5 Ethernet Switching Configuration Commands

5.1 MAC Address Table Configuration Commands

5.1.1 Command Support

Commands provided in this section and all the parameters in the commands are supported by all switch models (except the S5731-L and S5731S-L), unless otherwise specified. For details, see specific commands.

5.1.2 display bridge mac-address

Function

The **display bridge mac-address** command displays the bridge MAC address of a device.

Format

display bridge mac-address

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

When you need to view the bridge MAC address of a device, run the **display bridge mac-address** command.

Example

# Display the bridge MAC address of a device.

```
<HUAWEI> display bridge mac-address
System bridge MAC address: 00e0-fc4b-6d00
```

Table 5-1 Description of the display bridge mac-address command output

Item	Description
System bridge MAC address	Indicates the bridge MAC address of a device.

5.1.3 display mac-address

Function

The **display mac-address** command displays the MAC address table of the switch. A MAC address entry contains the destination MAC address, VLAN ID/VSI/BD, outbound interface, and entry type.

Format

display mac-address [*mac-address*] [**vlan** *vlan-id* | **vsi** *vsi-name*] [**verbose**]

display mac-address [**vlan** *vlan-id* | *interface-type interface-number*] * [**verbose**]

Parameters

Parameter	Description	Value
mac-address	Specifies the destination MAC address in an entry.	The value is in H-H-H format. H is a hexadecimal number of 4 digits, for example, 00e0 and fc01. If you enter less than four digits, 0s are prefixed to the input digits. For example, if you enter e0, the system changes e0 to 00e0. The MAC address cannot be FFFF-FFFF-FFFF, 0000-0000-0000, or a multicast MAC address.
vlan *vlan-id*	Displays MAC address entries in a specified VLAN.	The value is an integer that ranges from 1 to 4094.
vsi *vsi-name*	Displays MAC address entries in a specified VSI. **NOTE** Only the S5731-H, S5731S-H, S5732-H, S5731-S, S5731S-S, S6730-S, S6730S-S, S6735-S, S6720-EI, S6720S-EI, S6730S-H, and S6730-H support this parameter.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Parameter	Description	Value
interface-type interface-number	Displays the MAC address entries with a specified outbound interface. ● *interface-type* specifies the type of the outbound interface. ● *interface-number* specifies the number of the outbound interface.	-
verbose	Displays detailed information about MAC address entries.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

The MAC address table of the switch stores MAC addresses of other devices. When forwarding an Ethernet frame, the switch searches the MAC address table for the outbound interface according to the destination MAC address and VLAN ID in the Ethernet frame.

The **display mac-address** command displays all MAC address entries, such as dynamic MAC address entries, static MAC address entries, and blackhole MAC address entries. A MAC address entry contains the destination MAC address, VLAN ID/VSI/BD, outbound interface, and entry type.

Follow-up Procedure

If any MAC address entry in the command output is incorrect, run the **undo mac-address** command to delete the entry or run the **mac-address static** command to add a correct one.

Precautions

If you run the **display mac-address** command without parameters, all MAC address entries are displayed.

When the switch has a large number of MAC address entries, it is recommended that you specify parameters in the command to filter the output information. Otherwise, the following problems may occur due to excessive output information:

- The displayed information is repeatedly refreshed, so you cannot find the required information.
- The system traverses and retrieves information for a long time, and does not respond to any request.

Example

# Display all MAC address entries.

```
<HUAWEI> display mac-address
-------------------------------------------------------------------------------
MAC Address        VLAN/VSI/BD              Learned-From       Type
-------------------------------------------------------------------------------
00e0-fc12-3458     100/-/-                  GE0/0/1            dynamic
00e0-fc12-3457     200/-/-                  GE0/0/2            static
-------------------------------------------------------------------------------
Total items displayed = 2
```

# Display detailed information about all MAC address entries in VLAN 10.

```
<HUAWEI> display mac-address vlan 10 verbose
-------------------------------------------------------------------------------
MAC Address : 00e0-fc12-3457           VLAN : 10
Learned-From: GE0/0/2                Type : dynamic

-------------------------------------------------------------------------------
Total items displayed = 1
```

Table 5-2 Description of the **display mac-address** command output

Item	Description
MAC Address	Destination MAC address in a MAC address entry.
VLAN/VSI/BD	ID of the VLAN, or name of the VSI, or ID of the BD that a MAC address belongs to.
Learned-From	Interface that learns a MAC address.

Item	Description
Type	Type of a MAC address entry. ● static: indicates a static MAC address entry, which is manually configured and will not be aged out, configured by using the **mac-address static vlan**, **mac-address static vlanif**, **mac-address static vsi**, **mac-address static bridge-domain**, or **mac-address static bridge-domain vni** command. ● blackhole: indicates a blackhole MAC address entry, which is manually configured and will not be aged out, configured by using the **mac-address blackhole** command. ● dynamic: indicates a MAC address entry learned by the switch, which will be aged out when the aging time expires. ● security: indicates a MAC address entry that an interface learns after port security is enabled. ● sec-config: indicates a static secure MAC address entry configured by using the **port-security mac-address** command. ● sticky: indicates a MAC address entry that an interface learns after the sticky MAC function is enabled. ● mux: indicates a MAC address entry learned by a MUX VLAN enabled interface. ● snooping: indicates a static MAC address entry generated based on the dynamic DHCP snooping binding table. ● authen: indicates a MAC address entry corresponding to the NAC authentication user that obtains an IP address (excluding the Layer 3 authentication user of which the MAC address cannot be generated and wireless user in direct forwarding mode). ● evpn: indicates a MAC address entry of EVPN. ● sticky-config: indicates a MAC address entry configured through the **port-security mac-address sticky-config** command.

5.1.4 display mac-address aging-time

Function

The **display mac-address aging-time** command displays the aging time of dynamic MAC address entries in the MAC address table.

Format

display mac-address aging-time

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

This command displays the aging time of dynamic MAC address entries on the switch. You can check whether the aging time is suitable for network requirements and device performance.

Follow-up Procedure

If the aging time is unsuitable for requirements or device performance, run the **mac-address aging-time** command to set the aging time properly.

Precautions

If the aging time is 0, dynamic MAC addresses will not be aged out. In this case, MAC address entries increase sharply and the MAC address table will be full quickly.

Example

# Display the aging time of dynamic MAC address entries.

```
<HUAWEI> display mac-address aging-time
  Aging time: 300 second(s)
```

Table 5-3 Description of the display mac-address aging-time command output

Item	Description
Aging time	Aging time of dynamic MAC address entries, in seconds. To set the aging time, run the **mac-address aging-time** command.

5.1.5 display mac-address blackhole

Function

The **display mac-address blackhole** command displays blackhole MAC address entries.

Format

display mac-address blackhole [**vlan** *vlan-id* | **vsi** *vsi-name*] [**verbose**]

Parameters

Parameter	Description	Value
vlan *vlan-id*	Displays blackhole MAC address entries in a specified VLAN.	The value is an integer that ranges from 1 to 4094.
vsi *vsi-name*	Displays blackhole MAC address entries of a specified virtual switch instance (VSI). *vsi-name* specifies the name of a VSI. **NOTE** Only the S5731-H, S5731S-H, S5732-H, S5731-S, S5731S-S, S6730-S, S6730S-S, S6735-S, S6720-EI, S6720S-EI, S6730S-H, and S6730-H support this parameter.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
verbose	Displays detailed information about blackhole MAC address entries.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

The MAC address table of the switch stores MAC addresses of other devices. When forwarding an Ethernet frame, the switch searches the MAC address table for the outbound interface according to the destination MAC address and VLAN ID in the Ethernet frame.

The MAC address table contains the following MAC address entries:

- Blackhole MAC address entries that are used to discard packets with the specified MAC addresses or destination MAC addresses. Blackhole MAC address entries are manually configured and will not be aged out.
- Static MAC entries that are manually configured and will not be aged out.
- Dynamic MAC address entries that are learned by the switch and will be aged out when the aging time expires.

To check whether blackhole MAC address entries are configured correctly, run this command. These entries ensure communication between authorized users.

Follow-up Procedure

If any blackhole MAC address entry in the command output is incorrect, run the **undo mac-address** command to delete the entry or run the **mac-address blackhole** command to add a correct one.

Precautions

- If you run the **display mac-address blackhole** command without parameters, all blackhole MAC address entries are displayed.
- If the MAC address table does not contain any blackhole MAC address, no information is displayed.

Example

# Display all blackhole MAC address entries.

```
<HUAWEI> display mac-address blackhole
-------------------------------------------------------------------------------
MAC Address         VLAN/VSI/BD                 Learned-From         Type
-------------------------------------------------------------------------------
00e0-fc22-0033      100/-/-                 -                   blackhole
00e0-fc00-0001      200/-/-                 -                   blackhole

-------------------------------------------------------------------------------
Total items displayed = 2
```

# Display blackhole MAC address entries in VLAN 100.

```
<HUAWEI> display mac-address blackhole vlan 100
-------------------------------------------------------------------------------
MAC Address         VLAN/VSI/BD                 Learned-From        Type
-------------------------------------------------------------------------------
00e0-fc22-0033      100/-/-                  -                  blackhole
00e0-fc00-0001      100/-/-                  -                  blackhole

-------------------------------------------------------------------------------
Total items displayed = 2
```

Table 5-4 Description of the display mac-address blackhole command output

Item	Description
MAC Address	Destination MAC address in a blackhole MAC address entry.
VLAN/VSI/BD	ID of the VLAN, name of the VSI, or ID of the BD that a MAC address belongs to.
Learned-From	When the type of a MAC address entry is blackhole, "-" is displayed.

Item	Description
Type	Type of a MAC address entry. blackhole: indicates a blackhole MAC address entry, which is manually configured and will not be aged out, configured by using the **mac-address blackhole** command.

5.1.6 display mac-address dynamic

Function

The **display mac-address dynamic** command displays dynamic MAC address entries.

Format

display mac-address dynamic [[**slot**] *slot-id*] [**vlan** *vlan-id* | *interface-type interface-number*] * [**verbose**]

display mac-address dynamic [[**slot**] *slot-id*] [**vsi** *vsi-name* [**peer** *ip-address*]] [**verbose**]

Parameters

Parameter	Description	Value
slot *slot-id*	Displays dynamic MAC address entries on a specified card.	The value is an integer and must be the slot ID of a running card.
vlan *vlan-id*	Displays dynamic MAC address entries in a specified VLAN.	The value is an integer that ranges from 1 to 4094.
vsi *vsi-name*	Displays dynamic MAC address entries of a specified virtual switch instance (VSI). *vsi-name* specifies the name of a VSI. **NOTE** Only the S5731-H, S5731S-H, S5732-H, S5731-S, S5731S-S, S6730-S, S6730S-S, S6735-S, S6720-EI, S6720S-EI, S6730S-H, and S6730-H support this parameter.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Parameter	Description	Value
peer *ip-address*	Displays the dynamic MAC address entry mapped to a specified peer IPv4 address. **NOTE** Only the S5731-H, S5731S-H, S5732-H, S5731-S, S5731S-S, S6730-S, S6730S-S, S6735-S, S6720-EI, S6720S-EI, S6730S-H, and S6730-H support this parameter.	-
interface-type interface-number	Displays dynamic MAC address entries with a specified outbound interface. ● *interface-type* specifies the type of the outbound interface. ● *interface-number* specifies the number of the outbound interface.	-
verbose	Displays detailed information about dynamic MAC address entries.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

The MAC address table needs to be updated constantly because the network topology always changes. You can use this command to view learned MAC addresses in real time.

Follow-up Procedure

If the displayed dynamic MAC address entries are invalid, run the **undo mac-address** command to delete dynamic MAC address entries.

Precautions

If you run the **display mac-address dynamic** command without parameters, all dynamic MAC address entries are displayed.

If the MAC address table does not contain any dynamic MAC address entry, no information is displayed.

When the switch has a large number of dynamic MAC address entries, it is recommended that you specify parameters in the command to filter the output information. Otherwise, the following problems may occur due to excessive output information:

- The displayed information is repeatedly refreshed, so you cannot find the required information.
- The system traverses and retrieves information for a long time, and does not respond to any request.

Example

# Display all dynamic MAC address entries.

```
<HUAWEI> display mac-address dynamic
-------------------------------------------------------------------------------
MAC Address    VLAN/VSI/BD             Learned-From     Type
-------------------------------------------------------------------------------
00e0-fc22-0033  100/-/-                GE0/0/1          dynamic
00e0-fc00-0001  200/-/-                GE0/0/2          dynamic

-------------------------------------------------------------------------------
Total items displayed = 2
```

# Display all dynamic MAC address entries in VLAN 9.

```
<HUAWEI> display mac-address dynamic  vlan 9
-------------------------------------------------------------------------------
MAC Address   VLAN/VSI/BD                Learned-From      Type
-------------------------------------------------------------------------------
00e0-fc07-0122   9/-/-                   GE0/0/1           dynamic
00e0-fc07-0106   9/-/-                   GE0/0/1           dynamic
00e0-fc07-0114   9/-/-                   GE0/0/1           dynamic

-------------------------------------------------------------------------------
Total items displayed = 3
```

# Display detailed information about all dynamic MAC address entries in VLAN 9.

```
<HUAWEI> display mac-address dynamic vlan 9 verbose
-------------------------------------------------------------------------------
MAC Address : 00e0-fc07-0117          VLAN: 9
Learned-From: GE0/0/1               Type: dynamic

MAC Address : 00e0-fc07-0133          VLAN: 9
Learned-From: GE0/0/1               Type: dynamic

MAC Address : 00e0-fc07-0121          VLAN: 9
Learned-From: GE0/0/1               Type: dynamic

-------------------------------------------------------------------------------
Total items  displayed = 3
```

Table 5-5 Description of the display mac-address dynamic command output

Item	Description
MAC Address	Destination MAC address in a dynamic MAC address entry.
VLAN/VSI/BD	ID of the VLAN, or name of the VSI, or ID of the BD that a MAC address belongs to.
Learned-From	Interface that learns a MAC address.
Type	Type of a MAC address entry. dynamic: indicates a MAC address entry learned by the switch, which will be aged out when the aging time expires.

5.1.7 display mac-address flapping

Function

The **display mac-address flapping** command displays the configuration of MAC address flapping detection.

Format

display mac-address flapping

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

After MAC address flapping detection is configured, you can run the **display mac-address flapping** command to check the configuration.

The command output includes the following information:

- Whether MAC address flapping detection is configured.
- Aging time of flapping MAC addresses.
- Delay time before the interface joins a VLAN again after it is removed from the VLAN.

- VLAN that does not require MAC address flapping detection.
- List of VLANs of three security levels defined for MAC address flapping detection

Example

# Display the configuration of MAC address flapping detection.

```
<HUAWEI> display mac-address flapping
MAC address Flapping Configurations :
----------------------------------------------------------------------------
  Flapping detection          : Enable
  Aging time(sec)             : 300
  Quit VLAN Recover time(min) : 10
  Exclude VLAN list           : -
  Low level VLAN list         : -
  Middle level VLAN list      : 1 to 4094
  High level VLAN list        : -
----------------------------------------------------------------------------
```

Table 5-6 Description of the display mac-address flapping command output

Item	Description
Flapping detection	MAC address flapping detection status: ● Enable: MAC address flapping detection is enabled. ● Disable: MAC address flapping detection is disabled. To specify the parameter, run the **mac-address flapping detection** command.
Aging time(sec)	Aging time of flapping MAC addresses. To specify the parameter, run the **mac-address flapping aging-time** command.
Quit VLAN Recover time(min)	Delay time before the interface joins a VLAN again after it is removed from the VLAN. To specify the parameter, run the **mac-address flapping quit-vlan recover-time** command. The default value is 10. If the value is 0, the interface cannot join a VLAN again after it is removed from the VLAN.
Exclude VLAN list	VLAN that does not require MAC address flapping detection. To specify the parameter, run the **mac-address flapping detection exclude vlan** command. If such a VLAN is specified, the VLAN ID is displayed. If the VLAN is not specified, this field is displayed as -.
Low level VLAN list	List of VLANs of low security level defined for MAC address flapping detection. To specify the parameter, run the **mac-address flapping detection vlan security-level** command.

Item	Description
Middle level VLAN list	List of VLANs of middle security level defined for MAC address flapping detection. To specify the parameter, run the **mac-address flapping detection vlan security-level** command.
High level VLAN list	List of VLANs of high security level defined for MAC address flapping detection. To specify the parameter, run the **mac-address flapping detection vlan security-level** command.

5.1.8 display mac-address flapping record

Function

The **display mac-address flapping record** command displays MAC address flapping records.

Format

display mac-address flapping record [**slot** *slot-id*] [**begin** *YYYY/MM/DD HH:MM:SS*]

Parameters

Parameter	Description	Value
slot *slot-id*	Specifies a slot ID.	The value depends on the device configuration.
begin *YYYY/MM/DD HH:MM:SS*	Displays MAC address flapping records generated from the specified time to the current time. *YYYY/MM/DD* indicates year/month/date. *HH:MM:SS* indicates hour:minute:second.	• *YYYY/MM/DD* ranges from 2000/01/01 to 2099/12/31. • *HH:MM:SS* ranges from 00:00:00 to 23:59:59.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

The **display mac-address flapping record** command output helps locate the position where MAC address flapping occurs.

Precautions

The command output is displayed only when MAC address flapping has occurred.

Example

# Display all MAC address flapping records.

```
<HUAWEI> display mac-address flapping record
 S  : start time
 E  : end time
(Q) : quit VLAN
(D) : error down
-------------------------------------------------------------------------------
Move-Time             VLAN  MAC-Address   Original-Port Move-Ports   MoveNum
-------------------------------------------------------------------------------
S:2011-08-31 17:22:36 300  00e0-fc12-3456 Eth-Trunk1   Eth-Trunk2   81
E:2011-08-31 17:22:44

-------------------------------------------------------------------------------
Total items on slot 0: 1
```

# Display MAC address flapping records generated from 2012/06/04 09:00:00 to the current time.

```
<HUAWEI> display mac-address flapping record begin 2012/06/04 09:00:00
 S  : start time
 E  : end time
(Q) : quit VLAN
(D) : error down
-------------------------------------------------------------------------------
Move-Time                VLAN MAC-Address   Original-Port Move-Ports   MoveNum
-------------------------------------------------------------------------------
S:2012-06-04 17:22:38 300  00e0-fc12-3456 Eth-Trunk2   Eth-Trunk1   5
E:2012-06-04 17:22:42

-------------------------------------------------------------------------------
Total items on slot 0: 1
```

Table 5-7 Description of the display mac-address flapping record command output

Item	Description
Move-Time	Start time and end time MAC address flapping occurs. If the DST is configured, the DST plus the flapping start time or end time is displayed, for example: StartTime: 2012-02-02 15:54:10 DST.
VLAN	VLAN where MAC address flapping occurs.

Item	Description
MAC-Address	Flapping MAC address. **NOTE** Only one MAC address that flaps is displayed for the same VLAN on the same device.
Original-Port	Port that learns the MAC address first.
Move-Ports	Ports that learn the MAC address later.
MoveNum	Number of times the MAC address has flapped. The maximum value is 65535. When the number of times the MAC address has flapped exceeds 65535, the MoveNum field still displays 65535.

5.1.9 display mac-address hash-conflict record

Function

The **display mac-address hash-conflict record** command displays records of MAC address hash conflicts.

Format

display mac-address hash-conflict record [**slot** *slot-id*]

Parameters

Parameter	Description	Value
slot *slot-id*	Specifies a slot ID.	Set this parameter based on the actual device configuration.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Application Scenarios

When MAC address hash conflicts occur on the network, you can run this command to view conflict records.

Precautions

A maximum of 100 MAC address hash conflict records can be displayed. The latest 100 records are retained in time sequence.

