.
Expires	Remaining lifetime for the RP.
Preferred	Whether the static RP is preferred.
Configured ACL/ACL	ACL defining the multicast groups to which the static RP is designated.
Mode	Static RP service mode: PIM-SM.
RP mapping for this group	IP address of the RP that provides services for the multicast group.

display pim statistics

Use **display pim statistics** to display statistics for PIM packets.

Syntax

display pim statistics

Views

Any view

Predefined user roles

network-admin

network-operator

mdc-admin

mdc-operator

Examples

# Display statistics for PIM packets.

```
<Sysname> display pim statistics
 Received PIM packets: 3295
 Sent PIM packets    : 5975
                Valid       Invalid        Succeeded   Failed
     Hello    : 3128        0              4333        0
     Reg      : 14          0              0           0
     Reg-stop : 0           0              0           0
     JP       : 151         0              561         0
     BSM      : 0           0              1081        0
     Assert   : 0           0              0           0
     Graft    : 0           0              0           0
     Graft-ACK: 0           0              0           0
     C-RP     : 0           0              0           0
     SRM      : 0           0              0           0
     DF       : 0           0              0           0
```

Table 31 Command output

Field	Description
Received PIM packets	Total number of received PIM packets.
Sent PIM packets	Total number of sent PIM packets.
Valid	Number of received valid PIM packets.
Invalid	Number of received invalid PIM packets.
Succeeded	Number of valid PIM packets that were sent successfully.
Failed	Number of valid PIM packets that failed to be sent.
Hello	Hello message statistics.
Reg	Register message statistics.
Reg-stop	Register-stop message statistics.
JP	Join/prune message statistics.
BSM	BSM statistics.
Assert	Assert message statistics.
Graft	Graft message statistics.
Graft-ACK	Graft-ACK message statistics.
C-RP	C-RP message statistics.
SRM	State refresh message statistics.
DF	Designated forwarder message statistics.

hello-option dr-priority (PIM view)

Use **hello-option dr-priority** to set the global DR priority.

Use **undo hello-option dr-priority** to restore the default.

Syntax

hello-option dr-priority *priority*

undo hello-option dr-priority

Default

The global DR priority is 1.

Views

PIM view

Predefined user roles

network-admin

mdc-admin

Parameters

priority: Specifies a DR priority, in the range of 0 to 4294967295. The greater the value, the higher the priority.

Usage guidelines

You can set the DR priority for all interfaces in PIM view or for the current interface in interface view. The configuration made in interface view takes priority over the configuration made in PIM view.

Examples

# Set the global DR priority to 3 on the public network.

```
<Sysname> system-view
[Sysname] pim
[Sysname-pim] hello-option dr-priority 3
```

Related commands

pim hello-option dr-priority

hello-option holdtime (PIM view)

Use **hello-option holdtime** to set the global PIM neighbor lifetime.

Use **undo hello-option holdtime** to restore the default.

Syntax

hello-option holdtime *time*

undo hello-option holdtime

Default

The global PIM neighbor lifetime is 105 seconds.

Views

PIM view

Predefined user roles

network-admin

mdc-admin

Parameters

time: Specifies a PIM neighbor lifetime in the range of 1 to 65535 seconds. If you set the value to 65535 seconds, the PIM neighbors are always reachable.

Usage guidelines

You can set the PIM neighbor lifetime for all interfaces in PIM view or for the current interface in interface view. The configuration made in interface view takes priority over the configuration made in PIM view.

Examples

# Set the global PIM neighbor lifetime to 120 seconds on the public network.

```
<Sysname> system-view
[Sysname] pim
[Sysname-pim] hello-option holdtime 120
```

Related commands

pim hello-option holdtime

hello-option lan-delay (PIM view)

Use **hello-option lan-delay** to set the global PIM message propagation delay.

Use **undo hello-option lan-delay** to restore the default.

Syntax

hello-option lan-delay *delay*

undo hello-option lan-delay

Default

The global PIM message propagation delay is 500 milliseconds.

Views

PIM view

Predefined user roles

network-admin

mdc-admin

Parameters

delay: Specifies the PIM message propagation delay in the range of 1 to 32767 milliseconds.

Usage guidelines

You can set the PIM message propagation delay for all interfaces in PIM view or for the current interface in interface view. The configuration made in interface view takes priority over the configuration made in PIM view.

Examples

# Set the global PIM message propagation delay to 200 milliseconds on the public network.

```
<Sysname> system-view
[Sysname] pim
[Sysname-pim] hello-option lan-delay 200
```

Related commands

- **hello-option override-interval** (PIM view)
- **pim hello-option lan-delay**
- **pim hello-option override-interval**

hello-option neighbor-tracking (PIM view)

Use **hello-option neighbor-tracking** to enable neighbor tracking globally and disable join message suppression globally.

Use **undo hello-option neighbor-tracking** to restore the default.

Syntax

hello-option neighbor-tracking

undo hello-option neighbor-tracking

Default

Neighbor tracking is disabled, and join message suppression is enabled.

Views

PIM view

Predefined user roles

network-admin

mdc-admin

Usage guidelines

You can enable neighbor tracking for all interfaces in PIM view or for the current interface in interface view. The configuration made in interface view takes priority over the configuration made in PIM view.

Examples

# Enable neighbor tracking globally on the public network.

```
<Sysname> system-view
[Sysname] pim
[Sysname-pim] hello-option neighbor-tracking
```

Related commands

pim hello-option neighbor-tracking

hello-option override-interval (PIM view)

Use **hello-option override-interval** to set the global override interval.

Use **undo hello-option override-interval** to restore the default.

Syntax

hello-option override-interval *interval*

undo hello-option override-interval

Default

The global override interval is 2500 milliseconds.

Views

PIM view

Predefined user roles

network-admin

mdc-admin

Parameters

interval: Specifies an override interval in the range of 1 to 65535 milliseconds.

Usage guidelines

You can set the override interval for all interfaces in PIM view or for the current interface in interface view. The configuration made in interface view takes priority over the configuration made in PIM view.

Examples

# Set the global override interval to 2000 milliseconds on the public network.

```
<Sysname> system-view
[Sysname] pim
[Sysname-pim] hello-option override-interval 2000
```

Related commands

- **hello-option lan-delay** (PIM view)
- **pim hello-option lan-delay**
- **pim hello-option override-interval**

holdtime join-prune (PIM view)

Use **holdtime join-prune** to set the global joined/pruned state holdtime timer.

Use **undo holdtime join-prune** to restore the default.

Syntax

holdtime join-prune *time*

undo holdtime join-prune

Default

The global joined/pruned state holdtime timer is 210 seconds.

Views

PIM view

Predefined user roles

network-admin

mdc-admin

Parameters

time: Specifies a joined/pruned state holdtime timer in the range of 1 to 65535 seconds.

Usage guidelines

You can set the joined/pruned state holdtime timer for all interfaces in PIM view or for the current interface in interface view. The configuration made in interface view takes priority over the configuration made in PIM view.

Examples

# Set the global joined/pruned state holdtime timer to 280 seconds on the public network.

```
<Sysname> system-view
[Sysname] pim
[Sysname-pim] holdtime join-prune 280
```

Related commands

pim holdtime join-prune

jp-pkt-size (PIM view)

Use **jp-pkt-size** to set the maximum size of each join/prune message.

Use **undo jp-pkt-size** to restore the default.

Syntax

jp-pkt-size *size*

undo jp-pkt-size

Default

The maximum size of a join/prune message is 8100 bytes.

Views

PIM view

Predefined user roles

network-admin

mdc-admin

Parameters

size: Specifies the maximum size of each join/prune message, in the range of 100 to 8100 bytes.

Examples

# Set the maximum size of each join/prune message to 1500 bytes on the public network.

```
<Sysname> system-view
[Sysname] pim
[Sysname-pim] jp-pkt-size 1500
```

pim

Use **pim** to enter PIM view.

Use **undo pim** to remove all configurations in PIM view.

Syntax

pim [**vpn-instance** *vpn-instance-name*]

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

Views

System view

Predefined user roles

network-admin

mdc-admin

Parameters

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, you enter public network PIM view.

Examples

# Enable IP multicast routing on the public network and enter public network PIM view.

```
<Sysname> system-view
[Sysname] multicast routing
[Sysname-mrib] quit
[Sysname] pim
[Sysname-pim]
```

# Enable IP multicast routing in VPN instance **mvpn** and enter PIM view of VPN instance **mvpn**.

```
<Sysname> system-view
[Sysname] multicast routing vpn-instance mvpn
[Sysname-mrib-mvpn] quit
[Sysname] pim vpn-instance mvpn
[Sysname-pim-mvpn]
```

Related commands

multicast routing-enable

pim bfd enable

Use **pim bfd enable** to enable BFD for PIM.

Use **undo pim bfd enable** to disable BFD for PIM.

Syntax

pim bfd enable

undo pim bfd enable

Default

BFD is disabled for PIM.

Views

Interface view

Predefined user roles

network-admin

mdc-admin

Usage guidelines

This command takes effect only when PIM-DM or PIM-SM is enabled on the interface.

Examples

# On the public network, enable IP multicast routing, enable PIM-DM on VLAN-interface 100, and enable BFD for PIM on the interface.

```
<Sysname> system-view
[Sysname] multicast routing
[Sysname-mrib] quit
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] pim dm
[Sysname-Vlan-interface100] pim bfd enable
```

Related commands

- **pim dm**
- **pim sm**

pim bsr-boundary

Use **pim bsr-boundary** to configure a PIM-SM domain border, namely, a bootstrap message boundary.

Use **undo pim bsr-boundary** to remove the configured PIM domain border.

Syntax

pim bsr-boundary

undo pim bsr-boundary

Default

PIM domain borders are not configured.

Views

Interface view

Predefined user roles

network-admin

mdc-admin

Examples

# Configure VLAN-interface 100 as a PIM-SM domain border.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] pim bsr-boundary
```

Related commands

- **c-bsr** (PIM view)
- **multicast boundary**

pim dm

Use **pim dm** to enable PIM-DM.

Use **undo pim dm** to disable PIM-DM.

Syntax

pim dm

undo pim dm

Default

PIM-DM is disabled.

Views

Interface view

Predefined user roles

network-admin

mdc-admin

Usage guidelines

This command takes effect only when IP multicast routing is enabled on the public network or for the VPN instance to which the interface belongs.

Examples

# On the public network, enable IP multicast routing, and enable PIM-DM on VLAN-interface 100.

```
<Sysname> system-view
[Sysname] multicast routing
[Sysname-mrib] quit
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] pim dm
```

Related commands

multicast routing

pim hello-option dr-priority

Use **pim hello-option dr-priority** to set the DR priority on an interface.

Use **undo pim hello-option dr-priority** to restore the default.

Syntax

pim hello-option dr-priority *priority*

undo pim hello-option dr-priority

Default

The DR priority on an interface is 1.

Views

Interface view

Predefined user roles

network-admin

mdc-admin

Parameters

priority: Specifies a DR priority in the range of 0 to 4294967295. The greater the value, the higher the priority.

Usage guidelines

You can set the DR priority for all interfaces in PIM view or for the current interface in interface view. The configuration made in interface view takes priority over the configuration made in PIM view.

Examples

# Set the DR priority to 3 on VLAN-interface 100.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] pim hello-option dr-priority 3
```

Related commands

hello-option dr-priority (PIM view)

pim hello-option holdtime

Use **pim hello-option holdtime** to set the PIM neighbor lifetime on an interface.

Use **undo pim hello-option holdtime** to restore the default.

Syntax

pim hello-option holdtime *time*

undo pim hello-option holdtime

Default

The PIM neighbor lifetime on an interface is 105 seconds.

Views

Interface view

Predefined user roles

network-admin

mdc-admin

Parameters

time: Specifies the PIM neighbor lifetime in the range of 1 to 65535 seconds. If you set the value to 65535 seconds, the PIM neighbor is always reachable.

Usage guidelines

You can set the PIM neighbor lifetime for all interfaces in PIM view or for the current interface in interface view. The configuration made in interface view takes priority over the configuration made in PIM view.

Examples

# Set the PIM neighbor lifetime to 120 seconds on VLAN-interface 100.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] pim hello-option holdtime 120
```

Related commands

hello-option holdtime (PIM view)

pim hello-option lan-delay

Use **pim hello-option lan-delay** to set the PIM message propagation delay on an interface.

Use **undo pim hello-option lan-delay** to restore the default.

Syntax

pim hello-option lan-delay *delay*

undo pim hello-option lan-delay

Default

The PIM message propagation delay on an interface is 500 milliseconds.

Views

Interface view

Predefined user roles

network-admin

mdc-admin

Parameters

delay: Specifies the PIM message propagation delay in the range of 1 to 32767 milliseconds.

Usage guidelines

You can set the PIM message propagation delay for all interfaces in PIM view or for the current interface in interface view. The configuration made in interface view takes priority over the configuration made in PIM view.

Examples

# Set the PIM message propagation delay to 200 milliseconds on VLAN-interface 100.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] pim hello-option lan-delay 200
```

Related commands

- **hello-option lan-delay** (PIM view)
- **hello-option override-interval** (PIM view)
- **pim hello-option override-interval**

pim hello-option neighbor-tracking

Use **pim hello-option neighbor-tracking** to enable neighbor tracking and disable join message suppression on an interface.

Use **pim hello-option neighbor-tracking disable** to disable neighbor tracking on an interface when neighbor tracking is enabled globally.

Use **undo pim hello-option neighbor-tracking** to restore neighbor tracking on an interface to be consistent with the global setting.

Syntax

pim hello-option neighbor-tracking

pim hello-option neighbor-tracking disable

undo pim hello-option neighbor-tracking

Default

Neighbor tracking is disabled and join message suppression is enabled.

Views

Interface view

Predefined user roles

network-admin

mdc-admin

Usage guidelines

You can enable neighbor tracking for all interfaces in PIM view or for the current interface in interface view. The configuration made in interface view takes priority over the configuration made in PIM view.

Examples

# Enable neighbor tracking on VLAN-interface 100.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] pim hello-option neighbor-tracking
```

# On the public network, disable neighbor tracking on VLAN-interface 100 when neighbor tracking is enabled globally.

```
<Sysname> system-view
[Sysname] pim
[Sysname-pim] hello-option neighbor-tracking
[Sysname-pim] quit
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] pim hello-option neighbor-tracking disable
```

Related commands

hello-option neighbor-tracking (PIM view)

pim hello-option override-interval

Use **pim hello-option override-interval** to set the override interval on an interface.

Use **undo pim hello-option override-interval** to restore the default.

Syntax

pim hello-option override-interval *interval*

undo pim hello-option override-interval

Default

The override interval on an interface is 2500 milliseconds.

Views

Interface view

Predefined user roles

network-admin

mdc-admin

Parameters

interval: Specifies the override interval in the range of 1 to 65535 milliseconds.

Usage guidelines

You can set the override interval for all interfaces in PIM view or for the current interface in interface view. The configuration made in interface view takes priority over the configuration made in PIM view.

Examples

# Set the override interval to 2000 milliseconds on VLAN-interface 100.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] pim hello-option override-interval 2000
```

Related commands

- **hello-option lan-delay** (PIM view)
- **hello-option override-interval** (PIM view)
- **pim hello-option lan-delay**

pim holdtime join-prune

Use **pim holdtime join-prune** to set the joined/pruned state holdtime timer on an interface.

Use **undo pim holdtime join-prune** to restore the default.

Syntax

pim holdtime join-prune *time*

undo pim holdtime join-prune

Default

The joined/pruned state holdtime timer is 210 seconds.

Views

Interface view

Predefined user roles

network-admin

mdc-admin

Parameters

time: Specifies the joined/pruned state holdtime timer in the range of 1 to 65535 seconds.

Usage guidelines

You can set the joined/pruned state holdtime timer for all interfaces in PIM view or for the current interface in interface view. The configuration made in interface view takes priority over the configuration made in PIM view.

Examples

# Set the joined/pruned state holdtime timer to 280 seconds on VLAN-interface 100.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] pim holdtime join-prune 280
```

Related commands

holdtime join-prune (PIM view)

pim neighbor-policy

Use **pim neighbor-policy** to configure a PIM hello policy to define the legal source address range for hello messages.

Use **undo pim neighbor-policy** to restore the default.

Syntax

pim neighbor-policy *acl-number*

undo pim neighbor-policy

Default

No PIM hello policy exists on an interface, and all PIM hello messages are regarded as legal.

Views

Interface view

Predefined user roles

network-admin

mdc-admin

Parameters

acl-number: Specifies an IPv4 basic ACL number in the range of 2000 to 2999.

Usage guidelines

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

- For the rule to take effect, do not specify the **vpn-instance** *vpn-instance* option.
- The **source** *source-address source-wildcard* option specifies a source IP address.
- Among the other optional parameters, only the **fragment** keyword and the **time-range** *time-range-name* option take effect.

Examples

# Configure a PIM hello policy on VLAN-interface 100 so that only the devices on the 10.1.1.0/24 subnet can become PIM neighbors of this switch.