Example

# Display MAC address hash conflict records of slot 0.

```
<HUAWEI> display mac-address hash-conflict record slot 0
-------------------------------------------------------------------------------
 Time                   MAC Address         VLAN/VSI/BD    InterfaceName
-------------------------------------------------------------------------------
 2019-11-21 09:25:38     00e0-fc00-0004      4011/-/-       XGE0/0/5
 2019-11-21 09:25:38     00e0-fc00-0009      4011/-/-       XGE0/0/5
 2019-11-21 09:26:40     00e0-fc00-0003      -/-/10        XGE0/0/5
 2019-11-21 09:26:40     00e0-fc00-0008      -/-/10        XGE0/0/5
 2019-11-21 09:26:40     00e0-fc00-0001      -/-/10        XGE0/0/5
-------------------------------------------------------------------------------
Total items on slot 0: 5
```

Table 5-8 Description of the **display mac-address hash-conflict record** command output

Item	Description
Time	Time when a MAC address hash conflict occurs.
MAC Address	MAC address.
VLAN/VSI/BD	ID of the VLAN or name of the VSIor ID of the BD to which the MAC address belongs.
InterfaceName	Interface name.

5.1.10 display mac-address hash-mode

Function

The **display mac-address hash-mode** command displays the running hash mode and configured hash mode on the device.

NOTE

The S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735-S-I, S5735S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S do not support this command.

Format

display mac-address hash-mode

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

After a hash mode is configured, you can run the **display mac-address hash-mode** command to check the configuration.

Precautions

After the hash algorithm is changed, restart the device for the configuration to take effect.

Example

# Display the running hash mode and configured hash mode on the device.

```
<HUAWEI> display mac-address hash-mode
  MAC address hash mode status:
-------------------------------------------
 Slot       CurMode          CfgMode
-------------------------------------------
 0         crc16-lower     crc32-lower
-------------------------------------------
```

Table 5-9 Description of the display mac-address hash-mode command output

Item	Description
Slot	Slot ID.
CurMode	Running hash mode on the device. After changing the hash algorithm and saving the configuration, restart the device for the configuration to take effect.
CfgMode	Configured hash mode on the device. To specify the parameter, run the **mac-address hash-mode** command.

5.1.11 display mac-address mux

Function

The **display mac-address mux** command displays MUX MAC address entries.

Format

display mac-address mux [**vlan** *vlan-id* | *interface-type interface-number*] * [**verbose**]

Parameters

Parameter	Description	Value
vlan *vlan-id*	Displays MUX MAC address entries in a specified VLAN.	The value is an integer that ranges from 1 to 4094.
interface-type interface-number	Displays MUX MAC address entries with a specified outbound interface. ● *interface-type* specifies the type of the outbound interface. ● *interface-number* specifies the number of the outbound interface.	-
verbose	Displays detailed information about MUX MAC address entries. If this parameter is not specified, brief information about MUX MAC address entries is displayed.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

The MUX VLAN function isolates Layer 2 traffic between interfaces in a VLAN. A MUX MAC address entry is learned by a MUX VLAN enabled interface. The learned MUX MAC address entries are deleted after the switch restarts.

After configuring the MUX VLAN function, you can run the **display mac-address mux** command to check whether the learned MUX MAC address entries are correct.

Follow-up Procedure

If the displayed MUX MAC address entries are invalid, run the **undo mac-address** command to delete MUX MAC address entries.

Precautions

If you run the **display mac-address mux** command without parameters, all MUX MAC address entries are displayed.

If the MAC address table does not contain any MUX MAC address entry, no information is displayed.

When the switch has a large number of MUX MAC address entries, it is recommended that you specify parameters in the command to filter the output information. Otherwise, the following problems may occur due to excessive output information:

- The displayed information is repeatedly refreshed, so you cannot find the required information.
- The system traverses and retrieves information for a long time, and does not respond to any request.

Example

# Display all MUX MAC address entries.

```
<HUAWEI> display mac-address mux
-------------------------------------------------------------------------------
MAC Address          VLAN/VSI/BD                 Learned-From        Type
-------------------------------------------------------------------------------
00e0-fc12-3456       100/-/-                     GE0/0/2             mux

-------------------------------------------------------------------------------
Total items displayed = 1
```

# Display detailed information about all MUX MAC address entries in VLAN 10.

```
<HUAWEI> display mac-address mux vlan 10 verbose
-------------------------------------------------------------------------------
MAC Address : 00e0-fc12-3457            VLAN : 10
Learned-From: GE0/0/2                   Type : mux

-------------------------------------------------------------------------------
Total items displayed = 1
```

Table 5-10 Description of the display mac-address mux command output

Item	Description
MAC Address	Destination MAC address in a MUX MAC address entry.
VLAN/VSI/BD	ID of the VLAN, or name of the virtual switch instance (VSI), or ID of the BD that a MAC address belongs to.
Learned-From	Interface that learns a MAC address.

Item	Description
Type	Type of a MAC address entry. mux: indicates a MAC address entry learned by a MUX VLAN enabled interface.

5.1.12 display mac-address oam

Function

The **display mac-address oam** command displays information about MAC address entries of the OAM type.

NOTE

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

Format

display mac-address oam

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

VPLS data forwarding depends on MAC address learning. Data packets in a VPLS domain can be correctly forwarded only when the MAC addresses of the data packets are correctly learned by PEs.

VPLS MAC diagnostic tools can be used to check whether MAC address learning works properly on the devices in a VPLS domain. VPLS MAC diagnostic tools include MAC populate and MAC purge.

- MAC populate is used to check whether MAC addresses can be learned by devices in a VSI by populating an OAM MAC address into the VPLS domain.

  If the devices in a specified VSI in the VPLS domain have learned the populated MAC address, running the **display mac-address oam** command can display detailed information about the populated OAM MAC address.

- MAC purge is used to purge the populated OAM MAC address.

  If the learned OAM MAC address is purged on the device, running the **display mac-address oam** command can show that the learned OAM MAC address has been purged.

Prerequisites

- Configuring the diagnosis of the OAM MAC address learning capacity is completed before you check detailed information about the populated OAM MAC address.
- Purging the OAM MAC address learned by the devices on the VPLS network is completed before you check whether the OAM MAC has been purged.

Example

# Display MAC address entries of the OAM type in the MAC address table.

```
<HUAWEI> display mac-address oam
-------------------------------------------------------------------------------
MAC Address     VLAN/VSI/BD             Learned-From          Type
-------------------------------------------------------------------------------
00e0-fc00-0010  -/vsi1/-             GigabitEthernet0/0/1  OAM-PU
00e0-fc00-0020  -/vsi1/-             GigabitEthernet0/0/1  OAM-PO

-------------------------------------------------------------------------------
Total items displayed = 2
```

Table 5-11 Description of the **display mac-address oam** command output

Item	Description
MAC Address	Indicates the MAC address of the OAM type.
VLAN/VSI/BD	● VLAN: the value is always displayed as "-". ● VSI: indicates the VSI to which the MAC addresses of the OAM type belong. ● BD: the value is always displayed as "-".
Learned-From	Indicates an interface on which the MAC addresses of the OAM type are configured.
Type	Indicates the OAM type of the MAC address. ● **OAM-PU**: indicates the OAM MAC address entry that is used to discard data frames containing a specified destination MAC address, configured by using the **mac-purge** command. ● **OAM-PO**: indicates the OAM MAC address entry that is used to test whether the function of learning dynamic MAC addresses is normal on the device. The entry is displayed as the dynamic MAC address on the device. In addition, the entry, the same as a common dynamic MAC address, supports VPLS forwarding, configured by using the **mac-populate** command.

5.1.13 display mac-address static

Function

The **display mac-address static** command displays static MAC address entries.

Format

display mac-address static [**vsi** *vsi-name*] [**verbose**]

display mac-address static [**vlan** *vlan-id* | *interface-type interface-number*] * [**verbose**]

Parameters

Parameter	Description	Value
vlan *vlan-id*	Displays static MAC address entries in a specified VLAN.	The value is an integer that ranges from 1 to 4094.
vsi *vsi-name*	Displays static MAC address entries in a specified VSI. *vsi-name* specifies the name of a VSI. **NOTE** Only the S5731-H, S5731S-H, S5732-H, S5731-S, S5731S-S, S6730-S, S6730S-S, S6735-S, S6720-EI, S6720S-EI, S6730S-H, and S6730-H support this parameter.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
interface-type interface-number	Displays the static MAC address entries on a specified interface.	-
verbose	Displays detailed information about static MAC address entries.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

The MAC address table of the switch stores MAC addresses of other devices. When forwarding an Ethernet frame, the switch searches the MAC address table for the outbound interface according to the destination MAC address and VLAN ID in the Ethernet frame.

The MAC address table contains the following MAC address entries:

- Static MAC entries that are manually configured and will not be aged out.
- Blackhole MAC address entries that are used to discard packets with the specified source MAC addresses or destination MAC addresses. Blackhole MAC address entries are manually configured and will not be aged out.
- Dynamic MAC address entries that are learned by the switch and will be aged out when the aging time expires.

To improve network security, configure static MAC address entries to ensure that packets destined for specified MAC addresses are forwarded by the specified interfaces. This prevents attack packets with bogus MAC addresses and guarantees communication between the switch and the upstream device or server. After configuring static MAC address entries, you can run the **display mac-address static** command to verify the configuration.

Follow-up Procedure

If any static MAC address entry is incorrect, run the **undo mac-address** command to delete it.

Precautions

If you run the **display mac-address static** command without parameters, all static MAC address entries are displayed.

If the MAC address table does not contain any static MAC address entry, no information is displayed.

Example

# Display all static MAC address entries.

```
<HUAWEI> display mac-address static
-------------------------------------------------------------------------------
MAC Address          VLAN/VSI/BD                Learned-From        Type
-------------------------------------------------------------------------------
00e0-fc00-0033       100/-/-                    GE0/0/1             static
00e0-fc00-0001       200/-/-                    GE0/0/2             static

-------------------------------------------------------------------------------
Total items displayed = 2
```

# Display detailed information about all static MAC address entries in VLAN 10.

```
<HUAWEI> display mac-address static vlan 10 verbose
-------------------------------------------------------------------------------
MAC Address : 00e0-fc00-0001           VLAN : 10
Learned-From: GE0/0/1                  Type : static

-------------------------------------------------------------------------------
Total items displayed = 1
```

Table 5-12 Description of the display mac-address static command output

Item	Description
MAC Address	Destination MAC address in a static MAC address entry.
VLAN/VSI/BD	ID of the VLAN, or name of the VSI, or ID of the BD that a MAC address belongs to.
Learned-From	Interface that learns a MAC address.
Type	Type of a MAC address entry. static: indicates a static MAC address entry, which is manually configured and will not be aged out, configured by using the **mac-address static vlan**, **mac-address static vlanif**, **mac-address static vsi**, **mac-address static bridge-domain**, or **mac-address static bridge-domain vni** command.

5.1.14 display mac-address summary

Function

The **display mac-address summary** command displays statistics on MAC address entries.

Format

display mac-address summary [**slot** *slot-id*]

Parameters

Parameter	Description	Value
slot *slot-id*	Displays statistics on MAC address entries on a specified card.	The value is an integer and must be the slot ID of a running card.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

The MAC address table of the device stores MAC addresses of other devices. When forwarding an Ethernet frame, the switch searches the MAC address table for the outbound interface according to the destination MAC address and VLAN ID in the Ethernet frame.

When the switch has many MAC address entries of different types.

Precautions

- If **slot** *slot-id* is specified, this command displays statistics on MAC address entries on the specified card. If this parameter is not specified, this command displays statistics on MAC address entries on all cards.
- If no static or blackhole MAC addresses are configured on the device, statistics about the two types of MAC address entries are 0.
- Blackhole MAC address entries fall into global and VLAN- or VSI-based blackhole MAC address entries. Global blackhole MAC address entries are configured using the **mac-address blackhole** command with only a MAC address specified. They do not occupy the MAC address table space.
- If MAC address learning is disabled on the device, statistics about dynamic MAC address entries are 0.

  Using the **undo mac-address learning disable** command in the Ethernet interface view can enable MAC address learning.

Example

# View statistics on all MAC address entries in the system.

```
<HUAWEI> display mac-address summary
Summary information of slot 0:
-----------------------------------
Static        :              2
Blackhole     :              0
Dyn-Local     :              0
Dyn-Remote    :              0
Dyn-Trunk     :              0
Sticky        :              0
Security      :              0
Sec-config    :              0
Authen        :              0
Guest         :              0
Mux           :              0
Snooping      :              0
Pre-Mac       :              0
Evpn          :              0
Sticky-config :              0
In-used       :              5
Capacity      :              32768
-----------------------------------
```

Table 5-13 Description of the **display mac-address summary** command output

Item	Description
Static	Number of static MAC address entries.
Blackhole	Number of blackhole MAC address entries.
Dyn-Local	Number of MAC address entries learned by the local card.

Item	Description
Dyn-Remote	Number of MAC address entries synchronized from other cards.
Dyn-Trunk	Total number of MAC address entries learned by all trunk interfaces.
Sticky	Number of sticky MAC address entries.
Security	Number of secure dynamic MAC address entries.
Sec-config	Number of secure static MAC address entries.
Authen	Number of MAC address entries corresponding to authentication users.
Guest	Number of MAC address entries learned by interfaces in the guest VLAN.
Mux	Number of MAC address entries learned by interfaces enabled with the MUX VLAN function.
Snooping	Number of Snooping MAC address entries.
Pre-Mac	Number of Pre-authen MAC address entries.
Evpn	Number of EVPN MAC address entries.
Sticky-config	Number of MAC address entries of the sticky-config type.
In-used	Total number of existing MAC address entries. **NOTE** Global blackhole MAC address entries do not occupy the MAC address table space. If these MAC address entries are configured on the device, the In-used value may be greater than the Capacity value.
Capacity	Capacity of the MAC address table. The actual value varies according to device models.

5.1.15 display mac-address total-number

Function

The **display mac-address total-number** command displays the number of MAC address entries of a specified type.

Format

display mac-address total-number [**slot** *slot-id*]

display mac-address total-number [**vsi** *vsi-name*]

display mac-address total-number [**vlan** *vlan-id* | *interface-type interface-number*] *

display mac-address total-number vlan all

display mac-address total-number { **mux** | **security** | **sticky** | **sec-config** | **snooping** | **pre-authen** | **authen** | **sticky-config** } [**vlan** *vlan-id* | *interface-type interface-number*] *

display mac-address total-number blackhole [**vlan** *vlan-id* | **vsi** *vsi-name*]

display mac-address total-number dynamic [**slot** *slot-id*] [**vlan** *vlan-id* | *interface-type interface-number*] *

display mac-address total-number dynamic [**slot** *slot-id*] [**vsi** *vsi-name*]

display mac-address total-number static [**vlan** *vlan-id* | *interface-type interface-number*] *

display mac-address total-number static vsi *vsi-name*

Parameters

Parameter	Description	Value
slot *slot-id*	Displays the number of MAC address entries on a specified card.	The value is an integer and must be the slot ID of a running card.
mux	Displays the number of MUX MAC address entries.	-
dynamic	Displays the number of dynamic MAC address entries.	-
security	Displays the number of secure dynamic MAC address entries.	-
sec-config	Displays the number of secure static MAC address entries.	-
snooping	Displays the number of static MAC address entries generated based on the dynamic DHCP snooping binding table.	-
pre-authen	Displays the number of static MAC address entries corresponding to a user in pre-connection state after NAC authentication is enabled.	-

Parameter	Description	Value
authen	Displays the number of static MAC address entries that is generated after a user passes NAC authentication.	-
sticky-config	Displays the number of MAC address entries of the sticky-config type.	-
sticky	Displays the number of sticky MAC address entries.	-
blackhole	Displays the number of blackhole MAC address entries.	-
static	Displays the number of static MAC address entries.	-
vlan *vlan-id*	Displays the number of MAC address entries in a specified VLAN.	The value is an integer that ranges from 1 to 4094.
vlan all	Displays the number of MAC address entries in all VLANs.	-
interface-type interface-number	Displays the number of MAC address entries learned by a specified interface.	-
vsi *vsi-name*	Displays the number of MAC address entries in a specified VSI. **NOTE** Only the S5731-H, S5731S-H, S5732-H, S5731-S, S5731S-S, S6730-S, S6730S-S, S6735-S, S6720-EI, S6720S-EI, S6730S-H, and S6730-H support this parameter.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

The MAC address table of the switch stores MAC addresses of other devices. When forwarding an Ethernet frame, the switch searches the MAC address table for the outbound interface according to the destination MAC address and VLAN ID in the Ethernet frame.

When the switch has many MAC address entries of different types, you can use the **display mac-address total-number** command to view statistics on MAC address entries of a specified type.

Precautions

If no parameter is specified, the total number of MAC address entries in the system is displayed.

If no interface is specified in the **display mac-address total-number** command, the total number of MAC address entries learned by all interfaces is displayed.

If an interface is specified in the **display mac-address total-number** command, the total number of MAC address entries in the VLAN where the interface resides is displayed.

If no VLAN is specified in the **display mac-address total-number** command, the total number of MAC address entries in all VLANs is displayed.

Example

# Display the number of dynamic MAC address entries.

```
<HUAWEI> display mac-address total-number dynamic
Total number of MAC address : 20
```

Table 5-14 Description of the **display mac-address total-number** command output

Item	Description
Total number of MAC address	Total number of MAC address entries in the system.

5.1.16 display mac-limit

Function

The **display mac-limit** command displays the rules that limit the number of learned MAC addresses.

Format

display mac-limit [*interface-type interface-number* | **vlan** *vlan-id* | **vsi** *vsi-name*]

Parameters

Parameter	Description	Value
interface-type interface-number	Displays the MAC address limiting rule on a specified interface. ● *interface-type* specifies the type of the interface. ● *interface-number* specifies the number of the interface.	-
vlan *vlan-id*	Displays the MAC address limiting rules in a specified VLAN.	The value is an integer that ranges from 1 to 4094.
vsi *vsi-name*	Displays the MAC address limiting rules in a specified VSI. *vsi-name* specifies the name of a VSI. **NOTE** Only the S5731-H, S5731S-H, S5732-H, S5731-S, S5731S-S, S6730-S, S6730S-S, S6735-S, S6720-EI, S6720S-EI, S6730S-H, and S6730-H support this parameter.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

To check whether MAC address limiting rules are configured correctly, run the **display mac-limit** command. If a rule is incorrect, run the **mac-limit** command to modify the rule or run the **undo mac-limit all** command to delete it.

Precautions

If no parameter is specified, MAC address learning limit rules of all interfaces, VSIs, and VLANs are displayed.

Example

# Display the MAC address limiting rule on GigabitEthernet0/0/1.

```
<HUAWEI> display mac-limit GigabitEthernet 0/0/1
GigabitEthernet0/0/1 MAC limit:
  Maximum MAC count 1000, used count 0
  Action: forward, Alarm: enable
```

# Display all the MAC address limiting rules.

```
<HUAWEI> display mac-limit
MAC Limit is enabled
Total MAC Limit rule count : 1

PORT            VLAN/VSI/SI       SLOT Maximum Rate(ms) Action  Alarm
-------------------------------------------------------------------------------
GE0/0/1          -                -    100     -        forward enable
```

Table 5-15 Description of the display mac-limit command output

Item	Description
GigabitEthernet 0/0/1 MAC limit:	MAC address limiting rule for the interface. To specify the parameters, run the **mac-limit** command.
Maximum MAC count	Maximum number of MAC addresses that can be learned.
used count	Number of MAC addresses that have been learned.
Total MAC Limit rule count	Number of configured MAC address limiting rules.
PORT	Name of an interface.
VLAN/VSI/SI	ID of a VLAN VSI name, or service instance (SI) name.
SLOT	Slot ID of the card where a MAC address limiting rule is configured.
Maximum	Maximum number of MAC addresses that can be learned. To set the maximum number of MAC addresses, run the **mac-limit** command.
Rate(ms)	Indicates the interval at which MAC addresses are learned.
Action	Action performed on packets when the number of learned MAC addresses exceeds the maximum. The value **forward** indicates that packets are forwarded with new source MAC addresses.