```
<Sysname> system-view
[Sysname] acl number 2000
[Sysname-acl-basic-2000] rule permit source 10.1.1.0 0.0.0.255
```

```
[Sysname-acl-basic-2000] quit
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] pim neighbor-policy 2000
```

pim passive

Use **pim passive** to enable PIM passive mode on an interface.

Use **undo pim passive** to restore the default.

Syntax

pim passive

undo pim passive

Default

The PIM passive mode is disabled on an interface.

Views

Interface view

Predefined user roles

network-admin

mdc-admin

Usage guidelines

This command takes effect only when PIM-DM or PIM-SM is enabled on the interface.

Examples

# On the public network, enable IP multicast routing. Then, enable PIM-DM and PIM passive mode on VLAN-interface 100.

```
<Sysname> system-view
[Sysname] multicast routing
[Sysname-mrib] quit
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] pim dm
[Sysname-Vlan-interface100] pim passive
```

pim require-genid

Use **pim require-genid** to enable dropping hello messages without the generation ID options.

Use **undo pim require-genid** to restore the default.

Syntax

pim require-genid

undo pim require-genid

Default

Hello messages without the generation ID options are accepted.

Views

Interface view

Predefined user roles

network-admin

mdc-admin

Examples

# Enable VLAN-interface 100 to drop hello messages without the generation ID options.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] pim require-genid
```

pim sm

Use **pim sm** to enable PIM-SM.

Use **undo pim sm** to disable PIM-SM.

Syntax

pim sm

undo pim sm

Default

PIM-SM is disabled.

Views

Interface view

Predefined user roles

network-admin

mdc-admin

Usage guidelines

This command takes effect only when IP multicast routing is enabled on the public network or for the VPN instance to which the interface belongs.

Examples

# On the public network, enable IP multicast routing, and enable PIM-SM on VLAN-interface 100.

```
<Sysname> system-view
[Sysname] multicast routing
[Sysname-mrib] quit
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] pim sm
```

Related commands

multicast routing

pim state-refresh-capable

Use **pim state-refresh-capable** to enable the state refresh feature on the interface.

Use **undo pim state-refresh-capable** to disable the state refresh feature.

Syntax

pim state-refresh-capable

undo pim state-refresh-capable

Default

The state refresh feature is enabled on an interface.

Views

Interface view

Predefined user roles

network-admin

mdc-admin

Examples

# Disable state refresh on VLAN-interface 100.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] undo pim state-refresh-capable
```

Related commands

- **state-refresh-interval** (PIM view)
- **state-refresh-rate-limit** (PIM view)
- **state-refresh-ttl** (PIM view)

pim timer graft-retry

Use **pim timer graft-retry** to set the graft retry timer on an interface.

Use **undo pim timer graft-retry** to restore the default.

Syntax

pim timer graft-retry *interval*

undo pim timer graft-retry

Default

The graft retry timer on an interface is 3 seconds.

Views

Interface view

Predefined user roles

network-admin

mdc-admin

Parameters

interval: Specifies a graft retry timer in the range of 1 to 65535 seconds.

Examples

# Set the graft retry timer to 80 seconds on VLAN-interface 100.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] pim timer graft-retry 80
```

pim timer hello

Use **pim timer hello** to set the hello interval on an interface.

Use **undo pim timer hello** to restore the default.

Syntax

pim timer hello *interval*

undo pim timer hello

Default

The hello interval on an interface is 30 seconds.

Views

Interface view

Predefined user roles

network-admin

mdc-admin

Parameters

interval: Specifies a hello interval in the range of 0 to 18000 seconds. If you set the value to 0 seconds, the interface does not send hello messages.

Usage guidelines

You can set the hello interval for all interfaces in PIM view or for the current interface in interface view. The configuration made in interface view takes priority over the configuration made in PIM view.

Examples

# Set the hello interval to 40 seconds on VLAN-interface 100.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] pim timer hello 40
```

Related commands

timer hello (PIM view)

pim timer join-prune

Use **pim timer join-prune** to set the join/prune interval on an interface.

Use **undo pim timer join-prune** to restore the default.

Syntax

pim timer join-prune *interval*

undo pim timer join-prune

Default

The join/prune interval on an interface is 60 seconds.

Views

Interface view

Predefined user roles

network-admin

mdc-admin

Parameters

interval: Specifies an join/prune interval in the range of 0 to 18000 seconds. If you set the value to 0 seconds, the interface does not send join or prune messages.

Usage guidelines

You can set the join/prune interval for all interfaces in PIM view or for the current interface in interface view. The configuration made in interface view takes priority over the configuration made in PIM view.

Examples

# Set the join/prune interval to 80 seconds on VLAN-interface 100.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] pim timer join-prune 80
```

Related commands

timer join-prune (PIM view)

pim triggered-hello-delay

Use **pim triggered-hello-delay** to set the triggered hello delay (maximum delay for sending a hello message) on an interface.

Use **undo pim triggered-hello-delay** to restore the default.

Syntax

pim triggered-hello-delay *delay*

undo pim triggered-hello-delay

Default

The triggered hello delay on an interface is 5 seconds.

Views

Interface view

Predefined user roles

network-admin

mdc-admin

Parameters

delay: Specifies a triggered hello delay in the range of 1 to 60 seconds.

Examples

# Set the triggered hello delay to 3 seconds on VLAN-interface 100.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] pim triggered-hello-delay 3
```

register-policy (PIM view)

Use **register-policy** to configure a PIM register policy.

Use **undo register-policy** to remove the configured PIM register policy.

Syntax

register-policy *acl-number*

undo register-policy

Default

No PIM register policy exists, and all PIM register messages are regarded as legal.

Views

PIM view

Predefined user roles

network-admin

mdc-admin

Parameters

acl-number: Specifies an IPv4 advanced ACL number in the range of 3000 to 3999.

Usage guidelines

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

- For the rule to take effect, do not specify the **vpn-instance** *vpn-instance* option.
- The **source** *source-address source-wildcard* option specifies a multicast source address.
- The **destination** *dest-address dest-wildcard* option specifies a multicast group range.
- Among the other optional parameters, only the **fragment** keyword and the **time-range** *time-range-name* option take effect.

Examples

# On the public network, configure a PIM register policy to accept register messages from multicast sources on the subnet of 10.10.0.0/16 for multicast groups on the subnet of 225.1.0.0/16.

```
<Sysname> system-view
[Sysname] acl number 3000
[Sysname-acl-adv-3000] rule permit ip source 10.10.0.0 0.0.255.255 destination 225.1.0.0
0.0.255.255
[Sysname-acl-adv-3000] quit
[Sysname] pim
[Sysname-pim] register-policy 3000
```

register-whole-checksum (PIM view)

Use **register-whole-checksum** to configure the switch to calculate the checksum based on an entire register message.

Use **undo register-whole-checksum** to restore the default.

Syntax

register-whole-checksum

undo register-whole-checksum

Default

The switch calculates the checksum based on the register message header.

Views

PIM view

Predefined user roles

network-admin

mdc-admin

Examples

# Configure the switch to calculate the checksum based on an entire register message on the public network.

```
<Sysname> system-view
[Sysname] pim
[Sysname-pim] register-whole-checksum
```

source-lifetime (PIM view)

Use **source-lifetime** to set the multicast source lifetime.

Use **undo source-lifetime** to restore the default.

Syntax

source-lifetime *time*

undo source-lifetime

Default

The lifetime of a multicast source is 210 seconds.

Views

PIM view

Predefined user roles

network-admin

mdc-admin

Parameters

time: Specifies a multicast source lifetime in the range of 0 to 31536000. If you set the value to 0 seconds, multicast sources are never aged out.

Examples

# Set the multicast source lifetime to 200 seconds on the public network.

```
<Sysname> system-view
[Sysname] pim
[Sysname-pim] source-lifetime 200
```

source-policy (PIM view)

Use **source-policy** to configure a multicast source policy.

Use **undo source-policy** to remove the configured multicast source policy.

Syntax

source-policy *acl-number*

undo source-policy

Default

No multicast source policy exists. The device does not filter multicast data packets.

Views

PIM view

Predefined user roles

network-admin

mdc-admin

Parameters

acl-number: Specifies an IPv4 basic or advanced ACL number in the range of 2000 to 3999.

Usage guidelines

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

- For the rule to take effect, do not specify the **vpn-instance** *vpn-instance* option.
- In a basic ACL, the **source** *source-address source-wildcard* option specifies a source IP address.
- In an advanced ACL, the **source** *source-address source-wildcard* option specifies a source IP address. The **destination** *dest-address dest-wildcard* option specifies a multicast group address.
- Among the other optional parameters, only the **fragment** keyword and the **time-range** *time-range-name* option take effect.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

# On the public network, configure a multicast source policy to accept the multicast packets from the multicast source 10.10.1.2 and to discard the multicast packets from the multicast source 10.10.1.1.

```
<Sysname> system-view
[Sysname] acl number 2000
[Sysname-acl-basic-2000] rule permit source 10.10.1.2 0
[Sysname-acl-basic-2000] rule deny source 10.10.1.1 0
[Sysname-acl-basic-2000] quit
[Sysname] pim
[Sysname-pim] source-policy 2000
```

spt-switch-threshold (PIM view)

Use **spt-switch-threshold** to configure the switchover to SPT.

Use **undo spt-switch-threshold** to restore the default.

Syntax

spt-switch-threshold { **immediacy** | **infinity** } [**group-policy** *acl-number*]

undo spt-switch-threshold [**immediacy** | **infinity**] [**group-policy** *acl-number*]

Default

The switch immediately triggers the switchover to SPT after receiving the first multicast packet.

Views

PIM view

Predefined user roles

network-admin

mdc-admin

Parameters

immediacy: Triggers the switchover to SPT immediately.

infinity: Disables the switchover to SPT.

group-policy *acl-number*: Specifies an IPv4 basic ACL number in the range of 2000 to 2999. If you specify an ACL, this command takes effect on only the multicast groups that the ACL permits. The command takes effect on all multicast groups when one of the following conditions exists:

- You do not specify an ACL.
- The specified ACL does not exist.
- The specified ACL does not contain any valid rules.

Usage guidelines

△ **CAUTION:**

If the switch is an RP, disabling the switchover to SPT might cause multicast traffic forwarding failures on the source-side DR. When disabling the switchover to SPT, be sure you fully understand its impact on your network.

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

- For the rule to take effect, do not specify the **vpn-instance** *vpn-instance* option.
- The **source** *source-address source-wildcard* option specifies a multicast group address.
- Among the other optional parameters, only the **fragment** keyword and the **time-range** *time-range-name* option take effect.

Examples

# Disable the switchover to SPT on a receiver-side DR on the public network.

```
<Sysname> system-view
[Sysname] pim
[Sysname-pim] spt-switch-threshold infinity
```

ssm-policy (PIM view)

Use **ssm-policy** to configure the SSM group range.

Use **undo ssm-policy** to restore the default.

Syntax

ssm-policy *acl-number*

undo ssm-policy

Default

The SSM group range is 232.0.0.0/8.

Views

PIM view

Predefined user roles

network-admin

mdc-admin

Parameters

acl-number: Specifies a basic ACL number in the range of 2000 to 2999.

Usage guidelines

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

- For the rule to take effect, do not specify the **vpn-instance** *vpn-instance* option.
- The **source** *source-address source-wildcard* option specifies a multicast group range.
- Among the other optional parameters, only the **fragment** keyword and the **time-range** *time-range-name* option take effect.

You can use this command to define a multicast group address range. If a packet to a multicast group is permitted by the used ACL, the multicast mode for the packet is PIM-SSM. Otherwise, the multicast mode is PIM-SM.

Examples

# Configure the SSM group range to be 232.1.0.0/16.

```
<Sysname> system-view
[Sysname] acl number 2000
[Sysname-acl-basic-2000] rule permit source 232.1.0.0 0.0.255.255
[Sysname-acl-basic-2000] quit
[Sysname] pim
[Sysname-pim] ssm-policy 2000
```

state-refresh-interval (PIM view)

Use **state-refresh-interval** to set the state refresh interval.

Use **undo state-refresh-interval** to restore the default.

Syntax

state-refresh-interval *interval*

undo state-refresh-interval

Default

The state refresh interval is 60 seconds.

Views

PIM view

Predefined user roles

network-admin

mdc-admin

Parameters

interval: Specifies a state refresh interval in the range of 1 to 255 seconds.

Examples

# Set the state refresh interval to 70 seconds on the public network.

```
<Sysname> system-view
[Sysname] pim
[Sysname-pim] state-refresh-interval 70
```

Related commands

- **pim state-refresh-capable**
- **state-refresh-rate-limit** (PIM view)
- **state-refresh-ttl** (PIM view)

state-refresh-rate-limit (PIM view)

Use **state-refresh-rate-limit** to configure the amount of time that the switch waits before accepting a new state refresh message.

Use **undo state-refresh-rate-limit** to restore the default.

Syntax

state-refresh-rate-limit *time*

undo state-refresh-rate-limit

Default

The switch waits 30 seconds before it accepts a new state refresh message.

Views

PIM view

Predefined user roles

network-admin

mdc-admin

Parameters

time: Specifies the amount of time that the switch waits before accepting a new refresh message, in the range of 1 to 65535 seconds.

Examples

# Configure the switch to wait 45 seconds before it accepts a new state refresh message on the public network.

```
<Sysname> system-view
[Sysname] pim
[Sysname-pim] state-refresh-rate-limit 45
```

Related commands

- **pim state-refresh-capable**
- **state-refresh-interval** (PIM view)
- **state-refresh-ttl** (PIM view)

state-refresh-ttl (PIM view)

Use **state-refresh-ttl** to set the TTL value for state refresh messages.

Use **undo state-refresh-ttl** to restore the default.

Syntax

state-refresh-ttl *ttl-value*

undo state-refresh-ttl

Default

The TTL value of state refresh messages is 255.

Views

PIM view

Predefined user roles

network-admin

mdc-admin

Parameters

ttl-value: Specifies a TTL value for state refresh messages, in the range of 1 to 255.

Examples

# Set the TTL value for state refresh messages to be 45 on the public network.

```
<Sysname> system-view
[Sysname] pim
[Sysname-pim] state-refresh-ttl 45
```

Related commands

- **pim state-refresh-capable** (PIM view)
- **state-refresh-interval** (PIM view)
- **state-refresh-rate-limit** (PIM view)

static-rp (PIM view)

Use **static-rp** to configure a static RP.

Use **undo static-rp** to remove a static RP.

Syntax

static-rp *rp-address* [*acl-number* **| preferred**] *

undo static-rp *rp-address*

Default

Static RPs do not exist.

Views

PIM view

Predefined user roles

network-admin

mdc-admin

Parameters

rp-address: Specifies the IP address of the static RP. This address must be a real, valid unicast IP address, rather than an address on the 127.0.0.0/8 subnet.

acl-number: Specifies an IPv4 basic ACL number in the range of 2000 to 2999. If you specify an ACL, this command designates the static RP to only multicast groups that the ACL permits. The command designates the static RP to all multicast groups 224.0.0.0/4 when one of the following conditions exists:

- You do not specify an ACL.
- The specified ACL does not exist.
- The specified ACL does not contain any valid rules.

preferred: Gives priority to the static RP if the static RP and the dynamic RP exist at the same time in the network. The dynamic RP takes effect only if no static RP exists in the network. If you do not specify this keyword, the dynamic RP has priority. The static RP takes effect only if no dynamic RP exists in the network or when the dynamic RP fails.

Usage guidelines

You do not need to enable PIM on an interface that acts as a static RP.

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

- For the rule to take effect, do not specify the **vpn-instance** *vpn-instance* option.
- The **source** *source-address source-wildcard* option specifies a multicast group address.
- Among the other optional parameters, only the **fragment** keyword and the **time-range** *time-range-name* option take effect.

When the ACL rules used by a static RP change, new RPs must be elected for all multicast groups.

You can configure multiple static RPs by using this command multiple times. However, if you specify the same static RP address or reference the same ACL in this command, the most recent configuration takes effect. If you configure multiple static RPs for the same multicast group, the static RP with the highest IP address is used.

Examples

# On the public network, configure the interface with the IP address of 11.110.0.6 as a static RP for multicast groups 225.1.1.0/24, and give priority to this static RP.

```
<Sysname> system-view
[Sysname] acl number 2001
[Sysname-acl-basic-2001] rule permit source 225.1.1.0 0.0.0.255
[Sysname-acl-basic-2001] quit
[Sysname] pim
[Sysname-pim] static-rp 11.110.0.6 2001 preferred
```

Related commands

display pim rp-info

timer hello (PIM view)

Use **timer hello** to set the global hello interval.

Use **undo timer hello** to restore the default.

Syntax

timer hello *interval*

undo timer hello

Default

The global hello interval is 30 seconds.

Views

PIM view

Predefined user roles

network-admin

mdc-admin

Parameters

interval: Specifies a hello interval in the range of 0 to 18000 seconds. If you set the value to 0 seconds, the switch does not send hello messages.

Usage guidelines

You can set the hello interval for all interfaces in PIM view or for the current interface in interface view. The configuration made in interface view takes priority over the configuration made in PIM view.

Examples

# Set the global hello interval to 40 seconds on the public network.