Item	Description
Alarm	Whether an alarm is generated when the number of learned MAC addresses exceeds the maximum. ● enable: indicates that an alarm is generated. ● disable: indicates that an alarm is not generated.

5.1.17 drop illegal-mac alarm

Function

The **drop illegal-mac alarm** command configures the switch to send a trap to the network management system (NMS) when receiving a packet with an all-0 MAC address.

The **undo drop illegal-mac alarm** command deletes the configuration.

By default, the switch does not send a trap to the NMS when receiving a packet with an all-0 MAC address.

Format

drop illegal-mac alarm

undo drop illegal-mac alarm

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Some legacy computers or network devices may send packets with an all-0 source or destination MAC address when their network adapters fail. The **drop illegal-mac alarm** command configures the switch to send a trap to the NMS when receiving a packet with an all-0 MAC address. You can locate the faulty network adapter according to the trap message.

Precautions

If the alarm function is disabled on the switch, the NMS cannot receive any trap message.

After you run the **drop illegal-mac alarm** command, the switch sends a trap only once after receiving packets with an all-0 MAC address. To configure the switch to send traps continuously, run the **drop illegal-mac alarm** command repeatedly.

This command and IPv6 over IPv4 cannot be configured simultaneously on the S6720S-S, S5735S-H, S5736-S, and S5720I-SI.

Example

# Configure the switch to send a trap to the NMS when receiving a packet with an all-0 MAC address.

```
<HUAWEI> system-view
[HUAWEI] drop illegal-mac alarm
```

5.1.18 drop illegal-mac enable

Function

The **drop illegal-mac enable** command enables the switch to discard packets with an all-0 invalid MAC address.

The **undo drop illegal-mac enable** command disables the switch from discarding packets with an all-0 invalid MAC address.

By default, the switch does not discard packets with an all-0 MAC address.

Format

drop illegal-mac enable

undo drop illegal-mac enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Some legacy computers or network devices may send packets with an all-0 source or destination MAC address when their network adapters fail. You can run the **drop illegal-mac enable** command to configure the switch to discard such packets. After receiving the packets with an all-0 source or destination MAC address, the switch discards the packets.

This command reduces incorrect MAC address entries on the device.

Precautions

If the alarm function is disabled on the device, the network management system cannot receive any alarm message.

Example

# Configure the switch to discard packets with an all-0 invalid MAC address.

```
<HUAWEI> system-view
[HUAWEI] drop illegal-mac enable
```

5.1.19 mac-address aging-time

Function

The **mac-address aging-time** command sets the aging time of dynamic MAC address entries.

The **undo mac-address aging-time** command restores the default aging time of dynamic MAC address entries.

By default, the aging time of dynamic MAC address entries is 300 seconds.

Format

mac-address aging-time *aging-time*

undo mac-address aging-time

Parameters

Parameter	Description	Value
aging-time	Specifies the aging time of dynamic MAC address entries.	The value is 0 or an integer that ranges from 10 to 1000000, in seconds. The default value is 300. The value 0 indicates that dynamic MAC address entries will not be aged out.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The network topology changes frequently, and the switch will learn many MAC addresses. You can run the **mac-address aging-time** command to set a proper aging time for dynamic MAC address entries so that aged MAC address entries are deleted from the MAC address table. This reduces MAC address entries in the MAC address table.

The system starts an aging timer for each dynamic MAC address entry. If a dynamic MAC address entry is not updated within a certain period (twice the aging time), the entry is deleted. If the entry is updated within this period, the aging timer of this entry is reset. If the aging time is short, the switch is sensitive to network changes.

When setting the aging time of dynamic MAC address entries, follow these rules:

- Set a longer aging time on a stable network and a shorter aging time on an unstable network.
- The capacity of the MAC address table on a low-end device is small; therefore, set a relatively short aging time on low end devices to save the MAC address table space.

Precautions

- Dynamic MAC address entries are lost after system restart. Static MAC address entries and blackhole MAC address entries are not aged or lost.
- If the aging time is 0, dynamic MAC address entries will not be aged out. In this case, MAC address entries increase sharply and the MAC address table will be full quickly.
- If you run the **mac-address aging-time** command multiple times, only the latest configuration takes effect.
- If a MAC address entry is always matched to direct traffic forwarding, this entry will not be aged out.

Example

# Set the aging time of dynamic MAC address entries to 500 seconds.

```
<HUAWEI> system-view
[HUAWEI] mac-address aging-time 500
```

5.1.20 mac-address blackhole

Function

The **mac-address blackhole** command configures a blackhole MAC address entry.

The **undo mac-address blackhole** command deletes a blackhole MAC address entry.

By default, no blackhole MAC address entry is configured.

Format

mac-address blackhole *mac-address* [**vlan** *vlan-id* | **vsi** *vsi-name*]

undo mac-address blackhole [*mac-address*] [**vlan** *vlan-id* | **vsi** *vsi-name*]

Parameters

Parameter	Description	Value
mac-address	Specifies the MAC address in a blackhole MAC address entry.	The value is in H-H-H format. An H is a hexadecimal number of 1 to 4 digits. The MAC address cannot be FFFF-FFFF-FFFF, 0000-0000-0000, or a multicast MAC address.
vlan *vlan-id*	Specifies the VLAN ID in a blackhole MAC address entry.	The value is an integer that ranges from 1 to 4094.
vsi *vsi-name*	Specifies the name of a VSI in a blackhole MAC address entry. The VSI must have been created. **NOTE** Only the S5731-H, S5731S-H, S5732-H, S5731-S, S5731S-S, S6730-S, S6730S-S, S6735-S, S6720-EI, S6720S-EI, S6730S-H, and S6730-H support this parameter.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To protect a device or network against MAC address attacks, configure MAC addresses of untrusted users as blackhole MAC addresses. The device then directly discards the received packets of which the source or destination MAC addresses match the blackhole MAC address entries.

Prerequisites

The network administrator is familiar with the MAC addresses of all devices on the network. If the MAC address of an authorized user is configured as a blackhole MAC address, the user's communications will be interrupted.

Configuration Impact

If the source or destination MAC address of a packet matches a blackhole MAC address entry, the packet will be discarded. After being configured and saved, blackhole MAC address entries are not lost after the system reset.

Precautions

- Blackhole MAC address entries can be added or deleted, and they will not be aged.

  Unlike configuring a static MAC entry, you can configure a blackhole MAC entry without specifying an outbound interface.
- If the specified VLAN is the control VLAN for Rapid Ring Protection Protocol (RRPP), the **mac-address blackhole** command cannot be run.
- Blackhole MAC address entries fall into global and VLAN- or VSI-based blackhole MAC address entries. Global blackhole MAC address entries are configured using the **mac-address blackhole** command with only a MAC address specified. They do not occupy the MAC address table space.
- If you configure a VLAN- or VSI-based blackhole MAC address entry when the MAC address table is full, the device processes the MAC address entry as follows:
  - If a dynamic MAC address entry with the same MAC address and VLAN ID or VSI name exists in the MAC address table, the blackhole MAC address entry replaces the dynamic MAC address entry.
  - If no dynamic MAC address entry with the same MAC address exists in the MAC address table, the system deletes one dynamic MAC address entry and adds the blackhole MAC address entry to the MAC address table.
- You can run the **mac-address blackhole** command multiple times to configure multiple blackhole MAC address entries.
- For the SS1720GW-E, S1720GWR-E, S5720I-SI, S5720-LI, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5720S-LI, S5735-S, S500, S5735S-S, S5735-S-I, S5735S-H, S5736-S, or S6720S-S switch, if both traffic policy-based redirection action and VLAN-based blackhole MAC address are configured, the switch will not discard the packet if its source or destination MAC address is a blackhole MAC address and the packet matches the redirection policy. For other device models, the switch discards the packet.
- An existing MAC address entry whose MAC address type is **authen**, **pre-authen**, **security**, **sticky**, **static**, or **static-con mac** cannot be configured as a blackhole MAC address entry.
- In a Layer 3 forwarding scenario, if a device has learned an ARP entry and the MAC address in the ARP entry is configured as a VLAN-based blackhole MAC address, the device discards packets with this source MAC address only after the ARP entry ages out.

Example

# Add a blackhole MAC address entry to the MAC address table. In the blackhole MAC address entry, the MAC address is 00e0-fc04-0004 and the VLAN ID is VLAN 5.

```
<HUAWEI> system-view
[HUAWEI] vlan 5
```

```
[HUAWEI-vlan5] quit
[HUAWEI] mac-address blackhole 00e0-fc04-0004 vlan 5
```

# Configure a global blackhole MAC address entry in which the MAC address is 00e0-fc05-0005.

```
<HUAWEI> system-view
[HUAWEI] mac-address blackhole 00e0-fc05-0005
```

# Add a blackhole MAC address entry in which the MAC address is 00e0-fc33-4455 to VSI **a2**. The device directly discards the received frame in which the source or destination MAC address is 00e0-fc33-4455 and the VSI name is **a2**.

```
<HUAWEI> system-view
[HUAWEI] mac-address blackhole 00e0-fc33-4455 vsi a2
```

5.1.21 mac-address destination hit aging enable

Function

The **mac-address destination hit aging enable** command configures the device to age MAC address entries no matter whether the entries match destination MAC addresses of packets.

The **undo mac-address destination hit aging enable** command restores the default configuration.

By default, if MAC address entries match destination MAC addresses of packets, the system recalculates the aging time.

NOTE

S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735-S-I, and S5735S-S do not support this command.

Format

mac-address destination hit aging enable

undo mac-address destination hit aging enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When a user uses one-way services such as the video on demand service, packets are transmitted unidirectionally from the server to the user terminal. When the user terminal is shut down, the server still sends packets. Therefore, the dynamic MAC address entry with the destination MAC address of the packets remains in the MAC address table.

To delete MAC address entries matching one-way service packets after user terminals are shut down, run the **mac-address destination hit aging enable** command to enable the device to age dynamic MAC address entries matching dynamic MAC addresses of received packets.

Configuration Impact

This command is used only when one-way services are deployed on a network.

Precautions

This command only free up space in the MAC address table but cannot save system resources. If the device cannot find the matching entry in the MAC address table, it broadcasts the packets.

Example

# Configure the device to age MAC address entries no matter whether the entries match destination MAC addresses of packets.

```
<HUAWEI> system-view
[HUAWEI] mac-address destination hit aging enable
```

5.1.22 mac-address flapping action

Function

The **mac-address flapping action** command configures the action to perform on an interface when MAC address flapping is detected on the interface.

The **undo mac-address flapping action** command deletes the action.

By default, the system does not perform any action when detecting MAC address flapping on an interface.

Format

mac-address flapping action { **error-down** | **quit-vlan** }

undo mac-address flapping action { **error-down** | **quit-vlan** }

Parameters

Parameter	Description	Value
error-down	Shuts down an interface when MAC address flapping is detected on the interface.	-

Parameter	Description	Value
quit-vlan	Removes an interface from the VLAN where MAC address flapping occurs when MAC address flapping is detected on the interface.	-

Views

Ethernet interface view, GE interface view, XGE interface view, 40GE interface view, 100GE interface view, MultiGE interface view, Eth-Trunk interface view, port group view, 25GE interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the switch connects to a user network that does not support loop prevention protocols, configure a loop prevention action for the switch to perform when detecting MAC address flapping. This reduces the impact of MAC address flapping on the user network.

When MAC address flapping occurs on an interface with a loop prevention action configured, the switch performs the configured action. When the action is set to error-down, the switch shuts down the interface. When the action is set to quit-VLAN, the switch removes the interface from the VLAN where MAC address flapping occurs. Only one interface can be shut down during one aging time configured by the **mac-address flapping aging-time** command.

Follow-up Procedure

- When the action is set to **error-down**, the interface cannot be automatically restored after it is shut down. You can only restore the interface by running the **shutdown** and **undo shutdown** commands or the **restart** command in the interface view.

  To enable the interface to go Up automatically, you must run the **error-down auto-recovery cause mac-address-flapping** command in the system view before the interface enters the error-down state. This command enables an interface in error-down state to go Up and sets a recovery time. The interface goes Up automatically after the time expires.
- If the action is set to **quit-vlan**, the interface can be automatically restored after a specified time period after it is removed from the VLAN. The default recovery time is 10 minutes. The recovery delay time can be set using the **mac-address flapping quit-vlan recover-time** *time-value* command in the system view.

Precautions

Do not run the **mac-address flapping action** command on uplink interfaces.

MAC address flapping detection can only detect loops on interfaces, but cannot obtain the entire network topology. If the user network connected to the switch supports loop prevention protocols, use the loop prevention protocols instead of MAC address flapping detection.

If you run the **mac-address flapping action** command multiple times in the same interface view, only the latest configuration takes effect.

Example

# Configure the switch to shut down GE0/0/1 when detecting MAC address flapping on the interface.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] mac-address flapping action error-down
Info: This command may shut down the interface after MAC address flapping is detected.
```

# Configure the switch to remove GE0/0/1 from the VLAN where MAC address flapping occurs.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] mac-address flapping action quit-vlan
```

5.1.23 mac-address flapping action priority

Function

The **mac-address flapping action priority** command sets the priority for the action against MAC address flapping on an interface.

The **undo mac-address flapping action priority** command restores the default configuration.

By default, the action against MAC address flapping on an interface is 127.

Format

mac-address flapping action priority *priority*

undo mac-address flapping action priority

Parameters

Parameter	Description	Value
priority	Specifies the priority of the action against MAC address flapping on an interface.	The value is an integer that ranges from 0 to 255. A larger value indicates a higher priority. The default value is 127.

Views

Ethernet interface view, GE interface view, XGE interface view, 40GE interface view, 100GE interface view, MultiGE interface view, Eth-Trunk interface view, port group view, 25GE interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the switch connects to a user network that does not support loop prevention protocols, configure a loop prevention action for the switch to perform when detecting MAC address flapping. This reduces the impact of MAC address flapping on the user network. The **mac-address flapping action priority** command sets the priority of the action.

When a MAC address flaps between two interfaces and both the interfaces have an action and priority configured, the switch performs the action (error-down or quit-VLAN) configured on the interface with lower priority. If the two interfaces have the same priority, the switch performs the action on the interface that learns the MAC address later. If the later interface has no action configured, the switch performs the action on the interface that learns the MAC address earlier.

NOTE

The switch compares priorities of the interfaces only when the interfaces have the same action configured. If one interface is configured with the error-down action, and the other is configured with the quit-VLAN action, the switch performs the actions on both interfaces even if their priorities are same.

Precautions

If you run the **mac-address flapping action priority** command multiple times in the same interface view, only the latest configuration takes effect.

Example

# Set the priority of the action against MAC address flapping on GE0/0/1 to 3.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] mac-address flapping action priority 3
```

5.1.24 mac-address flapping aging-time

Function

The **mac-address flapping aging-time** command sets the aging time of flapping MAC addresses.

The **undo mac-address flapping aging-time** command restores the default aging time of flapping MAC addresses.

By default, the aging time of flapping MAC addresses is 300 seconds.

Format

mac-address flapping aging-time *aging-time*

undo mac-address flapping aging-time

Parameters

Parameter	Description	Value
aging-time	Specifies the aging time of flapping MAC addresses.	The value is an integer that ranges from 60 to 900, in seconds.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Increasing the aging time of flapping MAC addresses will cause MAC address flapping again and increase the error-down time. To ensure that the system performs MAC address flapping detection in a timely manner, run the **mac-address flapping aging-time** command to shorten the aging time of flapping MAC addresses.

Precautions

If you run the **mac-address flapping aging-time** command multiple times, only the latest configuration takes effect.

Example

# Set the aging time of flapping MAC addresses to 500 seconds.

```
<HUAWEI> system-view
[HUAWEI] mac-address flapping aging-time 500
```

5.1.25 mac-address flapping detection

Function

The **mac-address flapping detection** command enables global MAC address flapping detection.

The **undo mac-address flapping detection** command disables global MAC address flapping detection.

By default, global MAC address flapping detection is enabled.

Format

mac-address flapping detection

undo mac-address flapping detection

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

MAC address flapping occurs when a MAC address is learned by two interfaces in the same VLAN. The MAC address entry learned later replaces the earlier one.

MAC address flapping occurs in the following situations:

- Network cables of switches are connected incorrectly or switches use incorrect configurations.
- Unauthorized users simulate MAC address of valid network devices to attack the network.

Global MAC address flapping detection enables the Switch to check all MAC addresses. When MAC address flapping occurs, the Switch sends a trap message to the NMS. You can locate the fault according to the trap message. You can also run the **display mac-address flapping record** command to view MAC address flapping records.

NOTE

On the S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735-S-I, and S5735S-S, it takes several seconds to eliminate MAC address flapping if a large number of MAC address flapping events occur on the network. During this period, the number of MAC address flapping records may increase even if MAC address flapping is eliminated.

Example

# Enable global MAC address flapping detection.

```
<HUAWEI> system-view
[HUAWEI] mac-address flapping detection
```

5.1.26 mac-address flapping detection exclude vlan

Function

The **mac-address flapping detection exclude vlan** command excludes a VLAN from MAC address flapping detection.

The **undo mac-address flapping detection exclude vlan** command restores MAC address flapping detection for a VLAN.

By default, the system performs MAC address flapping detection in all VLANs.

Format

mac-address flapping detection exclude vlan { *vlan-id1* [**to** *vlan-id2*] } &<1-10>

undo mac-address flapping detection exclude vlan { { *vlan-id1* [**to** *vlan-id2*] } &<1-10> | **all** }

Parameters

Parameter	Description	Value
vlan-id1 [**to** *vlan-id2*]	Specifies the ID of a VLAN where MAC address flapping detection is not required. ● *vlan-id1* specifies the first VLAN ID. ● **to** *vlan-id2* specifies the last VLAN ID. *vlan-id2* must be greater than *vlan-id1*. You can specify a maximum of 10 VLANs.	● The value of *vlan-id1* is an integer that ranges from 1 to 4094. ● The value of *vlan-id2* is an integer that ranges from 1 to 4094.
all	Indicates that all VLANs are excluded from MAC address flapping detection.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

By default, the system performs MAC address flapping detection in all VLANs. When a switch connected to a load balancing server with dual network adapters, the server's MAC address may be learned by two interfaces on the switch. This is a normal situation where MAC address flapping detection is not required.

You can run the **mac-address flapping detection exclude vlan** command to exclude a VLAN from MAC address flapping detection. If MAC address flapping occurs in this VLAN, the system does not send a trap message or record this event.

Precautions

If you run the **mac-address flapping detection exclude vlan** command multiple times, multiple VLANs are excluded from MAC address flapping detection.

Example

# Exclude VLAN 5 from MAC address flapping detection.