```
<Sysname> system-view
[Sysname] pim
[Sysname-pim] timer hello 40
```

Related commands

pim timer hello

timer join-prune (PIM view)

Use **timer join-prune** to set the global join/prune interval.

Use **undo timer join-prune** to restore the default.

Syntax

timer join-prune *interval*

undo timer join-prune

Default

The global join/prune interval is 60 seconds.

Views

PIM view

Predefined user roles

network-admin

mdc-admin

Parameters

interval: Specifies a join/prune interval in the range of 0 to 18000 seconds. If you set the value to 0 seconds, the switch does not send join or prune messages.

Usage guidelines

You can set the join/prune interval for all interfaces in PIM view or for the current interface in interface view. The configuration made in interface view takes priority over the configuration made in PIM view.

Examples

# Set the global join/prune interval to 80 seconds on the public network.

```
<Sysname> system-view
[Sysname] pim
[Sysname-pim] timer join-prune 80
```

Related commands

pim timer join-prune

MSDP commands

cache-sa-enable

Use **cache-sa-enable** to enable the SA message cache mechanism to cache the (S, G) entries contained in SA messages.

Use **undo cache-sa-enable** to disable the SA message cache mechanism.

Syntax

cache-sa-enable

undo cache-sa-enable

Default

The SA message cache mechanism is enabled. The device caches the (S, G) entries contained in received SA messages.

Views

MSDP view

Predefined user roles

network-admin

mdc-admin

Examples

# Enable the SA message cache mechanism on the public network, so that the device caches the (S, G) entries contained in the received SA messages.

```
<Sysname> system-view
[Sysname] msdp
[Sysname-msdp] cache-sa-enable
```

Related commands

- **display msdp sa-cache**
- **display msdp sa-count**

display msdp brief

Use **display msdp brief** to display brief information about MSDP peers.

Syntax

display msdp [**vpn-instance** *vpn-instance-name*] **brief** [**state** { **connect** | **disabled** | **established** | **listen** | **shutdown** }]

Views

Any view

Predefined user roles

network-admin

network-operator

mdc-admin

mdc-operator

Parameters

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, this command displays brief information about MSDP peers on the public network.

state: Specifies a state. If you do not specify this keyword, the command displays brief information about MSDP peers in all states.

connect: Specifies the connecting state.

disabled: Specifies the connection failure state.

established: Specifies the session state.

listen: Specifies the listening state.

shutdown: Specifies the shutdown state.

Examples

# Display brief information about MSDP peers in all states on the public network.

```
<Sysname> display msdp brief
Configured   Established  Listen       Connect      Shutdown     Disabled
1            1            0            0            0            0

Peer address    State       Up/Down time    AS         SA count   Reset count
20.20.20.20     Established 00:00:13        100        0          0
```

Table 32 Command output

Field	Description
Configured	Number of MSDP peers that have been configured.
Established	Number of MSDP peers in established state.
Listen	Number of MSDP peers in listening state.
Connect	Number of MSDP peers in connecting state.
Shutdown	Number of MSDP peers in shutdown state.
Disabled	Number of MSDP peers in disabled state.
Peer address	MSDP peer address.
State	MSDP peer status: • **Established**—A session has been established and the MSDP peer is in session. • **Listen**—A session has been established and the local device acts as the server in listening state. • **Connect**—A session is not established and the local device acts as a client in connecting state. • **Shutdown**—The session has been torn down. • **Down**—The connection failed.
Up/Down time	Length of time since the MSDP peering connection was established or torn down.
AS	Number of the AS where the MSDP peer is located. If the system could not obtain the AS number, this field displays a question mark (?).
SA count	Number of (S, G) entries.
Reset count	MSDP peering connection reset times.

display msdp peer-status

Use **display msdp peer-status** to display detailed status of MSDP peers.

Syntax

display msdp [**vpn-instance** *vpn-instance-name*] **peer-status** [*peer-address*]

Views

Any view

Predefined user roles

network-admin

network-operator

mdc-admin

mdc-operator

Parameters

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, this command displays detailed status of the MSDP peers on the public network.

peer-address: Specifies an MSDP peer by its address. If you do not specify an MSDP peer, this command displays the detailed status of all MSDP peers.

Examples

# Display the detailed status of the MSDP peer 20.20.20.20 on the public network.

```
<Sysname> display msdp peer-status 20.20.20.20
MSDP peer 20.20.20.20; AS 100
 Description:
 Information about connection status:
   State: Disabled
   Up/down time: 14:41:08
   Resets: 0
   Connection interface: LoopBack0 (20.20.20.30)
   Received/sent messages: 867/867
   Discarded input messages: 0
   Discarded output messages: 0
   Elapsed time since last connection or counters clear: 14:42:40
   Mesh group peer joined: momo
   Last disconnect reason: Hold timer expired with truncated message
   Truncated packet: 5 bytes in buffer, type: 1, length: 20, without packet time: 75s
 Information about (Source, Group)-based SA filtering policy:
   Import policy: None
   Export policy: None
 Information about SA-Requests:
   Policy to accept SA-Requests: 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: 4294967295
 Input queue size: 0, Output queue size: 0
 Counters for MSDP messages:
```

```
RPF check failure: 0
Incoming/outgoing SA: 0/0
Incoming/outgoing SA-Request: 0/0
Incoming/outgoing SA-Response: 0/0
Incoming/outgoing Keepalive: 867/867
Incoming/outgoing Notification: 0/0
Incoming/outgoing Traceroutes in progress: 0/0
Incoming/outgoing Traceroute reply: 0/0
Incoming/outgoing Unknown: 0/0
Incoming/outgoing data packet: 0/0
```

Table 33 Command output

Field	Description
MSDP peer	MSDP peer address.
AS	Number of the AS where the MSDP peer is located. If the system could not obtain the AS number, this field displays a question mark (?).
State	MSDP peer status: • **Established**—A session has been established and the MSDP peer is in session. • **Listen**—A session has been established and the local device acts as the server in listening state. • **Connect**—A session is not established and the local device acts as a client in connecting state. • **Shutdown**—The session has been torn down. • **Disabled**—The connection failed.
Up/Down time	Length of time since the MSDP peering connection was established or torn down.
Resets	MSDP peering connection reset times.
Connection interface	Interface and IP address used for setting up a TCP connection with the remote MSDP peer.
Received/sent messages	Number of SA messages sent and received through this connection.
Discarded input messages	Number of discarded incoming messages.
Discarded output messages	Number of discarded outgoing messages.
Elapsed time since last connection or counters clear	Elapsed time since the MSDP peer information was last cleared.
Mesh group peer joined	Mesh group that the MSDP peer has joined. This field is not displayed if the MSDP peer does not join a mesh group.
Last disconnect reason	Reason why last MSDP peering connection was torn down. If the connection is not terminated, this field is not displayed. • **Hold timer expired without message**—Hold timer expires and the receiving cache has no messages. • **Hold timer expired with truncated message**—Hold timer expires and messages in the receiving cache are not intact. ○ **bytes in buffer**—Size of data in the receiving cache when the connection was terminated. ○ **type**—Type of packets in the receiving cache when the connection was terminated. ○ **length**—Length of packets in the receiving cache when the connection was terminated. If the packet is too small in size,

Field	Description
	this field cannot be resolved and is not displayed. ○ **without packet time**—Length of time since packets were last processed. • **Remote peer has been closed**—The MSDP peering connection has been torn down. • **TCP ERROR/HUP event received**—Error/hup event received by the TCP socket when the MSDP peer sent messages. • **Illegal message received**—The MSDP peer received illegal messages. • **Notification received**—The MSDP peer received notification messages. • **Reset command executed**—The user executed the **reset msdp peer** command. • **Shutdown command executed**—The user executed the **shutdown** command. • **Interface downed**—The MSDP peer received the interface down event when connecting to the remote MSDP peer.
Information about (Source, Group)-based SA filtering policy	SA message filtering list information: • **Import policy**—Filter list for receiving SA messages from the specified MSDP peer. • **Export policy**—Filter list for forwarding SA messages from the specified MSDP peer.
Information about SA-Requests	SA request information: • **Policy to accept SA request messages**—Filtering rule for receiving or forwarding SA request messages from the specified MSDP peer. If SA request messages are not filtered, this field displays **None**. • **Sending SA requests status**—Whether the MSDP peer is enabled to send an SA request message to the designated MSDP peer after receiving a new join message.
Minimum TTL to forward SA with encapsulated data	Minimum TTL value for the multicast packets encapsulated in SA messages.
SAs learned from this peer	Number of cached (S, G) entries learned from the specified MSDP peer.
SA-cache maximum for the peer	Maximum number of (S, G) entries learned from the specified MSDP peer that the device can cache.
Input queue size	Data size cached in the input queue.
Output queue size	Data size cached in the output queue.
Counters for MSDP message	MSDP peer statistics: • **RPF check failure**—Number of SA messages discarded because of RPF check failure. • **Incoming/outgoing SA**—Number of received and sent SA messages. • **Incoming/outgoing SA-Request**—Number of received and sent SA requests. • **Incoming/outgoing SA-Response**—Number of received and sent SA responses. • **Incoming/outgoing Keepalive**—Number of received and sent keepalive messages. • **Incoming/outgoing Notification**—Number of received and sent notification messages. • **Incoming/outgoing Traceroutes in progress**—Number of received and sent traceroute-in-progress messages.

Field	Description
	• **Incoming/outgoing Traceroute reply**—Number of received and sent traceroute replies. • **Incoming/outgoing Unknown**—Number of received and sent unknown messages. • **Incoming/outgoing data packet**—Number of received and sent SA messages encapsulated with multicast data.

display msdp sa-cache

Use **display msdp sa-cache** to display (S, G) entries in the SA cache.

Syntax

display msdp [**vpn-instance** *vpn-instance-name*] **sa-cache** [*group-address* | *source-address* | *as-number*] *

Views

Any view

Predefined user roles

network-admin

network-operator

mdc-admin

mdc-operator

Parameters

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, this command displays (S, G) entries in the SA cache on the public network.

group-address: Specifies a multicast group address in the range of 224.0.1.0 to 239.255.255.255. If you do not specify a multicast group, this command displays (S, G) entries for all multicast groups.

source-address: Specifies a multicast source address. If you do not specify a multicast source, this command displays (S, G) entries for all sources.

as-number: Specifies an AS number in the range of 1 to 4294967295. If you do not specify an AS number, this command displays (S, G) entries for all ASs.

Usage guidelines

You must execute the **cache-sa-enable** command before you execute this command. Otherwise, this command does not give any output.

Examples

# Display information about the (S, G) entries in the SA cache on the public network.