```
<HUAWEI> system-view
[HUAWEI] mac-address flapping detection exclude vlan 5
```

5.1.27 mac-address flapping detection vlan security-level

Function

The **mac-address flapping detection vlan security-level** command configures the security level of VLANs for MAC address flapping detection.

The **undo mac-address flapping detection vlan security-level** command restores the default security of VLANs for MAC address flapping detection.

By default, the security level of a VLAN for MAC address flapping detection is middle. At this security level, the system considers that a MAC address flapping occurs when a MAC address moves between interfaces 10 times.

Format

mac-address flapping detection vlan { { *vlan-id1* [**to** *vlan-id2*] } &<1-10> | **all** } **security-level** { **high** | **middle** | **low** }

undo mac-address flapping detection vlan { { *vlan-id1* [**to** *vlan-id2*] } &<1-10> | **all** } **security-level** [**high** | **middle** | **low**]

Parameters

Parameter	Description	Value
vlan-id1 [**to** *vlan-id2*]	Specifies the VLANs of which the security level needs to be set for MAC address flapping detection. ● *vlan-id1* specifies the ID of the first VLAN. ● **to** *vlan-id2* specifies the ID of the last VLAN. The value of *vlan-id2* must be larger than the value of *vlan-id1*. You can specify a maximum of 10 VLAN ID ranges in a command.	● The value of *vlan-id1* is an integer that ranges from 1 to 4094. ● The value of *vlan-id2* is an integer that ranges from 1 to 4094.
all	Configures security level of all VLANs for MAC address flapping detection.	-
high	Sets the security level of specified VLANs to high. At this security level, the system considers that a MAC address flapping occurs when a MAC address moves between interfaces three times.	-
middle	Sets the security level of specified VLANs to middle. At this security level, the system considers that a MAC address flapping occurs when a MAC address moves between interfaces 10 times.	-
low	Sets the security level of specified VLANs to low. At this security level, the system considers that a MAC address flapping occurs when a MAC address moves between interfaces 50 times.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

By default, the switch considers that a MAC address flapping occurs when a MAC address moves between interfaces 10 times. On an unstable network, it may be a normal situation when a MAC address moves between interfaces 10 times. You can set the security level for VLANs according to the actual situation of your network. The switch reports a MAC address flapping when a MAC address moves between interfaces for the specified number of times.

Example

# Set the security level of VLAN 5 to high for MAC address flapping.

```
<HUAWEI> system-view
[HUAWEI] mac-address flapping detection vlan 5 security-level high
```

5.1.28 mac-address flapping mac-syn-suppress disable

Function

The **mac-address flapping mac-syn-suppress disable** command disables real-time MAC address synchronization suppression triggered by MAC address flapping.

The **undo mac-address flapping mac-syn-suppress disable** command enables real-time MAC address synchronization suppression triggered by MAC address flapping.

By default, MAC address synchronization suppression triggered by MAC address flapping is enabled.

Format

mac-address flapping mac-syn-suppress disable

undo mac-address flapping mac-syn-suppress disable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

By default, real-time MAC address synchronization suppression is enabled on a device. With this function enabled, if a large number of real-time MAC address synchronization packets are generated due to persistent MAC address flapping, real-time MAC address synchronization suppression will be triggered. This will result in problems such as delay in obtaining DHCP addresses in terminal roaming scenarios. To address such problems, run the **mac-address flapping mac-syn-suppress disable** command to disable real-time MAC address synchronization suppression triggered by MAC address flapping.

Example

# Disable real-time MAC address synchronization suppression triggered by MAC address flapping.

```
<HUAWEI> system-view
[HUAWEI] mac-address flapping mac-syn-suppress disable
```

5.1.29 mac-address flapping quit-vlan recover-time

Function

The **mac-address flapping quit-vlan recover-time** command sets the delay time an interface waits to join a VLAN again after it is removed from the VLAN due to MAC address flapping.

The **undo mac-address flapping quit-vlan recover-time** command restores the default delay time.

By default, the delay time is 10 minutes.

Format

mac-address flapping quit-vlan recover-time *time-value*

undo mac-address flapping quit-vlan recover-time

Parameters

Parameter	Description	Value
time-value	Specifies the delay time an interface waits to join a VLAN again after it is removed from the VLAN due to MAC address flapping.	The value is an integer ranging from 0 to 1440, in minutes. The default value is 10. The value 0 indicates that the interface cannot join a VLAN again after it is removed from the VLAN.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If an interface is removed from a VLAN because MAC address flapping occurs in the VLAN, the interface can automatically join the VLAN again after a delay.

Precautions

If an interface is removed from multiple VLANs due to MAC address flapping, the system counts the delay time since the interface is removed from the last VLAN.

Example

# Set the delay time before an interface joins a VLAN again to 15 minutes.

```
<HUAWEI> system-view
[HUAWEI] mac-address flapping quit-vlan recover-time 15
```

# Restore the default delay time.

```
<HUAWEI> system-view
[HUAWEI] undo mac-address flapping quit-vlan recover-time
```

5.1.30 mac-address flapping unicast-suppress all disable

Function

The **mac-address flapping unicast-suppress all disable** command globally disables MAC address flapping suppression.

The **undo mac-address flapping unicast-suppress all disable** command cancels the configuration.

By default, unknown unicast traffic suppression is enabled globally.

Format

mac-address flapping unicast-suppress all disable

undo mac-address flapping unicast-suppress all disable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

By default, if MAC address flapping detection is enabled on a device and MAC address flapping is detected, traffic suppression is triggered on the corresponding interface. As a result, excess traffic is discarded, resulting in packet loss.

To prevent this, disable unknown unicast traffic suppression.

Example

# Globally disable unknown unicast traffic suppression.

```
<HUAWEI> system-view
[HUAWEI] mac-address flapping unicast-suppress all disable
```

5.1.31 mac-address flapping unicast-suppress disable

Function

The **mac-address flapping unicast-suppress disable** command disables MAC address flapping suppression on an interface.

The **undo mac-address flapping unicast-suppress disable** command cancels the configuration.

By default, unknown unicast traffic suppression is enabled on an interface.

Format

mac-address flapping unicast-suppress disable

undo mac-address flapping unicast-suppress disable

Parameters

None

Views

Interface view

Ethernet interface view, GE interface view, XGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, MultiGE interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

By default, if MAC address flapping detection is enabled on a device and MAC address flapping is detected, traffic suppression is triggered on the corresponding interface. As a result, excess traffic is discarded, resulting in packet loss.

To prevent this, disable unknown unicast traffic suppression.

Precautions

Unknown unicast traffic suppression takes effect on an interface only when the following conditions are met:

- Global MAC address flapping detection is configured.
- MAC address flapping occurs on the interface.
- Unknown unicast traffic suppression is enabled globally.
- Unknown unicast traffic suppression is enabled on the interface.

Example

# Disable unknown unicast traffic suppression on GE0/0/1.

```
<HUAWEI> system-view
<HUAWEI> interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] mac-address flapping unicast-suppress disable
```

5.1.32 mac-address hash-bucket-mode

Function

The **mac-address hash-bucket-mode** command sets the hash bucket size of the MAC address table.

The **undo mac-address hash-bucket-mode** command restores the default hash bucket size of the MAC address table.

By default, the hash bucket size of the MAC address table is 4.

NOTE

Only the SS1720GW-E, S1720GWR-E, S5720-LI, S5720S-LI, and S5720I-SI support this command.

Format

mac-address hash-bucket-mode { **size4** | **size8** | **size12** | **size16** }

undo mac-address hash-bucket-mode

Parameters

Parameter	Description	Value
size4	Indicates that the hash bucket size of the MAC address table is 4.	-

Parameter	Description	Value
size8	Indicates that the hash bucket size of the MAC address table is 8.	-
size12	Indicates that the hash bucket size of the MAC address table is 12.	-
size16	Indicates that the hash bucket size of the MAC address table is 16.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To improve the MAC address forwarding performance, the MAC address table of the device is saved using a hash link. When the same key value is obtained for multiple MAC addresses according to the hash algorithm, some MAC addresses may be not learned. That is, the MAC address hash conflict occurs. When the MAC address hash conflict occurs, traffic with this destination MAC address can only be broadcast. This occupies device bandwidth and resources.

When the MAC address hash conflict aggravates, run this command to increase the hash bucket size of the MAC address table.

Precautions

A larger hash bucket size will lower device forwarding performance.

When the hash bucket size becomes small, you need to restart the device.

Example

# Set the hash bucket size of the MAC address table to 16.

```
<HUAWEI> system-view
[HUAWEI] mac-address hash-bucket-mode size16
```

5.1.33 mac-address hash-mode

Function

The **mac-address hash-mode** command configures a MAC hash algorithm on the device.

The **undo mac-address hash-mode** command restores the default MAC hash algorithm on the device.

By default, the hash algorithm on the S6735-S, S6720-EI and S6720S-EI is **crc32-lower**. The hash algorithm on other models is **crc**.

NOTE

The S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735-S-I, S5735S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S do not support this command.

Format

On the S6735-S, S6720-EI and S6720S-EI:

mac-address hash-mode { **crc16-lower** | **crc16-upper** | **crc32-lower** | **crc32-upper** | **lsb** | **enhanced** } **slot** *slot-id*

undo mac-address hash-mode [**crc16-lower** | **crc16-upper** | **crc32-lower** | **crc32-upper** | **lsb** | **enhanced**] **slot** *slot-id*

On devices except S6735-S, S6720-EI and S6720S-EI:

mac-address hash-mode { **xor** | **crc** } **slot** *slot-id*

undo mac-address hash-mode [**xor** | **crc**] **slot** *slot-id*

Parameters

Parameter	Description	Value
crc	Indicates the CRC-based hash algorithm.	-
crc16-lower	Indicates the hash algorithm based on low order bits of CRC16.	-
crc16-upper	Indicates the hash algorithm based on high order bits of CRC16.	-
crc32-lower	Indicates the hash algorithm based on low order bits of CRC32.	-
crc32-upper	Indicates the hash algorithm based on high order bits of CRC32.	-

Parameter	Description	Value
lsb	Indicates the hash algorithm based on the lowest bit of the key value.	-
xor	Indicates the Exclusive-Or mode.	-
enhanced	Indicates the enhanced mode.	-
slot *slot-id*	Specifies a slot ID.	The value depends on the device configuration.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The device uses a hash algorithm to improve MAC address forwarding performance. If multiple MAC addresses match a key value, a hash conflict occurs.

When a hash conflict occurs, the device may fail to learn many MAC addresses and some traffic can only be broadcast. This results in heavy broadcast traffic on the device. If such a problem occurs, use an appropriate hash algorithm to reduce the hash conflict.

Precautions

- MAC addresses are distributed on a network randomly, so the system cannot determine the best hash algorithm. Generally, the default hash algorithm is the best one, so do not change the hash algorithm unless you have special requirement.
- An appropriate hash algorithm can only reduce hash conflicts, but cannot prevent them.
- After changing the hash algorithm and saving the configuration, restart the device for the configuration to take effect.
- If you run the **mac-address hash-mode** command multiple times, only the latest configuration takes effect.

Example

# Set the hash algorithm on the device to **crc**.

```
<HUAWEI> system-view
[HUAWEI] mac-address hash-mode crc slot 0
```

5.1.34 mac-address learning disable (interface view and VLAN view)

Function

The **mac-address learning disable** command disables MAC address learning.

The **undo mac-address learning disable** command enables MAC address learning.

By default, MAC address learning is enabled.

Format

mac-address learning disable [**action** { **discard** | **forward** }] (Interface view)

mac-address learning disable (VLAN view)

undo mac-address learning disable

Parameters

Parameter	Description	Value
action	Indicates the action that the interface takes after MAC address learning is disabled. ● This parameter takes effect only in the interface view and port group view, and the specified interface must be a Layer 2 interface. ● You can use this parameter to determine whether packets are forwarded when the specified interface does not need to learn MAC addresses. By default, an interface forwards the packets carrying new MAC addresses after MAC address learning is disabled.	-

Parameter	Description	Value
discard	Discards the packets whose source MAC addresses do not match the MAC address table.	-
forward	Forwards the packets according to the MAC address table.	-

Views

VLAN view, 100GE interface view, Ethernet interface view, GE interface view, XGE interface view, 40GE interface view, MultiGE interface view, Eth-Trunk interface view, port group view, 25GE interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If you want an interface to forward only packets with certain MAC addresses, use this command. For example, if an interface is connected to a server, configure a static MAC address entry with the MAC address of the server, and then disable MAC address learning and set the action to discard on the interface. The configuration prevents other servers or terminals from accessing the interface and improves network stability and security.

When a switch with MAC address learning enabled receives an Ethernet frame, it records the source MAC address and inbound interface of the Ethernet frame in a MAC address entry. When receiving other Ethernet frames destined for this MAC address, the switch forwards the frames through the corresponding outbound interface according to the MAC address entry. MAC address learning reduces broadcast packets on a network.

You can use the **mac-address learning disable** command to disable MAC address learning on an interface. The action performed on received packets can be set to **discard** or **forward**.

By default, the switch takes the forward action after MAC address learning is disabled. That is, the switch forwards packets according to the MAC address table. When the action is set to discard, the switch looks up the source MAC address of the packet in the MAC address table. If the source MAC address is found in the MAC address table, the switch forwards the packet according to the matching MAC address entry. If the source MAC address is not found, the switch discards the packet.

Precautions

- Before running the **mac-address learning disable** command on an Eth-Trunk interface, ensure that the Eth-Trunk interface works in Layer 2 mode; otherwise, the configuration fails. To switch an Eth-Trunk interface from the Layer 3 mode to the Layer 2 mode, you can run the **portswitch** command in the view of the Eth-Trunk interface.
- After MAC address learning is disabled on an interface, the device does not learn new MAC addresses on the interface. Untrusted terminals can still access the network.
- After MAC address learning is disabled on an interface, dynamic MAC address entries learned on the interface are not immediately deleted. These entries will be deleted after the aging time elapses or after you run a command to manually delete the entries. If a MAC address entry is always matched to direct traffic forwarding, this entry will not be aged out.
- On the S6735-S, if the number of MAC addresses learned in the VLAN reaches the upper limit or the MAC address learning function is disabled in the VLAN, the packet discarding function configured using the **mac-address learning disable action discard** command does not take effect on interfaces in the VLAN.

Example

# Disable MAC address learning in VLAN 2.

```
<HUAWEI> system-view
[HUAWEI] vlan 2
[HUAWEI-vlan2] mac-address learning disable
```

5.1.35 mac-address learning disable (traffic behavior view)

Function

The **mac-address learning disable** command disables MAC address learning in a traffic behavior.

The **undo mac-address learning disable** command enables MAC address learning in a traffic behavior.

By default, MAC address learning is enabled in a traffic behavior.

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735-S-I, S5735S-S, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Format

mac-address learning disable

undo mac-address learning disable

Parameters

None

Views

Traffic behavior view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **mac-address learning disable** command is used in the following scenarios:

- When a network is running stably and the MAC address of packets is fixed, a device does not need to learn MAC addresses of other packets. To save MAC addresses and improve device efficiency, apply a traffic policy and disable MAC address learning in all the traffic classifiers bound to the traffic policy.
- Some unauthorized users may change MAC addresses frequently to attack the network. To prevent MAC address overflow and protect device performance, apply a traffic policy and disable MAC address learning in all the traffic classifiers bound to the traffic policy.

Follow-up Procedure

Run the **traffic policy** command to create a traffic policy and run the **classifier behavior** command in the traffic policy view to bind the traffic classifier to the traffic behavior containing the action of disabling MAC address learning.

Precautions

After the traffic behavior containing **mac-address learning disable** is bound to the specified traffic classifier, the source MAC addresses of packets matching the traffic classifier are not learned. The source MAC addresses of packets that do not match the traffic classifier are still learned by default.

The **mac-address learning disable** command is similar to the **mac-address learning disable** command in the interface view or VLAN view. The difference is that the **mac-address learning disable** command is valid for the packets matching the user-defined traffic classifier and is applied to the system, an interface, or a VLAN by using the traffic policy. The **mac-address learning disable** command is used in the interface view, port group view, or VLAN view and is valid for all the packets in the corresponding view.

To disable MAC address learning on an interface, in a port group, or in a VLAN, run the **mac-address learning disable** command in the corresponding view. To disable MAC address learning for a specified traffic classifier, run the **mac-address learning disable** command in the traffic behavior view.

Example

# Disable MAC address learning in the traffic behavior **test**.

```
<HUAWEI> system-view
[HUAWEI] traffic behavior test
[HUAWEI-behavior-test] mac-address learning disable
```

5.1.36 mac-address learning self-healing enable

Function

The **mac-address learning self-healing enable** command enables self-healing for MAC address learning.

The **undo mac-address learning self-healing enable** command disables self-healing for MAC address learning.

By default, self-healing is enabled for MAC address learning.

Format

mac-address learning self-healing enable

undo mac-address learning self-healing enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

If the SAID node is enabled, the switch periodically checks whether MAC address learning of the Eth-Trunk, port security, and MAC address management modules is normal. You can run the **mac-address learning self-healing enable** command to enable self-healing for MAC address learning. After this function is enabled, self-healing is automatically performed upon detection of service status inconsistencies. This ensures that packets are forwarded correctly.

Example

# Enable self-healing for MAC address learning.

```
<HUAWEI> system-view
[HUAWEI] mac-address learning self-healing enable
```

5.1.37 mac-address static vlan

Function

The **mac-address static vlan** command configures a static MAC address entry.

The **undo mac-address static vlan** command deletes a static MAC address entry.

By default, no static MAC address entry is configured.

Format

mac-address static *mac-address interface-type interface-number* **vlan** *vlan-id*

undo mac-address static [*interface-type interface-number* | **vlan** *vlan-id*] *

undo mac-address static *mac-address interface-type interface-number* **vlan** *vlan-id*

NOTE

For details on how to configure a VSI-based static MAC address entry, see **mac-address static vlanif** and **mac-address static vsi**.

Parameters

Parameter	Description	Value
mac-address	Specifies the MAC address in a static MAC address entry.	The value is in H-H-H format. An H is a hexadecimal number of 1 to 4 digits. The MAC address cannot be FFFF-FFFF-FFFF, 0000-0000-0000, or a multicast MAC address.
interface-type interface-number	Specifies the outbound interface in a static MAC address entry.	-
vlan *vlan-id*	Specifies the ID of the VLAN that the outbound interface belongs to.	The value is an integer that ranges from 1 to 4094.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Static MAC address entries are used for the following purposes:

- Improve security. The device directly discards packets sent from unauthorized users using authorized users' MAC addresses.
- Guide unicast forwarding and save bandwidth.

Precautions

- The VLAN in a static MAC address entry must have been created and the outbound interface in the same static MAC address entry has been added to the VLAN.
- If you configure a static MAC address entry when the MAC address table is full, the device processes the MAC address entry as follows:
  - If a dynamic MAC address entry with the same MAC address and VLAN ID exists in the MAC address table, the static MAC address entry replaces the dynamic MAC address entry.
  - If no dynamic MAC address entry with the same MAC address exists in the MAC address table, the system deletes one dynamic MAC address entry and adds the static MAC address entry to the MAC address table.
- You can run the **mac-address static** command multiple times to configure multiple static MAC address entries.
- An existing MAC address entry of the authen, pre-authen, security, or sticky type cannot be configured as a static MAC address entry.

Example

# Add a static MAC address entry to the MAC address table. In the MAC address entry, the destination MAC address is 00e0-fc12-3456, the VLAN ID is 4, and the outbound interface is gigabitethernet0/0/2. That is, the device forwards packets with the destination MAC address of 00e0-fc12-3456 from VLAN 4 through gigabitethernet0/0/2.