```
<Sysname> display msdp sa-cache
Total Source-Active Cache - 5 entries
Matched 5 entries

Source          Group           Origin RP       Pro  AS         Uptime   Expires
10.10.1.2       225.0.0.1       10.10.10.10     BGP  100        00:00:11 00:05:49
10.10.1.2       225.0.0.2       10.10.10.10     BGP  100        00:00:11 00:05:49
10.10.1.2       225.0.0.3       10.10.10.10     BGP  100        00:00:11 00:05:49
10.10.1.2       225.0.0.4       10.10.10.10     BGP  100        00:00:11 00:05:49
```

```
10.10.1.2       225.0.0.5       10.10.10.10     BGP  100        00:00:11 00:05:49
```

Table 34 Command output

Field	Description
Total Source-Active Cache	Total number of multicast sources in the SA cache.
Matched	Total number of (S, G) entries that match a multicast source.
Source	Multicast source address.
Group	Multicast group address.
Origin RP	Address of the RP that generated the (S, G) entry.
Pro	Type of protocol from which the AS number of the origin RP originates. If the system could not obtain the AS number, this field displays a question mark (?).
AS	AS number of the origin RP. If the system could not obtain the AS number, this field displays a question mark (?).
Uptime	Length of time for which the cached (S, G) entry has existed.
Expires	Length of time in which the cached (S, G) entry will expire.

Related commands

cache-sa-enable

display msdp sa-count

Use **display msdp sa-count** to display the number of (S, G) entries in the SA cache.

Syntax

display msdp [**vpn-instance** *vpn-instance-name*] **sa-count** [*as-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

mdc-admin

mdc-operator

Parameters

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, this command displays the number of (S, G) entries in the SA cache on the public network.

as-number: Specifies an AS number in the range of 1 to 4294967295. If you do not specify an AS number, this command displays the number of (S, G) entries in the SA cache of all ASs.

Usage guidelines

You must execute the **cache-sa-enable** command before you execute this command. Otherwise, this command does not give any output.

Examples

# Display the number of (S, G) entries in the SA cache on the public network.

```
<Sysname> display msdp sa-count
(S, G) entries statistics, counted by peer
  Peer address       SA count
  10.10.10.10        5

(S, G) entries statistics, counted by AS
  AS         Source count        Group count
  ?          3                   3

5 (S, G) entries in total
```

Table 35 Command output

Field	Description
(S, G) entries statistics, counted by peer	Number of (S, G) entries on an MSDP peer basis.
Peer address	Address of the MSDP peer that sent SA messages.
SA count	Number of (S, G) entries from this MSDP peer.
(S, G) entries statistics, counted by AS	Number of cached (S, G) entries on an AS basis.
AS	AS number. If the system could not obtain the AS number, this field displays a question mark (?).
Source count	Number of multicast sources from this AS.
Group count	Number of multicast groups from this AS.
(S, G) entries in total	Total number of (S, G) entries.

Related commands

cache-sa-enable

encap-data-enable

Use **encap-data-enable** to enable multicast data encapsulation in SA messages.

Use **undo encap-data-enable** to restore the default.

Syntax

encap-data-enable

undo encap-data-enable

Default

An SA message contains only (S, G) entries. No multicast data is encapsulated in an SA message.

Views

MSDP view

Predefined user roles

network-admin

mdc-admin

Examples

# Enable multicast data encapsulation in SA messages on the public network.

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

```
[Sysname] msdp
[Sysname-msdp] encap-data-enable
```

import-source

Use **import-source** to configure an SA message creation policy.

Use **undo import-source** to remove the configured SA message creation policy.

Syntax

import-source [**acl** *acl-number*]

undo import-source

Default

When an SA message is created, all the (S, G) entries within the domain are advertised in the SA message.

Views

MSDP view

Predefined user roles

network-admin

mdc-admin

Parameters

acl-number: Specifies an IPv4 basic or advanced ACL number in the range of 2000 to 3999. If you specify an ACL, this command advertises only the (S, G) entries that the ACL permits. This command does not advertise any (S, G) entries when any of the following conditions exists:

- You do not specify an ACL.
- The specified ACL does not exist.
- The specified ACL does not have valid rules.

Usage guidelines

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

- For the rule to take effect, do not specify the **vpn-instance** *vpn-instance* option.
- In a basic ACL, the **source** *source-address source-wildcard* option specifies a multicast group address.
- In an advanced ACL, the **source** *source-address source-wildcard* option specifies a multicast source address. The **destination** *dest-address dest-wildcard* option specifies a multicast group address.
- Among the other optional parameters, only the **fragment** keyword and the **time-range** *time-range-name* option take effect.

This command controls the creation of SA messages. You can also use the **peer sa-policy** command to configure a filtering rule to control forwarding and acceptance of SA messages.

Examples

# On the public network, configure an SA creation policy to advertise only the (10.10.0.0/16, 225.1.0.0/16) entries when an SA message is created.

```
<Sysname> system-view
[Sysname] acl number 3101
[Sysname-acl-adv-3101] rule permit ip source 10.10.0.0 0.0.255.255 destination 225.1.0.0
0.0.255.255
```

```
[Sysname-acl-adv-3101] quit
[Sysname] msdp
[Sysname-msdp] import-source acl 3101
```

Related commands

peer sa-policy

msdp

Use **msdp** to enable MSDP and enter MSDP view.

Use **undo msdp** to disable MSDP and remove the configurations in MSDP.

Syntax

msdp [**vpn-instance** *vpn-instance-name*]

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

Default

MSDP is disabled.

Views

System view

Predefined user roles

network-admin

mdc-admin

Parameters

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, this command applies to the public network.

Usage guidelines

This command takes effect only when IP multicast routing is enabled.

Examples

# Enable IP multicast routing on the public network, and enable MSDP on the public network and enter public network MSDP view.

```
<Sysname> system-view
[Sysname] multicast routing
[Sysname-mrib] quit
[Sysname] msdp
[Sysname-msdp]
```

Related commands

multicast routing

originating-rp

Use **originating-rp** to configure an interface address as the RP address of SA messages.

Use **undo originating-rp** to remove the configuration.

Syntax

originating-rp *interface-type interface-number*

undo originating-rp

Default

The PIM RP address is used as the RP address of SA messages.

Views

MSDP view

Predefined user roles

network-admin

mdc-admin

Parameters

interface-type interface-number: Specifies an interface by its type and number.

Examples

# On the public network, specify the IP address of VLAN-interface 100 as the RP address of SA messages.

```
<Sysname> system-view
[Sysname] msdp
[Sysname-msdp] originating-rp vlan-interface 100
```

peer connect-interface

Use **peer connect-interface** to create an MSDP peering connection.

Use **undo peer connect-interface** to remove an MSDP peering connection.

Syntax

peer *peer-address* **connect-interface** *interface-type interface-number*

undo peer *peer-address*

Default

MSDP peering connection is not created.

Views

MSDP view

Predefined user roles

network-admin

mdc-admin

Parameters

peer-address: Specifies an MSDP peer by its IP address.

interface-type interface-number: Specifies an interface by its type and number. The local device uses the primary IP address of the specified interface as the source IP address when setting up a TCP connection with the remote MSDP peer.

Usage guidelines

You must execute this command before you use any other **peer** command. Otherwise, the system notifies you that the MSDP peer does not exist.

Examples

# On the public network, configure the router with the IP address 125.10.7.6 as the MSDP peer of the local router, and configure VLAN-interface 100 as the local connection port.