```
<HUAWEI> system-view
[HUAWEI] vlan 4
[HUAWEI-vlan4] quit
[HUAWEI] interface gigabitethernet 0/0/2
[HUAWEI-GigabitEthernet0/0/2] port link-type access
[HUAWEI-GigabitEthernet0/0/2] port default vlan 4
[HUAWEI-GigabitEthernet0/0/2] quit
[HUAWEI] mac-address static 00e0-fc12-3456 gigabitethernet 0/0/2 vlan 4
```

5.1.38 mac-address threshold-alarm

Function

The **mac-address threshold-alarm** command configures upper and lower alarm thresholds for the MAC address usage.

The **undo mac-address threshold-alarm** command restores the default upper and lower alarm thresholds for the MAC address usage.

By default, the upper and lower alarm thresholds for the MAC address usage are 80% and 70% respectively. An alarm is sent when the MAC address usage is higher than 80% or lower than 70%.

Format

mac-address threshold-alarm upper-limit *upper-limit-value* **lower-limit** *lower-limit-value*

undo mac-address threshold-alarm

Parameters

Parameter	Description	Value
upper-limit *upper-limit-value*	Specifies the upper alarm threshold for the MAC address usage, in percentage.	The value is an integer that ranges from 1 to 100. The default value is 80.
lower-limit *lower-limit-value*	Specifies the lower alarm threshold for the MAC address usage, in percentage.	The value is an integer that ranges from 1 to 100. The default value is 70. *lower-limit-value* must be smaller than or equal to *upper-limit-value*.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

MAC address resources are core resources of the device and the device supports limited MAC addresses. The MAC address usage affects device running. You can run the **mac-address threshold-alarm** command to configure upper and lower alarm thresholds for the MAC address usage. When the MAC address usage is larger than the upper alarm threshold or smaller than the lower alarm threshold, an alarm is generated to notify the administrator. The administrator then can learn the MAC address usage in a timely manner.

Precautions

When you run the **mac-address threshold-alarm** command multiple times, only the latest configuration takes effect.

Example

# Set upper and lower alarm thresholds for the MAC address usage to 90% and 20% respectively.

```
<HUAWEI> system-view
[HUAWEI] mac-address threshold-alarm upper-limit 90 lower-limit 20
```

5.1.39 mac-address trap hash-conflict enable

Function

The **mac-address trap hash-conflict enable** command enables the trap function for the MAC address hash conflict.

The **undo mac-address trap hash-conflict enable** command disables the trap function for the MAC address hash conflict.

By default, the trap function for the MAC address hash conflict is enabled.

Format

mac-address trap hash-conflict enable

undo mac-address trap hash-conflict enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

To improve the MAC address forwarding performance, the MAC address table of the device is saved using a hash link. When the same key value is obtained for multiple MAC addresses according to the hash algorithm, some MAC addresses may be not learned. That is, the MAC address hash conflict occurs.

In this situation, the MAC address table space is not full but the MAC address entry cannot be learned. When the MAC address hash conflict occurs, traffic with this destination MAC address can be only broadcast. This occupies device bandwidth and resources. You can replace the device or network adapter of the terminal.

After the trap function for the MAC address hash conflict is configured, the administrator can immediately discover MAC address hash conflicts.

Example

# Enable the trap function for the MAC address hash conflict.

```
<HUAWEI> system-view
[HUAWEI] mac-address trap hash-conflict enable
```

5.1.40 mac-address trap hash-conflict history

Function

The **mac-address trap hash-conflict history** command sets the number of alarms reported at an interval when the MAC address hash conflict occurs.

The **undo mac-address trap hash-conflict history** command restores the default number of alarms reported at an interval when the MAC address hash conflict occurs.

By default, 10 alarms are reported at an interval when the MAC address hash conflict occurs.

Format

mac-address trap hash-conflict history *history-number*

undo mac-address trap hash-conflict history

Parameters

Parameter	Description	Value
history-number	Specifies the number of alarms reported at an interval when the MAC address hash conflict occurs.	The value is an integer that ranges from 1 to 20.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the trap function for the MAC address hash conflict is enabled, the device reports a maximum of 10 alarms every 60s. Each alarm carries a MAC address for which the hash conflict occurs.

If hash values of more than 10 MAC addresses conflict, reports about subsequent MAC address hash conflicts cannot be reported. You can run this command to set the number of alarms reported at an interval.

Precautions

When you run the **mac-address trap hash-conflict history** command multiple times, only the latest configuration takes effect.

Example

# Set the number of alarms reported at an interval to 12 when the MAC address hash conflict occurs.

```
<HUAWEI> system-view
[HUAWEI] mac-address trap hash-conflict history 12
```

5.1.41 mac-address trap hash-conflict interval

Function

The **mac-address trap hash-conflict interval** command sets the interval at which alarms are reported when the MAC address hash conflict occurs.

The **undo mac-address trap hash-conflict interval** command restores the default interval at which alarms are reported when the MAC address hash conflict occurs.

By default, alarms are reported at intervals of 60s when the MAC address hash conflict occurs.

Format

mac-address trap hash-conflict interval *interval-time*

undo mac-address trap hash-conflict interval

Parameters

Parameter	Description	Value
interval-time	Specifies the interval at which alarms are reported when the MAC address hash conflict occurs.	The value is an integer that ranges from 60 to 3600, in seconds.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the trap function for the MAC address hash conflict is enabled, the device reports a maximum of 10 alarms every 60s. Each alarm carries a MAC address for which the hash conflict occurs.

If a small interval is used, alarms about MAC address hash conflicts are reported immediately. When there are many MAC address hash conflicts, many alarms are reported.

If a long interval is used and many MAC address hash conflicts occur, alarms will be suppressed. You can adjust the interval according to the requirements.

Precautions

When you run the **mac-address trap hash-conflict interval** command multiple times, only the latest configuration takes effect.

Example

# Set the interval at which alarms are reported to 90s when the MAC address hash conflict occurs.

```
<HUAWEI> system-view
[HUAWEI] mac-address trap hash-conflict interval 90
```

5.1.42 mac-address trap hash-conflict threshold

Function

The **mac-address trap hash-conflict threshold** command sets the lower alarm threshold for MAC address hash conflicts.

The **mac-address trap hash-conflict threshold** command restores the default value of the lower alarm threshold for MAC address hash conflicts.

By default, the lower alarm threshold for MAC address hash conflicts is 0.

Format

mac-address trap hash-conflict threshold *threshold-value*

undo mac-address trap hash-conflict threshold

Parameters

Parameter	Description	Value
threshold-value	Specifies the lower alarm threshold for MAC address hash conflicts.	The value is an integer that ranges from 0 to 20. The default value is 0.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the trap function for MAC address hash conflicts is configured on a switch, the switch sends an alarm if a MAC address hash conflict occurs. This helps you detect and rectify the fault in time.

If a small number of MAC address hash conflicts occur on the network and users do not need to be aware of the conflicts, you can run the **mac-address trap hash-conflict threshold** command on a switch to set the lower alarm threshold for MAC address hash conflicts. The switch sends an alarm only if the number of MAC address hash conflicts exceeds the lower alarm threshold.

Precautions

If you run this command multiple times, only the latest configuration takes effect.

If the lower alarm threshold for MAC address hash conflict is set to 20 on a device, the device does not report MAC address hash conflict alarms regardless of the number of MAC address hash conflict alarms generated during each period.

Example

# Set the lower alarm threshold for MAC address hash conflicts to 10.

```
<HUAWEI> system-view
[HUAWEI] mac-address trap hash-conflict threshold 10
```

5.1.43 mac-address trap notification

Function

The **mac-address trap notification** command enables the trap function for MAC address learning or aging.

The **undo mac-address trap notification** command disables the trap function for MAC address learning or aging.

By default, the trap function for MAC address learning or aging is disabled.

Format

mac-address trap notification { **aging** | **learn** | **all** }

undo mac-address trap notification

Parameters

Parameter	Description	Value
aging	Enables the trap function for MAC address aging.	-

Parameter	Description	Value
learn	Enables the trap function for MAC address learning.	-
all	Enables the trap function for MAC address learning and aging.	-

Views

Ethernet interface view, GE interface view, XGE interface view, 40GE interface view, 100GE interface view, MultiGE interface view, Eth-Trunk interface view, port group view, 25GE interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To learn MAC address change in a timely manner, run the **mac-address trap notification** command to enable the trap function for MAC address learning or aging.

Precautions

When you run the **mac-address trap notification** command multiple times, only the latest configuration takes effect.

The trap function for MAC address learning or aging is not supported for the MAC address entries in a VSI.

Example

# Enable the trap function for MAC address learning on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface GigabitEthernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] mac-address trap notification learn
```

5.1.44 mac-address trap notification interval

Function

The **mac-address trap notification interval** command sets the interval at which the device checks MAC address learning or aging.

The **undo mac-address trap notification interval** command restores the default interval at which the device checks MAC address learning or aging.

By default, the device checks MAC address learning or aging at intervals of 10s.

Format

mac-address trap notification interval *interval-time*

undo mac-address trap notification interval

Parameters

Parameter	Description	Value
interval-time	Specifies the interval at which the device checks MAC address learning or aging.	The value is an integer that ranges from 10 to 600, in seconds. The default value is 10.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

After the **mac-address trap notification** command is used to enable the trap function when the device learns MAC addresses or MAC addresses are aged, the device periodically checks whether MAC addresses are learned or aged. You can run the **mac-address trap notification interval** command to set the interval.

Example

# Set the interval at which the device checks MAC address learning or aging to 20s.

```
<HUAWEI> system-view
[HUAWEI] mac-address trap notification interval 20
```

5.1.45 mac-address update arp

Function

The **mac-address update arp** command enables the MAC address-triggered ARP entry update function. That is, the Switch is enabled to update outbound interfaces in ARP entries when outbound interfaces in MAC address entries change.

The **undo mac-address update arp** command disables the MAC address-triggered ARP entry update function.

By default, the MAC address-triggered ARP entry update function is disabled.

Format

mac-address update arp

undo mac-address update arp

NOTE

The S200, S1730S-S1 does not support this command.

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On the Ethernet, MAC address entries are used to guide Layer 2 data forwarding. The ARP entries that define the mapping between IP addresses and MAC addresses guide communication between devices on different network segments.

The outbound interface in a MAC address entry is updated by packets, whereas the outbound interface in an ARP entry is updated after the aging time is reached. In this case, the outbound interfaces in the MAC address entry and ARP entry may be different. To address this issue, run the **mac-address update arp** command to enable the Switch to update outbound interfaces in ARP entries when outbound interfaces in MAC address entries change.

Precautions

This command takes effect only for dynamic ARP entries. Static ARP entries are not updated when the corresponding MAC address entries change.

The **mac-address update arp** command does not take effect after ARP entry fixing is enabled by using the **arp anti-attack entry-check { fixed-mac | fixed-all | send-ack } enable** command.

After the **mac-address update arp** command is run, the Switch updates an ARP entry only if the outbound interface in the corresponding MAC address entry changes.

After this command is executed, the **arp anti-attack gratuitous-arp drop** command becomes invalid and the Switch cannot drop gratuitous ARP packets.

Example

# Enable the MAC address-triggered ARP entry update function.

```
<HUAWEI> system-view
[HUAWEI] mac-address update arp
```

5.1.46 mac-learning priority

Function

The **mac-learning priority** command sets the MAC address learning priority of an interface.

The **undo mac-learning priority** command restores the default MAC learning priority of an interface.

By default, the MAC address learning priority of an interface is 0.

NOTE

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

Format

mac-learning priority *priority-id*

undo mac-learning priority

Parameters

Parameter	Description	Value
priority *priority-id*	Specifies the MAC address learning priority of an interface.	The value is an integer that ranges from 0 to 3. A larger value indicates a higher priority.

Views

GE interface view, XGE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, port group view, 25GE interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

An uplink interface of the switch is connected to a server, and downlink interfaces are connected to users. To prevent unauthorized users from using the server MAC address to connect to the switch, run the **mac-learning priority** command to set the priority of the uplink interface to be higher than the user-side interfaces. When these interfaces learn the same MAC address, the MAC address entry learned by the uplink interface overrides MAC address entries learned by the user-side interfaces. Therefore, the switch will not learn MAC addresses of unauthorized users, and authorized users can access the server and use network resources.

You can run the **undo mac-learning priority allow-flapping** command to forbid MAC address flapping between interfaces with the same priority.

Both the **undo mac-learning priority allow-flapping** command and the **mac-learning priority** command can prevent MAC address flapping. The difference between the two commands is as follows:

- The **undo mac-learning priority allow-flapping** command prevents MAC address flapping between interfaces with the same priority. If an attacker uses the server MAC address to connect to the switch after the server is powered off, the switch learns the MAC address of the forged server. After the real server is powered on, the switch cannot learn the correct server MAC address.
- The **mac-learning priority** command prevents MAC address flapping between interfaces with different priorities. If an attacker uses the server MAC address to connect to the switch after the server is powered off, the switch learns the MAC address of the forged server. After the real server is powered on, the switch can learn the correct server MAC address.

Precautions

If you run the **mac-learning priority** command multiple times in the same interface view, only the latest configuration takes effect.

The function is not supported for the MAC address entries in a VSI.

Example

# Set the MAC address learning priority of GigabitEthernet0/0/2 to 3.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/2
[HUAWEI-GigabitEthernet0/0/2] mac-learning priority 3
```

5.1.47 mac-learning priority allow-flapping

Function

The **mac-learning priority allow-flapping** command allows MAC address flapping between interfaces with the same priority.

The **undo mac-learning priority allow-flapping** command prevents MAC address flapping between interfaces with the same priority.

By default, MAC address flapping between interfaces with the same priority is allowed.

NOTE

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

Format

mac-learning priority *priority-id* **allow-flapping**

undo mac-learning priority *priority-id* **allow-flapping**

Parameters

Parameter	Description	Value
priority *priority-id*	Specifies the MAC address learning priority of an interface.	The value is an integer that ranges from 0 to 3. A larger value indicates a higher priority.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

An uplink interface of the switch is connected to a server, and downlink interfaces are connected to users. To prevent unauthorized users from using the server MAC address to connect to the switch, you can run the **undo mac-learning priority allow-flapping** command to forbid MAC address flapping between interfaces with the same priority. MAC address then will not be learned by multiple interfaces. This prevents attackers from using the MAC addresses of valid devices to attack the switch.

Both the **mac-learning priority** command and the **undo mac-learning priority allow-flapping** command can prevent MAC address flapping. The difference between the two commands is as follows:

- The **undo mac-learning priority allow-flapping** command prevents MAC address flapping between interfaces with the same priority. If an attacker uses the server MAC address to connect to the switch after the server is powered off, the switch learns the MAC address of the forged server. After the real server is powered on, the switch cannot learn the correct server MAC address.
- The **mac-learning priority** command prevents MAC address flapping between interfaces with different priorities. If an attacker uses the server MAC address to connect to the switch after the server is powered off, the switch learns the MAC address of the forged server. After the real server is powered on, the switch can learn the correct server MAC address.

Precautions

The function is not supported for the MAC address entries in a VSI.

Example

# Forbid MAC address flapping between interfaces with priority 1.

```
<HUAWEI> system-view
[HUAWEI] undo mac-learning priority 1 allow-flapping
```

5.1.48 mac-learning priority flapping-defend action

Function

The **mac-learning priority flapping-defend action** command configures an action to be taken when the switch is configured to prohibit MAC address flapping.

The **undo mac-learning priority flapping-defend action** command restores the default action when the switch is configured to prohibit MAC address flapping.

By default, the action is **forward** when the switch is configured to prohibit MAC address flapping.

NOTE

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

Format

mac-learning priority flapping-defend action { **forward** | **discard** }

undo mac-learning priority flapping-defend action

Parameters

Parameter	Description	Value
forward	Packets are forwarded when the switch is configured to prohibit MAC address flapping.	-
discard	Packets are discarded when the switch is configured to prohibit MAC address flapping.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

An uplink interface of the switch is connected to a server, and a downlink interface is connected to a user. To prevent a malicious user from using a forged server's MAC address to attack the switch, run the **mac-learning priority** command in the interface view or the **undo mac-learning priority allow-flapping** command in the system view to prohibit MAC address flapping. A MAC address then will not be learned by multiple interfaces, and the malicious user cannot use the MAC address of a valid device to attack the switch. However, packets of the malicious user are still forwarded. You can configure the **discard** action to discard packets from the malicious user when MAC address flapping is prohibited.

Precautions

- If the **mac-learning priority** or **undo mac-learning priority allow-flapping** command is not used, the action specified using this command is invalid.
- This command is invalid for MAC addresses in a VSI.

Example

# Configure the switch to discard packets when the switch is configured to prohibit MAC address flapping.

```
<HUAWEI> system-view
[HUAWEI] mac-learning priority flapping-defend action discard
```

5.1.49 mac-limit

Function

The **mac-limit** command configures a rule to limit the number of MAC addresses that can be learned.

The **undo mac-limit** command deletes the rule.

By default, the number of learned MAC addresses is not limited.

Format

mac-limit { **maximum** *max-num* | **action** { **discard** | **forward** } | **alarm** { **disable** | **enable** } } * (Interface view)

mac-limit { **maximum** *max-num* | **action** { **discard** | **forward** } | **alarm** { **disable** | **enable** } } * (This command is supported in the VLAN view only on the S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735S-S, S5735-S-I, S5731-H, S5731-S, S5731S-S, S5731S-H, S5732-H, S6730-H, S6730S-H, S6730-S, S6730S-S.)

mac-limit { **maximum** *max-num* | **alarm** { **disable** | **enable** } } * (This command is supported in the VLAN view only on the devices except the S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735S-S, S5735-S-I, S5731-H, S5731-S, S5731S-S, S5731S-H, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S. When the number of learned MAC address entries reaches the limit on a device, the device still forwards packets with new source MAC addresses, but does not add the new MAC addresses to the MAC address table.)

undo mac-limit

Parameters

Parameter	Description	Value
action { **discard** | **forward** }	Indicates the action performed when the number of learned MAC address entries reaches the limit. ● **discard**: discards packets with new source MAC addresses. ● **forward**: forwards packets with new source MAC addresses but does not add the new MAC addresses to the MAC address table.	If no action is specified in the command, the default action **discard** is used. **NOTE** On the S5735-L, S5735S-L, S5735S-L-M, S5735-S, S5735S-S, S5735-S-I, S5731-H, S5731-S, S5731S-S, S5731S-H, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S, running a version earlier than V200R019C10, the **action** parameter is unavailable. When the number learned of MAC addresses reaches the limit, the system takes the **forward** action by default.
alarm { **disable** | **enable** }	Indicates whether the system generates an alarm when the number of learned MAC address entries reaches the limit. ● **disable**: indicates that no alarm is generated when the number of learned MAC addresses reaches the limit. ● **enable**: indicates that an alarm is generated when the number of learned MAC addresses reaches the limit.	If you do not set this parameter in the command, the alarm function is enabled by default.

Parameter	Description	Value
maximum *max-num*	Sets the maximum number of MAC addresses that can be learned. **NOTE** If **maximum** is not set, you must run the **mac-limit** command with **maximum** specified. If you have run the **mac-limit** command to set the maximum number of MAC addresses that can be learned, you do not need to set **maximum** *max-num* when running this command again.	The value is a decimal integer that ranges from 0 to 4096. The value 0 indicates that the highest rate of MAC address learning is not limited.

Views

VLAN view, Ethernet interface view, 100GE interface view, 40GE interface view, GE interface view, XGE interface view, MultiGE interface view, Eth-Trunk interface view, port group view, 25GE interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **mac-limit** command limits the number of access users and prevents attacks to the MAC address tables. You can enable the function to improve network security.

Precautions

- The **mac-limit** command configuration takes effect only for dynamically learned MAC addresses. If some MAC addresses have been learned, run the **undo mac-address dynamic** command to delete the learned MAC address entries. If you do not delete them, less new MAC addresses can be learned than the value configured using the **mac-limit** command.
- After the **port-security enable** command is configured on an interface, **mac-limit** cannot take effect. Do not configure **mac-limit** and **port-security enable** simultaneously.
- The MAC address limiting function and NAC conflict on an interface; therefore, the **mac-limit** and **mac-authen**, **dot1x enable**, **web-auth-server** or **authentication-profile** commands cannot be used on the same interface.
- On the S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735-S-I, and S5735S-S, a maximum of 32 VLANs can be configured with the **action discard** parameter.

- If you run the **mac-limit** command in the interface view, the command takes effect only for MAC addresses learned from VLANs.
- On the S6735-S, if the number of MAC addresses learned in the VLAN reaches the upper limit or the MAC address learning function is disabled in the VLAN, the packet discarding function configured using the **mac-address learning disable action discard** command does not take effect on interfaces in the VLAN.

Example

# Set the maximum number of MAC addresses that can be learned by GigabitEthernet0/0/2 to 30. Configure the device to generate an alarm when the number learned of MAC addresses reaches the limit.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/2
[HUAWEI-GigabitEthernet0/0/2] mac-limit maximum 30 alarm enable
```

5.1.50 mac-spoofing-defend enable (interface view)

Function

The **mac-spoofing-defend enable** command configures an interface as a trusted interface.

The **undo mac-spoofing-defend enable** command restores an interface to an untrusted interface.

By default, an interface is untrusted.

NOTE

S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S do not support this command.

Format

mac-spoofing-defend enable

undo mac-spoofing-defend enable

Parameters

None

Views

GE interface view, Ethernet interface view, XGE interface view, 40GE interface view, MultiGE interface view, Eth-Trunk interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

User behaviors are uncontrollable; therefore, a user device may send bogus packets with the server MAC address to prevent other users from accessing the real server. To prevent such attacks, you can use the **mac-spoofing-defend enable** command to configure the network-side interface connected to the server as a trusted interface. The MAC address learned by the interface will not be learned by other interfaces. This prevents the attacks of bogus packets with the server MAC address.

Prerequisites

The MAC spoofing defense function has been enabled by using the **mac-spoofing-defend enable** command in the system view.

Precautions

- After the device connected to the trusted interface is powered off, the MAC address entry matching the device MAC address is aged out after a certain period. After another device is connected to the interface, the MAC address of this device will not be learned by other interfaces.
- On the SS1720GW-E, S1720GWR-E, S5720I-SI, S5720-LI, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5720S-LI, S5735-S, S500, S5735S-S, S5735-S-I, S5735S-H, S5736-S, and S6720S-S, when the TPID configured by the **qinq protocol** command on the inbound interface is different from the TPID in received packets and the **mac-spoofing-defend enable** command is also used on the inbound interface, the MAC address of packets in the VLAN specified by the PVID is learned, but not the MAC address-based VLAN, protocol-based VLAN, IP subnet-based VLAN, or policy VLAN. For example, the TPID on port A is 0x9100, the PVID is 10, MAC address-based VLAN is VLAN 20, received packet A contains VLAN 30 and TPID of 0x8100 that matches the MAC address-based VLAN. Because TPID values are different, the interface considers that packet A is untagged and adds VLAN 20 to packet A. The MAC address in VLAN 20 is therefore learned. If the **mac-spoofing-defend enable** command is configured on port A, the MAC address in VLAN 10 is incorrectly learned.

Example

# Configure GigabitEthernet0/0/1 as a trusted interface.

```
<HUAWEI> system-view
[HUAWEI] interface GigabitEthernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] mac-spoofing-defend enable
```

5.1.51 mac-spoofing-defend enable (system view)

Function

The **mac-spoofing-defend enable** command enables global MAC spoofing defense.

The **undo mac-spoofing-defend enable** command disables global MAC spoofing defense.

By default, global MAC spoofing defense is disabled.

NOTE

S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S do not support this command.

Format

mac-spoofing-defend enable

undo mac-spoofing-defend enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

User behaviors are uncontrollable; therefore, a user device may send bogus packets with the server MAC address to prevent other users from accessing the real server. To prevent such attacks, you can use the **mac-spoofing-defend enable** command to configure the network-side interface connected to the server as a trusted interface. The MAC address learned by the interface will not be learned by other interfaces. This prevents the attacks of bogus packets with the server MAC address.

Before configuring an interface as a trusted interface, you must use the **mac-spoofing-defend enable** command to enable global MAC spoofing defense.

Precautions

After you run the **undo mac-spoofing-defend enable** command in the system view to disable global MAC spoofing defense, the **mac-spoofing-defend enable** command cannot be used in the interface view.

On the S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735-S-I, and S5735S-S, after MAC spoofing defense is enabled globally, the real-time performance of MAC address flapping detection on the interfaces that are not enabled with MAC spoofing defense decreases.

On the S300 and S500, after MAC spoofing defense is enabled globally, the real-time performance of MAC address flapping detection on the interfaces that are not enabled with MAC spoofing defense decreases.

Example

# Enable global MAC spoofing defense.

```
<HUAWEI> system-view
[HUAWEI] mac-spoofing-defend enable
```

5.1.52 mac-syn realtime enable

Function

The **mac-syn realtime enable** command enables real-time MAC address synchronization.

The **undo mac-syn realtime enable** command disables real-time MAC address synchronization.

By default, real-time MAC address synchronization is disabled.

Format

mac-syn realtime enable { **all** | **slot** *slot-id* }

undo mac-syn realtime enable { **all** | **slot** *slot-id* }

NOTE

This command is supported only on the S6720-EI, S6720S-EI, and S6735-S.

Parameters

Parameter	Description	Value
all	Enables real-time MAC address synchronization in all slots.	-
slot *slot-id*	Enables real-time MAC address synchronization in a specified slot.	The value is an integer and must be the slot ID of a running card.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the device connects to a Linux server through an aggregated link, to ensure that services are not affected in the case of an active/standby link switchover on the server, run the **mac-syn realtime enable** command on the device to enable real-time MAC address synchronization.

Prerequisites

Before running the **mac-syn realtime enable** { **all** | **slot** *slot-id* } command, run the **mac-syn receive enable** { **all** | **slot** *slot-id* } command in the diagnostic view.

Example

# Enable real-time MAC address synchronization.

```
<HUAWEI> system-view
[HUAWEI] mac-syn realtime enable all
```

5.1.53 port bridge enable

Function

The **port bridge enable** command enables the port bridge function on an interface. The interface then can forward packets whose source and destination MAC addresses are both learned by this interface.

The **undo port bridge enable** command disables the port bridge function.

By default, the port bridge function is disabled on an interface.

Format

port bridge enable

undo port bridge enable

Parameters

None

Views

Ethernet interface view, GE interface view, XGE interface view, 40GE interface view, MultiGE interface view, 100GE interface view, Eth-Trunk interface view, port group view, 25GE interface view

Default Level

2: Configuration level

Usage Guidelines

The port bridge function enables an interface to forward packets whose source and destination MAC addresses are both learned on the interface. By default, an interface discards packets whose source and destination MAC addresses are both learned on the interface.

When enabled with the port bridge function, the interface forwards such packets if their destination MAC addresses are found in the MAC address table.

The port bridge function is used in the following scenarios:

- The switch connects to devices that do not support Layer 2 forwarding. When users connected to the devices need to communicate, the devices send user packets to the switch for forwarding. Because source and destination MAC addresses of the packets are learned on the same interface, the port bridge function needs to be enabled on the interface so that the interface can forward such packets.
- The switch is used as an access device in a data center and is connected to servers. For example, take multiple servers hosting multiple virtual machines that need to transmit data to each other. By enabling the port bridge function on the interfaces connected to the servers, you allow the switch to forward data packets between the virtual machines at a higher speed than if the servers perform the switching operations.

Example

# Enable the port bridge function on GigabitEthernet0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface GigabitEthernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] port bridge enable
```

5.1.54 remark destination-mac

Function

The **remark destination-mac** command configures an action of re-marking the destination MAC address in packets in a traffic behavior.

The **undo remark destination-mac** command deletes the configuration.

By default, an action of re-marking the destination MAC address in packets is not configured in a traffic behavior.

NOTE

Only the S6735-S, S6720-EI and S6720S-EI support this command.

Format

remark destination-mac *mac-address*

undo remark destination-mac

Parameters

Parameter	Description	Value
mac-address	Specifies the destination MAC address.	The value is in H-H-H format. An H is a hexadecimal number with 1 to 4 digits. The value must be a unicast MAC address.

Views

Traffic behavior view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can use the **remark destination-mac** command to re-mark the destination MAC address in packets in a traffic behavior so that the downstream device can identify packets and provide differentiated services.

Follow-up Procedure

Run the **traffic policy** command to create a traffic policy and run the **classifier behavior** command in the traffic policy view to bind the traffic classifier to the traffic behavior containing destination MAC address re-marking.

Precautions

- In a traffic behavior, the **remark destination-mac** command cannot be used with the **redirect ip-nexthop** or **redirect ip-multihop** command.
- A traffic policy containing **remark destination-mac** cannot be applied to the outbound direction.
- If you run the **remark destination-mac** command in the same traffic classifier view multiple times, only the latest configuration takes effect.

Example

# Configure the traffic behavior **b1**: The destination MAC address of packets is re-marked to 00e0-fc07-bed3.

```
<HUAWEI> system-view
[HUAWEI] traffic behavior b1
[HUAWEI-behavior-b1] remark destination-mac 00e0-fc07-bed3
```

5.1.55 reset mac-address flapping record

Function

The **reset mac-address flapping record** command clears MAC address flapping records.

Format

reset mac-address flapping record

Parameters

None

Views

All views

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Before collecting MAC address flapping statistics, run the **reset mac-address flapping record** command to clear the current statistics.

Precautions

This command deletes only the historical MAC address flapping records that have been aged.

After clearing MAC address flapping records, you can run the **display mac-address flapping record** command to view current MAC address flapping records.

The cleared MAC address flapping records cannot be restored.

Example

# Clear MAC address flapping records.

```
<HUAWEI> reset mac-address flapping record
```

5.1.56 undo mac-address

Function

The **undo mac-address** command deletes one or more MAC address entries.

Format

undo mac-address [**all** | **dynamic**] [*interface-type interface-number* | **vlan** *vlan-id*] *

undo mac-address { **all** | **dynamic** } [**vsi** *vsi-name*]

undo mac-address *mac-address* [**vlan** *vlan-id* | **vsi** *vsi-name*]

Parameters

Parameter	Description	Value
mac-address	Specifies the MAC address in a MAC address entry to be deleted.	The value is in H-H-H format. An H is a hexadecimal number of 1 to 4 digits. The MAC address cannot be FFFF-FFFF-FFFF, 0000-0000-0000, or a multicast MAC address.
interface-type interface-number	Specifies the interface in a MAC address entry to be deleted.	-
vlan *vlan-id*	Specifies the VLAN ID in a MAC address entry to be deleted.	The value is an integer that ranges from 1 to 4094.
all	Specifies that all MAC address entries excluding DHCP sticky MAC address entries, sticky-config MAC address and NAC MAC address entries are deleted.	-
vsi *vsi-name*	Specifies the name of a VSI. The VSI must have been created. **NOTE** Only the S5731-H, S5731S-H, S5732-H, S5731-S, S5731S-S, S6730-S, S6730S-S, S6735-S, S6720-EI, S6720S-EI, S6730S-H, and S6730-H support this parameter.	-
dynamic	Deletes dynamic MAC address entries, that is, MAC address entries learned by an interface.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A MAC address table saves a limited number of MAC addresses. If the MAC address table is full, the device cannot learn new MAC address entries until old MAC addresses are aged out. Packets matching no MAC address entry are broadcast, wasting bandwidth resources. This command can delete useless MAC address entries to release the MAC address table space.

You can delete some of MAC address entries as required. For example:

- If you do not specify *interface-type interface-number*, the command deletes MAC address entries of the specified type on all interfaces.
- If you do not specify **vlan** *vlan-id*, the command deletes MAC address entries of the specified type in all VLANs.

Precautions

If port security and NAC authentication are enabled on an interface and a user is successfully authenticated on the interface and connects to the network, the **undo mac-address** command cannot delete MAC address entries of the user. For the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S, if **authentication mode** is used to set the user access mode to multi-share, the **undo mac-address** command can delete MAC address entries of the user.

MAC address entries of the sticky-config type cannot be deleted through the **undo mac-address** command, and can be deleted only through the **undo port-security mac-address sticky-config** command.

Example

# Delete all MAC address entries.

```
<HUAWEI> system-view
[HUAWEI] undo mac-address all
```

# Delete all dynamic MAC address entries.

```
<HUAWEI> system-view
[HUAWEI] undo mac-address dynamic
```

# Delete all MAC address entries on gigabitethernet0/0/1.

```
<HUAWEI> system-view
[HUAWEI] undo mac-address gigabitethernet 0/0/1
```

# Delete all MAC address entries in VLAN 5.

```
<HUAWEI> system-view
[HUAWEI] undo mac-address vlan 5
```

# Delete all dynamic MAC address entries in the VSI **a2**.

```
<HUAWEI> system-view
[HUAWEI] undo mac-address dynamic vsi a2
```

# Delete all MAC address entries in which the MAC address is 00e0-fc04-0004.

```
<HUAWEI> system-view
[HUAWEI] undo mac-address 00e0-fc04-0004
```

5.1.57 undo mac-address temporary

Function

The **undo mac-address temporary** command deletes all the temporary MAC address entries in the system.

Format

undo mac-address temporary

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

When the interface card is pulled out, the static MAC address entries configured on the interfaces are reserved as temporary MAC address entries. After the interface card is plugged again, the static MAC address entries are restored.

If the interface card is not plugged after being pulled out, the temporary MAC address entries become unnecessary and occupy the system resources. In this case, you can run the **undo mac-address temporary** command to delete all the temporary MAC address entries in the system.

Example

# Delete all the temporary MAC address entries in the system.

```
<HUAWEI> system-view
[HUAWEI] undo mac-address temporary
```

5.1.58 undo mac-limit all

Function

The **undo mac-limit all** command deletes all MAC address limiting rules.

Format

undo mac-limit all

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

This command deletes all the rules configured by the **mac-limit** command.

Precautions

Before using this command, run the **display mac-limit** command to check the MAC address limiting rules and confirm your operation.

Example

# Delete all MAC address limiting rules.

```
<HUAWEI> system-view
[HUAWEI] undo mac-limit all
```

5.2 Link Aggregation Commands

5.2.1 Command Support

Commands provided in this section and all the parameters in the commands are supported by all switch models (except the S5731-L and S5731S-L), unless otherwise specified. For details, see specific commands.

5.2.2 authentication-mode (E-Trunk view)

Function

The **authentication-mode** command configures the E-Trunk authentication and encryption mode.

The **undo authentication-mode** command restores the default E-Trunk authentication and encryption mode.

By default, the E-Trunk authentication and encryption mode is hmac-sha1.

NOTE

Only the S5720I-SI, S5735-S, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6720S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Format

authentication-mode { **hmac-sha1** | **hmac-sha256** | **enhanced-hmac-sha256** }

undo authentication-mode

Parameters

Parameter	Description	Value
hmac-sha1	Indicates that the E-Trunk authentication and encryption mode is hmac-sha1.	-
hmac-sha256	Indicates that the E-Trunk authentication and encryption mode is hmac-sha256. NOTE **hmac-sha256** is more secure than **hmac-sha1**, so you are advised to configure **hmac-sha256** as the E-Trunk authentication and encryption mode.	-
enhanced-hmac-sha256	Indicates that the E-Trunk authentication and encryption mode is **enhanced-hmac-sha256**. NOTE **enhanced-hmac-sha256** is more secure than **hmac-sha256** and **hmac-sha1**, so you are advised to configure **enhanced-hmac-sha256** as the E-Trunk authentication and encryption mode.	-

Views

E-Trunk view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To improve system security, run the **authentication-mode** command to configure the E-Trunk authentication and encryption mode.

Precautions

Two devices in an E-Trunk must have the same E-Trunk authentication and encryption mode.

Example

# Configure the E-Trunk authentication and encryption mode as **enhanced-hmac-sha256**.

```
<HUAWEI> system-view
```

```
[HUAWEI] e-trunk 1
[HUAWEI-e-trunk-1] authentication-mode enhanced-hmac-sha256
```

5.2.3 assign trunk

Function

The **assign trunk** command sets the maximum number of link aggregation groups (LAGs) and the maximum number of member interfaces in each LAG.

The **undo assign trunk** command restores the default maximum number of LAGs and the default maximum number of member interfaces in each LAG.

Table 5-16 describes the default maximum numbers of LAGs and member interfaces in each LAG on a device.

Table 5-16 Default maximum numbers of LAGs and member interfaces in each LAG

Model	Default Maximum Number of LAGs	Default Maximum Number of Member Interfaces in each LAG
S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S	128	32
S6735-S, S6720-EI and S6720S-EI	128	8

NOTE

This command is supported only on the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, S6730S-S, S6720-EI and S6720S-EI.

Format

assign trunk { **trunk-group** *group-number* | **trunk-member** *member-number* }*

undo assign trunk

Parameters

Parameter	Description	Value
trunk-group*group-number*	Specifies the number of LAGs.	The value is an integer ranging 32 to 512 for the S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S, and 32 to 128 for other models. The value multiplied by *member-number* cannot exceed 2048 on the S6735-S, S6720-EI and S6720S-EI. The value multiplied by *member-number* cannot exceed 8192 on the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S.
trunk-member*member-number*	Specifies the maximum number of member interfaces in each LAG.	The value is an integer that can be 8, 16, 32, or 64.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In most cases, a switch supports a fixed maximum number of LAGs and a fixed maximum number of member interfaces in each LAG. On the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, S6730S-S, S6735-S, S6720-EI, and S6720S-EI, you can run the **assign trunk** command to set the maximum number of LAGs and the maximum number of member interfaces in each LAG, implementing flexible networking and meeting various service requirements.

Precautions

- By default, if the value of *member-number* configured for an Eth-Trunk using the **assign trunk** { **trunk-group** *group-number* | **trunk-member** *member-number* }* command is larger than or equal to 16 on the S6735-S, S6720-EI and S6720S-EI or larger than 32 on the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S, known unicast packets are load balanced using the enhanced mode, and broadcast, unknown-unicast, and multicast (BUM) packets are load balanced based on their source and destination MAC addresses. Known unicast packets must be load balanced using the enhanced mode (the load balancing mode can be configured using the **load-balance** command). Otherwise, packet loss or uneven load balancing may occur.

- After the Eth-Trunk specifications are modified, save the configuration and restart the switch to make the modification take effect.
- If you use the **assign trunk** command to modify Eth-Trunk specifications, the existing Eth-Trunk configuration will become invalid or be lost. Exercise caution when you run the **assign trunk** command. When the configured Eth-Trunk specifications are reduced and the Eth-Trunks that exceed the specifications are configured, the configuration of excess Eth-Trunks is invalid.
- If an Eth-Trunk interface has been created on a switch and you want to expand the Eth-Trunk specifications, you need to run the **load-balance enhanced profile** command to configure an enhanced load balancing profile for all Eth-Trunks first. After Eth-Trunk specifications are expanded, you are advised not to delete the configured enhanced load balancing profile because this operation will cause uneven load balancing.
- After the **reset netconf db-configuration** or **reset saved-configuration** command is run, the **assign trunk** command configuration is cleared, that is, the default configuration is restored.

Example

# Set the maximum number of LAGs to 64 and the maximum number of member interfaces in each LAG to 16.