```
<Sysname> system-view
[Sysname] msdp
[Sysname-msdp] peer 125.10.7.6 connect-interface vlan-interface 100
```

peer description

Use **peer description** to configure a description for an MSDP peer.

Use **undo peer description** to delete the description for an MSDP peer.

Syntax

peer *peer-address* **description** *text*

undo peer *peer-address* **description**

Default

No description is configured for an MSDP peer.

Views

MSDP view

Predefined user roles

network-admin

mdc-admin

Parameters

peer-address: Specifies an MSDP peer by its IP address.

text: Specifies a description, a case-sensitive string of 1 to 80 characters, including spaces.

Examples

# On the public network, configure the description for the device at 125.10.7.6 as **CustomerA**.

```
<Sysname> system-view
[Sysname] msdp
[Sysname-msdp] peer 125.10.7.6 description CustomerA
```

peer mesh-group

Use **peer mesh-group** to configure an MSDP peer as a mesh group member.

Use **undo peer mesh-group** to remove an MSDP peer from the mesh group.

Syntax

peer *peer-address* **mesh-group** *name*

undo peer *peer-address* **mesh-group**

Default

An MSDP peer does not belong to any mesh group.

Views

MSDP view

Predefined user roles

network-admin

mdc-admin

Parameters

peer-address: Specifies an MSDP peer by its IP address.

name: Specifies a mesh group, a case-sensitive string of 1 to 32 characters. A mesh group name must not contain any spaces.

Examples

# On the public network, configure the MSDP peer 125.10.7.6 as a member of the mesh group **Group1**.

```
<Sysname> system-view
[Sysname] msdp
[Sysname-msdp] peer 125.10.7.6 mesh-group Group1
```

peer minimum-ttl

Use **peer minimum-ttl** to configure the lower TTL threshold for multicast data packets encapsulated in SA messages.

Use **undo peer minimum-ttl** to restore the default.

Syntax

peer *peer-address* **minimum-ttl** *ttl-value*

undo peer *peer-address* **minimum-ttl**

Default

The lower TTL threshold for a multicast packet to be encapsulated in an SA message is 0.

Views

MSDP view

Predefined user roles

network-admin

mdc-admin

Parameters

peer-address: Specifies an MSDP peer by its IP address.

ttl-value: Specifies the lower TTL threshold in the range of 0 to 255.

Examples

# On the public network, set the lower TTL threshold for multicast packets to be encapsulated in SA messages to 10. Only multicast data packets whose TTL value is larger than or equal to 10 can be encapsulated in SA messages and forwarded to the MSDP peer 110.10.10.1.

```
<Sysname> system-view
[Sysname] msdp
[Sysname-msdp] peer 110.10.10.1 minimum-ttl 10
```

peer password

Use **peer password** to configure an MD5 authentication key used by both MSDP peers to establish a TCP connection.

Use **undo peer password** to restore the default.

Syntax

peer *peer-address* **password** { **cipher** | **simple** } *password*

undo peer *peer-address* **password**

Default

MSDP peers do not perform MD5 authentication to establish TCP connections.

Views

MSDP view

Predefined user roles

network-admin

mdc-admin

Parameters

peer-address: Specifies an MSDP peer by its IP address.

cipher: Specifies a ciphertext MD5 authentication key.

simple: Specifies a plaintext MD5 authentication key.

password: Specifies the key string. This argument is case sensitive. If **simple** is specified, it must be a string of 1 to 80 characters. If **cipher** is specified, it must be a ciphertext string of 33 to 137 characters.

Usage guidelines

The MSDP peers involved in MD5 authentication must be configured with the same authentication method and key. Otherwise, the authentication fails and the TCP connection cannot be established.

For security purposes, all keys, including keys configured in plain text, are saved in cipher text.

Examples

# On the public network, configure an MD5 authentication key in plaintext as **aabbcc** for the TCP connections between the local end and the MSDP peer 10.1.100.1. The configuration on the remote peer is similar.

```
<Sysname> system-view
[Sysname] msdp
[Sysname-msdp] peer 10.1.100.1 password simple aabbcc
```

peer request-sa-enable

Use **peer request-sa-enable** to enable the device to send an SA request message to an MSDP peer after receiving a new join message.

Use **undo peer request-sa-enable** to disable the device from sending an SA request message to the specified MSDP peer.

Syntax

peer *peer-address* **request-sa-enable**

undo peer *peer-address* **request-sa-enable**

Default

After receiving a new join message, the device does not send an SA request message to any MSDP peer. Instead, it waits for the next SA message to come.

Views

MSDP view

Predefined user roles

network-admin

mdc-admin

Parameters

peer-address: Specifies an MSDP peer by its IP address.

Usage guidelines

You must disable SA message cache mechanism before you execute this command. Otherwise, the device does not send out SA request messages.

Examples

# On the public network, disable the SA message cache mechanism. Enable the device to send an SA request message to the MSDP peer 125.10.7.6 after it receives a new join message.

```
<Sysname> system-view
[Sysname] msdp
[Sysname-msdp] undo cache-sa-enable
[Sysname-msdp] peer 125.10.7.6 request-sa-enable
```

Related commands

- **cache-sa-enable**
- **display msdp peer-status**

peer sa-cache-maximum

Use **peer sa-cache-maximum** to configure the maximum number of cached (S, G) entries learned from an MSDP peer.

Use **undo peer sa-cache-maximum** to restore the default.

Syntax

peer *peer-address* **sa-cache-maximum** *sa-limit*

undo peer *peer-address* **sa-cache-maximum**

Default

The device can cache a maximum of 4294967295 (S, G) entries learned from any MSDP peer.

Views

MSDP view

Predefined user roles

network-admin

mdc-admin

Parameters

peer-address: Specifies an MSDP peer by its IP address.

sa-limit: Specifies the maximum number of (S, G) entries that the device can cache, in the range of 1 to 4294967295.

Examples

# On the public network, enable the device to cache up to 100 (S, G) entries learned from its MSDP peer 125.10.7.6.

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

```
[Sysname] msdp
[Sysname-msdp] peer 125.10.7.6 sa-cache-maximum 100
```

Related commands

- **display msdp brief**
- **display msdp peer-status**
- **display msdp sa-count**

peer sa-policy

Use **peer sa-policy** to configure an SA incoming or outgoing policy.

Use **undo peer sa-policy** to remove the configured SA incoming or outgoing policy.

Syntax

peer *peer-address* **sa-policy** { **export** | **import** } [**acl** *acl-number*]

undo peer *peer-address* **sa-policy** { **export** | **import** }

Default

All SA messages are accepted or forwarded.

Views

MSDP view

Predefined user roles

network-admin

mdc-admin

Parameters

export: Specifies the outgoing direction.

import: Specifies the incoming direction.

peer-address: Specifies an MSDP peer by its IP address.

acl-number: Specifies an IPv4 advanced ACL number in the range of 3000 to 3999. If you specify an ACL, the device accepts and forwards only SA messages that the ACL permits. If you do not specify an ACL, the device discards all SA messages when any of the following conditions exists:

- You do not specify an ACL.
- The specified ACL does not exist.
- The specified ACL does not have valid rules.

Usage guidelines

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

- For the rule to take effect, do not specify the **vpn-instance** *vpn-instance* option.
- The **source** *source-address source-wildcard* option specifies a multicast source address.
- The **destination** *dest-address dest-wildcard* option specifies a multicast group address.
- Among the other optional parameters, only the **fragment** keyword and the **time-range** *time-range-name* option take effect.

This command controls the acceptance and forwarding of SA messages. You can also use the **import-source** command to configure a filtering rule to control the creation of SA messages.

Examples

# On the public network, configure an SA outgoing policy to forward only SA messages that ACL 3100 permits to the MSDP peer 125.10.7.6.