```
<HUAWEI> system-view
[HUAWEI] assign trunk trunk-group 64 trunk-member 16
```

5.2.4 collect forward-path

Function

The **collect forward-path** command configures the device to collect traffic information.

The **undo collect forward-path** command configures the device not to collect traffic information.

By default, the device does not collect traffic information.

NOTE

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

Format

collect forward-path { { **sip** *source-ip-address* **dip** *destination-ip-address* [**sport** *source-port* **dport** *destination-port* [**protocol** { *protocol-number* | **gre** | **icmp** | **igmp** | **ip** | **ipinip** | **ospf** | **tcp** | **udp** }]] } | { **smac** *source-mac-address* | **dmac** *dest-mac-address* | **vlan** *vlan-id* | **l2-protocol** { *protocol-value* | **arp** | **ip** | **ipv6** | **mpls** | **rarp** } } * } { **ingress** | **egress** | **both** } [**interval** *interval-time*]

undo collect forward-path { { **sip** *source-ip-address* **dip** *destination-ip-address* [**sport** *source-port* **dport** *destination-port* [**protocol** { *protocol-number* | **gre** | **icmp** | **igmp** | **ip** | **ipinip** | **ospf** | **tcp** | **udp** }]] } | { **smac** *source-mac-address* | **dmac** *dest-mac-address* | **vlan** *vlan-id* | **l2-protocol** { *protocol-value* | **arp** | **ip** | **ipv6** | **mpls** | **rarp** } } * } { **ingress** | **egress** | **both** } [**interval** *interval-time*]

Parameters

Parameter	Description	Value
sip *source-ip-address*	Specifies the source IP address.	The value is in dotted decimal notation.
dip *destination-ip-address*	Specifies the destination IP address.	The value is in dotted decimal notation.
sport *source-port*	Specifies the source port number.	The value is an integer that ranges from 0 to 65535.
dport *destination-port*	Specifies the destination port number.	The value is an integer that ranges from 0 to 65535.
protocol { *protocol-number* | **gre** | **icmp** | **igmp** | **ip** | **ipinip** | **ospf** | **tcp** | **udp** }	Specifies the protocol number or type. ● *protocol-number* specifies the protocol number. ● **gre** indicates that the protocol type is GRE. ● **icmp** indicates that the protocol type is ICMP. ● **igmp** indicates that the protocol type is IGMP. ● **ip** indicates that the protocol type is IP. ● **ipinip** indicates that the protocol type is IPinIP. ● **ospf** indicates that the protocol type is OSPF. ● **tcp** indicates that the protocol type is TCP. ● **udp** indicates that the protocol type is UDP.	The value of *protocol-number* is an integer that ranges from 1 to 255.

Parameter	Description	Value
smac *source-mac-address*	Specifies the source MAC address.	The value is in hexadecimal notation.
dmac *dest-mac-address*	Specifies the destination MAC address.	The value is in hexadecimal notation.
vlan *vlan-id*	Specifies the ID of a VLAN.	The value is an integer that ranges from 1 to 4094.
l2-protocol { *protocol-value* | **arp** | **ip** | **ipv6** | **mpls** | **rarp** }	Specifies the Layer 2 protocol number or type. ● *protocol-value* specifies the protocol number. ● **arp** indicates that the protocol type is ARP and the protocol number is 0x0806. ● **ip** indicates that the protocol type is IP and the protocol number is 0x0800. ● **ipv6** indicates that the protocol type is IPv6 and the protocol number is 0x86dd. ● **mpls** indicates that the protocol type is MPLS and the protocol number is 0x8847. ● **rarp** indicates that the protocol type is RARP and the protocol number is 0x8035.	The value of *protocol-value* is in hexadecimal notation and must start with 0x. The value contains three or six digits.
ingress	Indicates the inbound direction.	-
egress	Indicates the outbound direction.	-
both	Indicates the inbound and outbound directions.	-

Parameter	Description	Value
interval *interval-time*	Indicates the collection duration.	The value is an integer that ranges from 0 to 1440, in minutes. The default value is 10. The value 0 indicates that the device continuously collects inbound and outbound interfaces and traffic information in packets with 5-tuple information.

Views

User view, System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The packet information contains the source and destination IP addresses, source and destination port numbers, source and destination MAC addresses, and protocol type. Traffic transmitted on each device interface contains different information. You can run this command to configure the device to collect traffic information, which helps you locate faults and understand the traffic forwarding path.

Precautions

The device can collect inbound and outbound interfaces and traffic information of a maximum of 8 flows.

In the outbound direction, traffic information collection (with the **egress** or **both** parameter specified) conflicts with a traffic policy or simplified traffic policy. If traffic information collection, traffic policy, or simplified traffic policy are configured, one of them may not take effect.

When the device restarts or an active/standby switchover occurs in a CSS, the collection information and report configured by the **collect forward-path** command will be deleted.

If traffic information collection is no longer required after the collection time ends, run the **undo collect forward-path** command to disable the device from collecting traffic information.

After the **undo collect forward-path** command is run, the collected traffic statistics will be deleted.

If commands for collecting statistics on traffic with the same packet information are configured and the directions in two consecutive commands are the same or overlap, only the previous command takes effect. Examples are as follows:

- Scenarios where **collect forward-path sip 10.1.1.1 dip 10.2.2.2 ingress interval 20** and **collect forward-path sip 10.1.1.1 dip 10.2.2.2 ingress interval 30** are configured in sequence: The **collect forward-path sip 10.1.1.1 dip 10.2.2.2 ingress interval 30** command does not take effect.
- Scenarios where **collect forward-path sip 10.1.1.1 dip 10.2.2.2 ingress** and **collect forward-path sip 10.1.1.1 dip 10.2.2.2 both** are configured in sequence: The **collect forward-path sip 10.1.1.1 dip 10.2.2.2 both** command does not take effect.
- Scenarios where **collect forward-path sip 10.1.1.1 dip 10.2.2.2 both** and **collect forward-path sip 10.1.1.1 dip 10.2.2.2 ingress** are configured in sequence: The **collect forward-path sip 10.1.1.1 dip 10.2.2.2 ingress** command does not take effect.

Example

# Configure the device to collect traffic information with source IP address 10.1.1.1 and destination IP address 10.2.2.2.

```
<HUAWEI> system-view
[HUAWEI] collect forward-path sip 10.1.1.1 dip 10.2.2.2 both
```

5.2.5 display eth-trunk

Function

The **display eth-trunk** command displays the Eth-Trunk configuration.

Format

display eth-trunk [*trunk-id* [**interface** *interface-type interface-number* | **verbose**]]

Parameters

Parameter	Description	Value
trunk-id	Specifies the ID of an Eth-Trunk.	The value is an integer. The value varies according to device model: ● SS1720GW-E, S1720GWR-E, S2730S-S, S5720I-SI, S5720-LI, and S5720S-LI: 0-119 ● S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735-S-I, S5735S-S, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S: 0-127 ● S5735S-H, S5736-S, S6720S-S: 0-249 On the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, S6730S-S, S6735-S, S6720-EI, and S6720S-EI, you can run the **assign trunk** command to set the value, and run the **display trunk configuration** command to check the configuration.
interface *interface-type interface-number*	Specifies a member interface. *interface-type* specifies the type of the member interface. *interface-number* specifies the number of the member interface.	-
verbose	Displays the detailed configuration of a specified Eth-Trunk, including the Eth-Trunk traffic statistics.	-

Views

All views

Default Level

1 : Monitoring level

Usage Guidelines

Usage Scenario

After configuring an Eth-Trunk on a device, you can run the **display eth-trunk** command to check whether the Eth-Trunk configuration is correct.

When using the **display eth-trunk** command, pay attention to the following points:

- If no parameter is specified, the **display eth-trunk** command displays the configurations of all Eth-Trunks.
- If only *trunk-id* is specified, the **display eth-trunk** command displays the configuration of a specified Eth-Trunk.
- If *trunk-id* and **interface** *interface-type interface-number* are specified, the configuration of member interfaces of the specified Eth-Trunk is displayed.
- If *trunk-id* is specified and **verbose** is configured, the **display eth-trunk** command displays detailed configuration of a specified Eth-Trunk, including the Eth-Trunk traffic statistics.

Prerequisites

The Eth-Trunk has been correctly configured. If no Eth-Trunk is configured, when you run this command, the system displays an error message.

Precautions

If there are traffic statistics about many Eth-Trunks, you are advised to specify *trunk-id* or **interface** *interface-type interface-number* to filter output information. Otherwise, the following problems may occur due to excessive output information:

- The displayed information is repeatedly updated, and required information cannot be located.
- The system does not respond because of long-time information traverse and search.

Example

# Display the configurations of all Eth-Trunks.

```
<HUAWEI> display eth-trunk
Eth-Trunk10's state information is:
Local:
LAG ID: 10                  WorkingMode: LACP
Preempt Delay Time: 10      Hash arithmetic: According to SIP-XOR-DIP
System Priority: 120        System ID: 0018-82d4-04c3
Least Active-linknumber: 1  Max Active-linknumber: 2
Operate status: up          Number Of Up Port In Trunk: 2
--------------------------------------------------------------------------------
ActorPortName               Status   PortType     PortPri PortNo PortKey PortState Weight
GigabitEthernet0/0/2         Selected 1GE         10      262    2609    10111100  1
GigabitEthernet0/0/3         Selected 1GE         10      263    2609    10111100  1
GigabitEthernet0/0/4         Unselect 1GE         32768   264    2609    10100000  1

Partner:
--------------------------------------------------------------------------------
ActorPortName               SysPri  SystemID    PortPri PortNo  PortKey   PortState
GigabitEthernet0/0/2         32768  00e0-fc6e-bb11  32768  262   2609      10111100
GigabitEthernet0/0/3         32768  00e0-fc6e-bb11  32768  263   2609      10111100
GigabitEthernet0/0/4         32768  00e0-fc6e-bb11  32768  264   2609      10110000
```

```
Eth-Trunk11's state information is:
WorkingMode: NORMAL         Hash arithmetic: According to SIP-XOR-DIP
Least Active-linknumber: 1  Max Bandwidth-affected-linknumber: 8
Operate status: up          Number Of Up Port In Trunk: 1
--------------------------------------------------------------------------------
PortName                              Status      Weight
GigabitEthernet0/0/1                     Up          1
```

# Display the configuration of Eth-Trunk 11 in manual load balancing mode.

```
<HUAWEI> display eth-trunk 11
Eth-Trunk11's state information is:
WorkingMode: NORMAL         Hash arithmetic: According to SIP-XOR-DIP
Least Active-linknumber: 1  Max Bandwidth-affected-linknumber: 8
Operate status: up          Number Of Up Port In Trunk: 1
--------------------------------------------------------------------------------
PortName                              Status      Weight
GigabitEthernet0/0/1                     Up          1
```

# Display the configuration of Eth-Trunk 10 in LACP mode.

```
<HUAWEI> display eth-trunk 10
Eth-Trunk10's state information is:
Local:
LAG ID: 10                  WorkingMode: LACP
Preempt Delay Time: 10      Hash arithmetic: According to SIP-XOR-DIP
System Priority: 120        System ID: 0018-82d4-04c3
Least Active-linknumber: 1  Max Active-linknumber: 2
Operate status: up          Number Of Up Port In Trunk: 2
--------------------------------------------------------------------------------
ActorPortName                  Status   PortType     PortPri PortNo PortKey PortState Weight
GigabitEthernet0/0/2            Selected 1GE          10      262    2609    10111100  1
GigabitEthernet0/0/3            Selected 1GE          10      263    2609    10111100  1
GigabitEthernet0/0/4            Unselect 1GE          32768   264    2609    10100000  1

Partner:
--------------------------------------------------------------------------------
ActorPortName                  SysPri    SystemID  PortPri PortNo  PortKey   PortState
GigabitEthernet0/0/2            32768  00e0-fc6e-bb11  32768  262   2609      10111100
GigabitEthernet0/0/3            32768  00e0-fc6e-bb11  32768  263   2609      10111100
GigabitEthernet0/0/4            32768  00e0-fc6e-bb11  32768  264   2609      10110000
```

# Display the detailed configuration of Eth-Trunk 11 in manual load balancing mode.

```
<HUAWEI> display eth-trunk 11 verbose
Eth-Trunk11's state information is:
WorkingMode: NORMAL         Hash arithmetic: According to SIP-XOR-DIP
Least Active-linknumber: 1  Max Bandwidth-affected-linknumber: 8
Operate status: up          Number Of Up Port In Trunk: 1
--------------------------------------------------------------------------------
PortName                              Status      Weight
GigabitEthernet0/0/1                     Up          1

Flow statistic
 Interface GigabitEthernet0/0/1,
    Last 300 seconds input rate 0 bits/sec, 0 packets/sec
    Last 300 seconds output rate 0 bits/sec, 0 packets/sec
    0 packets input, 0 bytes, 0 drops
    0 packets output, 0 bytes, 0 drops
 Interface Eth-Trunk11
    Last 300 seconds input rate 0 bits/sec, 0 packets/sec
    Last 300 seconds output rate 0 bits/sec, 0 packets/sec
    0 packets input, 0 bytes, 0 drops
    0 packets output, 0 bytes, 0 drops
```

# Display the detailed configuration of Eth-Trunk 10 in LACP mode.

```
<HUAWEI> display eth-trunk 10 verbose
Eth-Trunk10's state information is:
Local:
```

```
LAG ID: 10                 WorkingMode: LACP
Preempt Delay Time: 10      Hash arithmetic: According to SIP-XOR-DIP
System Priority: 120        System ID: 0018-82d4-04c3
Least Active-linknumber: 1  Max Active-linknumber: 2
Operate status: up          Number Of Up Port In Trunk: 2
--------------------------------------------------------------------------------
ActorPortName                Status   PortType     PortPri PortNo PortKey PortState Weight
GigabitEthernet0/0/2          Selected 1GE          10      262    2609    10111100  1
GigabitEthernet0/0/3          Selected 1GE          10      263    2609    10111100  1
GigabitEthernet0/0/4          Unselect 1GE          32768   264    2609    10100000  1

Partner:
--------------------------------------------------------------------------------
ActorPortName                SysPri    SystemID  PortPri PortNo  PortKey   PortState
GigabitEthernet0/0/2          32768  00e0-fc6e-bb11  32768  262   2609      10111100
GigabitEthernet0/0/3          32768  00e0-fc6e-bb11  32768  263   2609      10111100
GigabitEthernet0/0/4          32768  00e0-fc6e-bb11  32768  264   2609      10110000

Flow statistic
 Interface GigabitEthernet0/0/2,
   Last 300 seconds input rate 32 bits/sec, 0 packets/sec
   Last 300 seconds output rate 32 bits/sec, 0 packets/sec
   148 packets input, 18944 bytes, 0 drops
   246 packets output, 31488 bytes, 0 drops
 Interface GigabitEthernet0/0/3,
   Last 300 seconds input rate 32 bits/sec, 0 packets/sec
   Last 300 seconds output rate 32 bits/sec, 0 packets/sec
   147 packets input, 18816 bytes, 0 drops
   246 packets output, 31488 bytes, 0 drops
 Interface GigabitEthernet0/0/4,
   Last 300 seconds input rate 56 bits/sec, 0 packets/sec
   Last 300 seconds output rate 48 bits/sec, 0 packets/sec
   144 packets input, 18432 bytes, 0 drops
   174 packets output, 22272 bytes, 0 drops
 Interface Eth-Trunk10
   Last 300 seconds input rate 96 bits/sec, 0 packets/sec
   Last 300 seconds output rate 96 bits/sec, 0 packets/sec
   439 packets input, 56192 bytes, 0 drops
   666 packets output, 85248 bytes, 0 drops
```

Table 5-17 Description of the **display eth-trunk** command output

Item	Description
Local	Configuration of the local Eth-Trunk.
LAG ID	ID of the Eth-Trunk.
WorkingMode	Working mode of the Eth-Trunk: ● NORMAL: manual load balancing mode ● LACP: LACP mode
Preempt Delay Time	Preemption delay time: ● If LACP preemption is enabled, the preemption time is displayed and expressed in seconds. ● If LACP preemption is disabled, the value is displayed as Disabled.

Item	Description
Hash arithmetic	Hash algorithm used for load balancing among member interfaces of the Eth-Trunk. The hash algorithm is configured by using the **load-balance** command. The SS1720GW-E, S1720GWR-E, S5720I-SI, S5720-LI, S5720S-LI, S5735S-H, S5736-S, and S6720S-S use the **src-dst-ip**, source TCP or UDP port number, and destination TCP or UDP port number in the hash algorithm for load balancing regardless of whether you configure this parameter.
SysPri	System LACP priority. To configure the LACP system priority, run the **lacp priority** command.
SystemID	System ID.
Least Active-linknumber	Minimum number of active member links in Up state. To configure the minimum number of active member links in Up state, run the **least active-linknumber** command.
Max Active-linknumber	Maximum number of active member links in Up state. To configure the maximum number of active member links in Up state, run the **max active-linknumber** command.
Max Bandwidth-affected-linknumber	Maximum number of connections that affect the Eth-Trunk bandwidth.
Operate status	Eth-Trunk status: ● UP ● DOWN
Number Of Up Port In Trunk	Number of member interfaces in Up state in the Eth-Trunk.
ActorPortName	Name of a member interface.

Item	Description
Status	Status of the local member interface in LACP mode: ● Selected: A member interface in Selected state is active. ● Unselect: A member interface in Unselected state is inactive. ● ForceFwd: A member interface can forward Layer 2 traffic. Status of the local member interface in manual load balancing mode: ● Up: indicates that the interface is properly started. ● Down: indicates that the interface is faulty.
PortType	Type of the local member interface.
PortPri	LACP priority of the member interface.
PortNo	Number of the member interface in LACP mode.
PortKey	Key value of the member interface in LACP mode.

Item	Description
PortState	Status variable of the member interface. The status variable is eight bits, such as 10111100. The descriptions of each bit are as follows: ● Bit 1: Whether the member interface is an Actor. This bit has a fixed value 1. ● Bit 2: Whether the member interface uses a long or short timeout interval to receive LACPDUs. 1: The member interface uses a short timeout interval. 0: The member interface uses a long timeout interval. By default, an Eth-Trunk member interface uses the long timeout interval (90s) to receive LACPDUs. To set the timeout interval, run the **lacp timeout** command. ● Bit 3: Whether the system allows the member interface to be aggregated. 1: The system allows the member interface to be aggregated. 0: The system does not allow the member interface to be aggregated. ● Bit 4: Whether the member interface is added to the link aggregation group (LAG). 1: The member interface is added to the LAG. 0: The member interface is not added to the LAG. ● Bit 5: Whether the member interface can receive LACPDUs. 1: The member interface can receive LACPDUs. 0: The member interface cannot receive LACPDUs. ● Bit 6: Whether the member interface can send LACPDUs. 1: The member interface can send LACPDUs. 0: The member interface cannot send LACPDUs. ● Bit 7: Whether the LACPDUs contain default parameter values.

Item	Description
	1: The LACPDUs contain default parameter values. 0: The LACPDUs do not contain default parameter values. ● Bit 8: Whether the receive state machine of the Actor is in Expired state. 1: The receive state machine of the Actor is in Expired state. 0: The receive state machine of the Actor is not in Expired state.
Weight	Weight of the member interface.
Partner	Information about member interfaces of the remote Eth-Trunk. The Eth-Trunk must work in LACP mode.
Flow statistic	Eth-Trunk traffic statistics.
Last 300 seconds input/output rate	Rates for sending and receiving bits and packets on the interface in the last 300 seconds.
input/output	Number of packets received or sent by the interface.
packets	Total number of packets that the interface receives or sends.
bytes	Total number of bytes that the interface receives or sends.
drops	Number of packets that the interface drops.

5.2.6 display trunk configuration

Function

The **display trunk configuration** command displays the maximum number of LAGs and the maximum number of member interfaces in each LAG.

NOTE

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

Format

display trunk configuration

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

To facilitate flexible networking, run the **assign trunk** command to set the maximum number of LAGs and the maximum number of member interfaces in each LAG. You can run the **display trunk configuration** command to view the configuration.

Example

# Display the maximum number of LAGs and the maximum number of member interfaces in each LAG.