```
<Sysname> system-view
[Sysname] acl number 3100
[Sysname-acl-adv-3100] rule permit ip source 170.15.0.0 0.0.255.255 destination 225.1.0.0
0.0.255.255
[Sysname-acl-adv-3100] quit
[Sysname] msdp
[Sysname-msdp] peer 125.10.7.6 connect-interface vlan-interface 100
[Sysname-msdp] peer 125.10.7.6 sa-policy export acl 3100
```

Related commands

- **display msdp peer-status**
- **import-source**

peer sa-request-policy

Use **peer sa-request-policy** to configure an SA request policy.

Use **undo peer sa-request-policy** to remove the configured SA request policy.

Syntax

peer *peer-address* **sa-request-policy** [**acl** *acl-number*]

undo peer *peer-address* **sa-request-policy**

Default

SA request messages are not filtered.

Views

MSDP view

Predefined user roles

network-admin

mdc-admin

Parameters

peer-address: Specifies an MSDP peer by its IP address.

acl-number: Specifies an IPv4 basic ACL number in the range of 2000 to 2999. If you specify an ACL, the switch accepts only SA requests that the ACL permits. All SA requests are filtered out when any of the following conditions exists:

- You do not specify an ACL.
- The specified ACL does not exist.
- The specified ACL does not have valid rules.

Usage guidelines

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

- For the rule to take effect, do not specify the **vpn-instance** *vpn-instance* option.
- The **source** *source-address source-wildcard* option specifies a multicast group address.
- Among the other optional parameters, only the **fragment** keyword and the **time-range** *time-range-name* option take effect.

Examples

# On the public network, configure an SA request policy to process SA requests originated from the MSDP peer 175.58.6.5 with multicast groups in the range of 225.1.1.0/24.

```
<Sysname> system-view
[Sysname] acl number 2001
[Sysname-acl-basic-2001] rule permit source 225.1.1.0 0.0.0.255
[Sysname-acl-basic-2001] quit
[Sysname] msdp
[Sysname-msdp] peer 175.58.6.5 sa-request-policy acl 2001
```

reset msdp peer

Use **reset msdp peer** to reset the TCP connection with an MSDP peer and clear statistics for the MSDP peer.

Syntax

reset msdp [**vpn-instance vpn-instance**-*name*] **peer** [*peer-address*]

Views

User view

Predefined user roles

network-admin

mdc-admin

Parameters

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, this command resets the TCP connection with the specified MSDP peer and clears statistics for the MSDP peer on the public network.

peer-address: Specifies an MSDP peer by its IP address. If you do not specify an MSDP peer, this command resets the TCP connections with all MSDP peers and clears statistics for all MSDP peers.

Examples

# On the public network, reset the TCP connection with the MSDP peer 125.10.7.6, and clear all statistics for this MSDP peer.

```
<Sysname> reset msdp peer 125.10.7.6
```

reset msdp sa-cache

Use **reset msdp sa-cache** to clear (S, G) entries from the SA cache.

Syntax

reset msdp [**vpn-instance vpn-instance**-*name*] **sa-cache** [*group-address*]

Views

User view

Predefined user roles

network-admin

mdc-admin

Parameters

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, this command clears (S, G) entries from the SA cache on the public network.

group-address: Specifies a multicast group address in the range of 224.0.1.0 to 239.255.255.255. If you do not specify a multicast group, this command clears the cached (S, G) entries for all multicast groups from the SA cache.

Examples

# Clear the (S, G) entries for the multicast group 225.5.4.3 from the SA cache on the public network.

```
<Sysname> reset msdp sa-cache 225.5.4.3
```

Related commands

- **cache-sa-enable**
- **display msdp sa-cache**

reset msdp statistics

Use **reset msdp statistics** to clear statistics for the specified MSDP peer without resetting the TCP connection with the MSDP peer.

Syntax

reset msdp [**vpn-instance vpn-instance**-*name*] **statistics** [*peer-address*]

Views

User view

Predefined user roles

network-admin

mdc-admin

Parameters

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, this command clears statistics for the specified MSDP peer without resetting the TCP connection with the MSDP peer on the public network.

peer-address: Specifies an MSDP peer by its IP address. If you do not specify an MSDP peer, this command clears statistics for all MSDP peers without resetting the TCP connection with all the MSDP peers.

Examples

# Clear statistics for the MSDP peer 125.10.7.6 without resetting the TCP connection with the MSDP peer on the public network.

```
<Sysname> reset msdp statistics 125.10.7.6
```

shutdown (MSDP view)

Use **shutdown** to tear down the connection with an MSDP peer.

Use **undo shutdown** to re-establish the connection with an MSDP peer.

Syntax

shutdown *peer-address*

undo shutdown *peer-address*

Default

The connections with all MSDP peers are active.

Views

MSDP view

Predefined user roles

network-admin

mdc-admin

Parameters

peer-address: Specifies an MSDP peer by its IP address.

Examples

# Tear down the connection with the MSDP peer 125.10.7.6 on the public network.

```
<Sysname> system-view
[Sysname] msdp
[Sysname-msdp] shutdown 125.10.7.6
```

Related commands

- **display msdp brief**
- **display msdp peer-status**

static-rpf-peer

Use **static-rpf-peer** to configure a static RPF peer.

Use **undo static-rpf-peer** to remove a static RPF peer.

Syntax

static-rpf-peer *peer-address* [**rp-policy** *ip-prefix-name*]

undo static-rpf-peer *peer-address*

Default

No static RPF peer is configured.

Views

MSDP view

Predefined user roles

network-admin

mdc-admin

Parameters

peer-address: Specifies an MSDP peer by its IP address.

rp-policy *ip-prefix-name*: Specifies a filtering policy based on the RP addresses in SA messages. The *ip-prefix-name* argument is the filtering policy name, a case-sensitive string of 1 to 63 characters.

Usage guidelines

When you configure multiple static RPF peers at the same time, observe the following rules:

- If the **rp-policy** keyword is specified for all the static RPF peers, SA messages from the active static RPF peers are filtered according to the configured filtering policy. The router receives only SA messages that have passed the filtering.
- If the **rp-policy** keyword is not specified for the static RPF peers, the router receives all SA messages from the active static RPF peers.

Examples

# Configure a static RPF peer on the public network.

```
<Sysname> system-view
[Sysname] ip prefix-list list1 permit 130.10.0.0 16 greater-equal 16 less-equal 32
[Sysname] msdp
[Sysname-msdp] peer 130.10.7.6 connect-interface vlan-interface 100
[Sysname-msdp] static-rpf-peer 130.10.7.6 rp-policy list1
```

Related commands

- **display msdp peer-status**
- **ip prefix-list**

timer retry

Use **timer retry** to configure the interval between MSDP peering connection attempts.

Use **undo timer retry** to restore the default.

Syntax

timer retry *interval*

undo timer retry

Default

The interval between MSDP peering connection attempts is 30 seconds.

Views

MSDP view

Predefined user roles

network-admin

mdc-admin

Parameters

interval: Specifies an interval between MSDP peering connection attempts, in the range of 1 to 60 seconds.

Examples

# Set the MSDP peering connection attempt interval to 60 seconds on the public network.

```
<Sysname> system-view
[Sysname] msdp
[Sysname-msdp] timer retry 60
```

Document conventions and icons

Conventions

This section describes the conventions used in the documentation.

Port numbering in examples

The port numbers in this document are for illustration only and might be unavailable on your device.

Command conventions

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

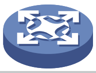
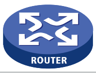
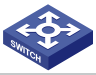
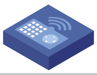
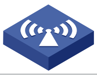
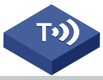
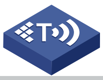
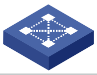
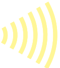
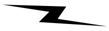
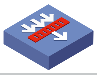
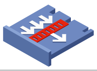
GUI conventions

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

Symbols

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

Network topology icons

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

Support and other resources

Accessing Hewlett Packard Enterprise Support

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

  www.hpe.com/assistance
- To access documentation and support services, go to the Hewlett Packard Enterprise Support Center website:

  www.hpe.com/support/hpesc

Information to collect

- Technical support registration number (if applicable)
- Product name, model or version, and serial number
- Operating system name and version
- Firmware version
- Error messages
- Product-specific reports and logs
- Add-on products or components
- Third-party products or components

Accessing updates

- Some software products provide a mechanism for accessing software updates through the product interface. Review your product documentation to identify the recommended software update method.
- To download product updates, go to either of the following:
  - Hewlett Packard Enterprise Support Center **Get connected with updates** page:

    www.hpe.com/support/e-updates
  - Software Depot website:

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

www.hpe.com/support/AccessToSupportMaterials

IMPORTANT:

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

Websites

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

Customer self repair

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

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

www.hpe.com/support/selfrepair

Remote support

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

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

www.hpe.com/info/insightremotesupport/docs

Documentation feedback

Hewlett Packard Enterprise is committed to providing documentation that meets your needs. To help us improve the documentation, send any errors, suggestions, or comments to Documentation Feedback (docsfeedback@hpe.com). When submitting your feedback, include the document title, part number, edition, and publication date located on the front cover of the document. For online help content, include the product name, product version, help edition, and publication date located on the legal notices page.

Index