```
<HUAWEI> display trunk configuration
--------------------------------------------------
Item           Default    Current    Configured
--------------------------------------------------
trunk-group     128        64         64
trunk-member     8          16         16
--------------------------------------------------
```

Table 5-18 Description of the **display trunk configuration** command output

Item	Description
Item	The name of item.
Default	Default Eth-Trunk specifications supported by the device.
Current	Current Eth-Trunk specifications supported by the device.
Configured	Configured Eth-Trunk specifications. If the configured Eth-Trunk specifications are different from the current Eth-Trunk specifications, the configured Eth-Trunk specifications take effect after the device restarts. To specify the parameter, run the **assign trunk** command.
trunk-group	Maximum number of Eth-Trunks supported by the device.
trunk-member	Maximum number of member interfaces in each Eth-Trunk.

5.2.7 display eth-trunk load-balance

Function

The **display eth-trunk load-balance** command displays the load balancing mode of an Eth-Trunk.

Format

display eth-trunk [*trunk-id*] **load-balance**

Parameters

Parameter	Description	Value
trunk-id	Displays the load balancing mode of a specified Eth-Trunk. *trunk-id* specifies the ID of the Eth-Trunk.	The value is an integer. The value varies according to device model: ● SS1720GW-E, S1720GWR-E, S2730S-S, S5720I-SI, S5720-LI, and S5720S-LI: 0-119 ● S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735-S-I, S5735S-S, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S: 0-127 ● S5735S-H, S5736-S, S6720S-S: 0-249 On the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, S6730S-S, S6735-S, S6720-EI, and S6720S-EI, you can run the **assign trunk** command to set the value, and run the **display trunk configuration** command to check the configuration.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After the load balancing mode of an Eth-Trunk is configured, you can run this command to view the load balancing mode of the Eth-Trunk. If *trunk-id* is not specified, the load balancing modes of all Eth-Trunks are displayed.

Example

# Display the load balancing mode of Eth-Trunk 1.

```
<HUAWEI> display eth-trunk 1 load-balance
Eth-Trunk1's load-balance information:
 Load-balance Configuration: SIP-XOR-DIP
 Load-balance options used per-protocol:
  L2  : Source XOR Destination MAC address, Vlan ID, Ethertype, Ingress-port
  IPv4: Source XOR Destination IP address, Source XOR Destination TCP/UDP port
  IPv6: Source XOR Destination IP address, Source XOR Destination TCP/UDP port
  MPLS: Source XOR Destination IP address, Source XOR Destination TCP/UDP port
```

Table 5-19 Description of the **display eth-trunk load-balance** command output

Item	Description
Load-balance Configuration	Configured load balancing mode. The options are as follows: ● SIP: Eth-Trunk load balancing based on source IP addresses. ● DIP: Eth-Trunk load balancing based on destination IP addresses. ● SIP-XOR-DIP: Eth-Trunk load balancing based on source and destination IP addresses. ● SA: Eth-Trunk load balancing based on source MAC addresses. ● DA: Eth-Trunk load balancing based on destination MAC addresses. ● SA-XOR-DA: Eth-Trunk load balancing based on source and destination MAC addresses. ● ENHANCED: Enhanced Eth-Trunk load balancing. The SS1720GW-E, S1720GWR-E, S5720I-SI, S5720-LI, S5720S-LI, S5735S-H, S5736-S, and S6720S-S use the **src-dst-ip**, source TCP or UDP port number, and destination TCP or UDP port number in the hash algorithm for load balancing regardless of whether you configure this parameter.
Unicast load-balance enhanced mode **NOTE** This information is displayed only when the load balancing mode is set to ENHANCED.	Whether traffic is load balanced based on the inner IP address, outer IP address, or both. ● outer: Traffic is load balanced based on the outer IP address. ● inner: Traffic is load balanced based on the inner IP address. ● inner and outer: Traffic is load balanced based on both the inner and outer IP addresses.
Load-balance enhanced profile **NOTE** This information is displayed only when the load balancing mode is set to ENHANCED.	Name of a load balancing profile.

Item	Description
Load-balance options used per-protocol	Load balancing parameters of different types of packets.

5.2.8 display e-trunk

Function

The **display e-trunk** command displays E-Trunk information.

Format

display e-trunk { **brief** | *e-trunk-id* }

NOTE

Only the S5720I-SI, S5735-S, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6720S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Parameters

Parameter	Description	Value
brief	Displays brief E-Trunk information.	-
e-trunk-id	Specifies the ID of an E-Trunk.	The value is an integer that ranges from 1 to 16.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After an E-Trunk is configured, you can run the **display e-trunk** command to view information about the E-Trunk.

Example

# Display information about E-Trunk 1.

```
<HUAWEI> display e-trunk 1
                         The E-Trunk information
E-TRUNK-ID : 1                         Revert-Delay-Time (s) : 120
```

```
Priority : 10                    System-ID : 00e0-fc12-3456
Peer-IP : 10.1.1.2                 Source-IP : 10.1.1.1
State : Master                     Causation : TIMEOUT
Send-Period (100ms) : 10                Fail-Time (100ms) : 200
Receive : 1                      Send : 1006
RecDrop : 0                        SndDrop : 0
Peer-Priority : -                 Peer-System-ID : -
Peer-Fail-Time (100ms) : -             BFD-Session : 1
Description : -
Sequence : Enable
-------------------------------------------------------------------------------
                          The Member information
Type      ID  LocalPhyState  Work-Mode     State   Causation        Remote-
ID
Eth-Trunk 10  Up            auto          Master  ETRUNK_INIT      17
```

Table 5-20 Description of the **display e-trunk** command output

Item	Description
E-TRUNK-ID	E-Trunk ID. To specify the parameter, run the **e-trunk** command.
Revert-Delay-Time	Revertive switching delay of the E-Trunk. To specify the parameter, run the **timer revert delay** command.
Priority	Priority of the E-Trunk. To specify the parameter, run the **priority** command.
System-ID	System ID of the local end. To specify the parameter, run the **lacp e-trunk system-id** command.
Peer-IP/Source-IP	Local and remote IP addresses of the E-Trunk. To specify the parameter, run the **peer-address source-address** command.
State	E-Trunk status: ● 1: Init ● 2: Backup ● 3: Master

Item	Description
Causation	E-Trunk status change cause: ● PRI(1): The E-Trunk status is determined by the E-Trunk priority. ● TIMEOUT(2): The local device changes from the backup to the master because it does not receive hello packets from the remote device within the timeout interval. ● BFD_DOWN(3): The BFD session on the local device detects that the link between the local device and the remote device is Down. ● PEER_TIMEOUT(4): The remote device changes from the backup to the master because it does not receive hello packets from the local device within the timeout interval. ● PEER_BFD_DOWN(5): The BFD session on the remote device detects that the link between the local device and the remote device is Down. ● ALL_MEMBER_DOWN(6): Both the two member devices of the E-Trunk are Down. ● INIT(7): The E-Trunk is being initialized.
Send-Period	Interval for sending hello packets. To specify the parameter, run the **timer hello** command.
Fail-Time	Timeout interval for the E-Trunk to receive packets. To specify the parameter, run the **timer hold-on-failure multiplier** command.
Receive/Send	Number of packets received and sent by the E-Trunk.
RecDrop/SndDrop	Number of received and sent packets discarded by the E-Trunk.
Peer-Priority	Priority of the remote device.
Peer-System-ID	System MAC address of the remote device.
Peer-Fail-Time	Timeout interval of the remote device.
BFD-Session	BFD session bound to the E-Trunk. To specify the parameter, run the **e-trunk track bfd-session** command.
Description	Description of the E-Trunk.

Item	Description
Sequence	E-Trunk sequence number check function status: ● Enable ● Disable You can run the **sequence enable** command in the E-Trunk view to configure the E-Trunk sequence number check function or modify its state.
Type	Member type. The value is Eth-Trunk.
ID	Member ID. To add Eth-Trunks with different IDs on two devices to the same E-Trunk, run the **e-trunk** *e-trunk-id* **remote-eth-trunk** *eth-trunk-id* command on the Eth-Trunk interface view of the two devices to specify remote Eth-Trunk IDs to ensure that the E-Trunk works properly.
LocalPhyState	Physical status of a member link: ● 1: Up ● 2: Down
Work-Mode	Working mode of a member interface: ● 1: auto ● 2: force-backup ● 3: force-master To specify the parameter, run the **e-trunk mode** command.
State	Status of a member interface: ● 1: Master ● 2: Backup

Item	Description
Causation	Cause for the member interface status change: ● FORCE_BACKUP(1): The member interface is forcibly to work in backup state. ● FORCE_MASTER(2): The member interface is forcibly to work in master state. ● ETRUNK_INIT(3): The member interface works in automatic state but the E-Trunk is being initialized. ● ETRUNK_BACKUP(4): The member interface works in automatic state but the E-Trunk is in backup state. ● ETRUNK_MASTER(5): The member interface works in automatic state but the E-Trunk is in master state. ● PEER_MEMBER_DOWN(6): The remote device is Down. ● PEER_MEMBER_UP(7): The remote device is Up. ● NO_PEER_MEMBER(8): There is no remote device.
Remote-ID	Eth-Trunk ID of the remote device.

5.2.9 display e-trunk packet-statistics

Function

The **display e-trunk packet-statistics** command displays E-Trunk packet statistics.

NOTE

Only the S5720I-SI, S5735-S, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6720S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Format

display e-trunk packet-statistics [**e-trunk-id** *e-trunk-id*]

Parameters

Parameter	Description	Value
e-trunk-id *e-trunk-id*	Display packet statistics about an E-Trunk. *e-trunk-id* specified the ID of the E-Trunk.	The value is an integer that ranges from 1 to 16.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After an E-Trunk is successfully configured, you can run the **display e-trunk packet-statistics** command to check packet statistics about the E-Trunk. The command output helps you to determine whether data is normal and to locate faults.

Example

# Display E-Trunk packet statistics on the device.

```
<HUAWEI> display e-trunk packet-statistics
E-Trunk-ID errors : 0
Length errors     : 0

E-TRUNK-ID : 10
  Sent packets                             : 355
  Failed to send packets                   : 355
  Received packets                         : 0
  Received packets with priority errors       : 0
  Received packets with fail-time errors      : 0
  Received packets with state errors          : 0
  Received packets with state reason errors   : 0
  Received packets with peer-ip errors        : 0
  Received packets with authentication errors : 0
  Received packets with TLV check errors      : 0
  Received packets with system-id errors      : 1
  Dropped packets with BFD protection         : 0
  Received packets with member errors         : 53
  Received packets with sequence check errors : 0
```

Table 5-21 Description of the **display e-trunk packet-statistics** command output

Item	Description
E-Trunk-ID errors	Number of packets with incorrect E-Trunk IDs.
Length errors	Number of packets with incorrect lengths.
E-TRUNK-ID	E-Trunk ID.
Sent packets	Number of sent E-Trunk packets.
Failed to send packets	Number of E-Trunk packets that fails to be sent.
Received packets	Number of received E-Trunk packets.
Received packets with priority errors	Number of received E-Trunk packets with incorrect priorities.
Received packets with fail-time errors	Number of received E-Trunk packets with timeout errors.

Item	Description
Received packets with state errors	Number of received E-Trunk packets with incorrect states.
Received packets with state reason errors	Number of received E-Trunk packets with incorrect state reasons.
Received packets with peer-ip errors	Number of received E-Trunk packets with incorrect remote IP addresses.
Received packets with authentication errors	Number of received E-Trunk packets with authentication errors.
Received packets with TLV check errors	Number of received E-Trunk packets with TLV check errors.
Received packets with system-id errors	Number of received E-Trunk packets with incorrect system IDs.
Dropped packets with BFD protection	Number of E-Trunk packets dropped during the active/standby switchover because BFD is used.
Received packets with member errors	Number of packets generated when the switch detects that Eth-Trunk member interfaces at both ends are different.
Received packets with sequence check errors	Number of received E-Trunk packets failing the sequence number check.

5.2.10 display e-trunk state-change

Function

The **display e-trunk state-change** command displays the latest 10 status changes of an E-Trunk member interface.

NOTE

Only the S5720I-SI, S5735-S, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6720S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Format

display e-trunk *e-trunk-id* **state-change member-interface** *interface-type interface-number*

Parameters

Parameter	Description	Value
e-trunk-id	Displays the latest 10 status changes of a specified E-Trunk.	The value is an integer that ranges from 1 to 16.
member-interface *interface-type interface-number*	Displays the latest 10 status changes of a specified E-Trunk member interface. *interface-type* can only be Eth-Trunk.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

After an E-Trunk is configured, you can run the **display e-trunk state-change** command to check the status changes of an E-Trunk member interface.

Prerequisites

An Eth-Trunk has been added to the E-Trunk.

Example

# Display the status changes of Eth-Trunk 10 in E-Trunk 1.

```
<HUAWEI> display e-trunk 1 state-change member-interface Eth-Trunk 10
Time                         SourceState    DestState   Reason
------------------------------------------------------------------------------
2013-07-25 10:41:30-08:00      Backup          Master      PEER_MEMBER_DOWN
```

Table 5-22 Description of the **display e-trunk state-change** command output

Item	Description
Time	Time when the status of the E-Trunk's member Eth-Trunk changed.
SourceState	Status of the E-Trunk's member Eth-Trunk before the status change.
DestState	State of the E-Trunk's member Eth-Trunk after the status change

Item	Description
Reason	Reason for the status change of the E-Trunk's member Eth-Trunk: ● FORCE_BACKUP: The E-Trunk's member Eth-Trunk is forcibly in backup state. ● FORCE_MASTER: The E-Trunk's member Eth-Trunk is forcibly in master state. ● ETRUNK_INIT: The E-Trunk is in initialization state. ● ETRUNK_BACKUP: The E-Trunk is in backup state. ● ETRUNK_MASTER: The E-Trunk is in master state. ● PEER_MEMBER_DOWN: The remote member Eth-Trunk goes Down. ● PEER_MEMBER_UP: The remote member Eth-Trunk goes Up. ● NO_PEER_MEMBER: There is no remote device.

5.2.11 display forward-path

Function

The **display forward-path** command displays collected traffic information.

NOTE

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

Format

display forward-path

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

To locate faults and understand the traffic forwarding path, run the **collect forward-path** command to configure the device to collect traffic information. To check collected packet information, run the **display forward-path** command.

Prerequisites

The device has been configured to collect traffic information.

Example

# Display collected traffic information.

```
<HUAWEI> display forward-path
The brief information of forward-path(s) for L3:
Id       : Report id
SIP      : Source IP address
DIP      : Destination IP address
Sport    : Source port
Dport    : Destination port
Pro      : Protocol type or protocol number
Dir      : Direction
Interval : Interval time (in minutes), 0 means that the system keeps
collecting
------------------------------------------------------------------------------
Id SIP           DIP           Sport Dport Pro    Dir     Interval   Status
------------------------------------------------------------------------------
1  10.1.1.1       10.2.2.2       -     -     -      both    10        done

The brief information of forward-path(s) for L2:
Id       : Report id
SMAC     : Source MAC address
DMAC     : Destination MAC address
VLAN     : VLAN id
Pro      : Protocol type or protocol number
Dir      : Direction
Interval : Interval time (in minutes), 0 means that the system keeps
collecting
------------------------------------------------------------------------------
Id SMAC            DMAC            VLAN   Pro    Dir      Interval     Status
------------------------------------------------------------------------------
2  00e0-fc12-3456   00e0-fc12-3456   10     -     both     10          doing
```

Table 5-23 Description of the **display forward-path** command output

Item	Description
Id	Report ID, that is, number of collected flows. You can run the **display forward-path report** command to view detailed information about inbound and outbound interfaces according to the specified report ID. The IDs are displayed according to the sequence in which the **collect forward-path** command was executed. If an ID is deleted, the existing IDs remain unchanged. The ID configured later is displayed in the position of the deleted ID. For example, IDs 1 and 2 exist on the device. If ID 1 is deleted, ID 2 remains unchanged. If the **collect forward-path** command is used, the new ID is displayed in the position of deleted ID 1. The device can collect inbound and outbound interfaces and traffic information of a maximum of 8 flows.
SIP	Source IP address of collected packets.
DIP	Destination IP address of collected packets.
Sport	Source port number of collected packets.
Dport	Destination port number of collected packets.
Pro	Protocol number or type of collected packets. To configure the protocol number or type of collected packets, run the **collect forward-path** command.
Dir	Direction where packets are collected.
Interval	The collection duration.
Status	Status of collected packets.
SMAC	Source MAC address of collected packets.
DMAC	Destination MAC address of collected packets.
VLAN	VLAN ID of collected packets.

5.2.12 display forward-path report

Function

The **display forward-path report** command displays traffic statistics.

NOTE

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

Format

display forward-path report *report-id*

Parameters

Parameter	Description	Value
report-id	Specifies the ID of collected traffic.	The value is an integer that ranges from 1 to 8. The IDs are displayed according to the sequence in which the **collect forward-path** command was executed. If an ID is deleted, the existing IDs remain unchanged. The ID configured later is displayed in the position of the deleted ID. For example, IDs 1 and 2 exist on the device. If ID 1 is deleted, ID 2 remains unchanged. If the **collect forward-path** command is used, the new ID is displayed in the position of deleted ID 1.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

To locate faults and understand the traffic forwarding path, run the **collect forward-path** command to configure the device to collect traffic information. Then run the **display forward-path report** command to check the collection result.

Prerequisites

The device has been configured to collect traffic information.

Example

# Display traffic statistics of the report ID 1.

```
<HUAWEI> display forward-path report 1
Source IP address      : 10.1.1.1
Destination IP address : 10.2.2.2
Source port            : -
Destination port       : -
Protocol type          : -
Direction              : both
Interval time          : 10 minute(s)
Status                 : doing
Start time             : 2010-12-30 11:39:11
End time               : -
```

```
-------------------------------------------------------------------------------
Port          Eth-Trunk       Packets         Bytes         Direction
-------------------------------------------------------------------------------
GE0/0/1        1               6555            20            ingress
GE0/0/2        -              6555            20            egress
```

# Display traffic statistics of the report ID 2.

```
<HUAWEI> display forward-path report 2
Source MAC address      : 00e0-fc05-0005
Destination MAC address : 00e0-fc06-0006
L2 protocol type        : arp
VLAN id                 : 5
Direction               : both
Interval time           : 1440 minute(s)
Status                  : doing
Start time              : 2015-11-23 17:15:33+02:00
End time                : -
-------------------------------------------------------------------------------
Port          Eth-Trunk       Packets         Bytes         Direction
------------------------------------------------------------------------------
GE0/0/1        -              46004724        0             ingress
GE0/0/2        -              45999397        0             ingress
```

Table 5-24 Description of the **display forward-path report** command output

Item	Description
Source IP address	Source IP address of collected packets.
Destination IP address	Destination IP address of collected packets.
Source port	Source port number of collected packets.
Destination port	Destination port number of collected packets.
Protocol type	Protocol number or type of collected packets. To configure the protocol number or type of collected packets, run the **collect forward-path** command.
Direction	Direction where packets are collected.
Interval time	The collection duration.
Status	Collected packet status.
Start time	Start time when packets were collected.
End time	End time when packets were collected.
Port	Inbound and outbound interfaces of packets.
Eth-Trunk	Eth-Trunk that interfaces join.
Source MAC address	Source MAC address of collected packets.
Destination MAC address	Destination MAC address of collected packets.
L2 protocol type	Layer 2 protocol type of collected packets.

Item	Description
VLAN id	VLAN ID of collected packets.
Packets	Number of forwarded packets.
Bytes	Number of forwarded bytes.

5.2.13 display interface eth-trunk

Function

The **display interface eth-trunk** command displays status and traffic statistics about Eth-Trunk interfaces.

Format

display interface eth-trunk [*trunk-id* | **main**]

display interface eth-trunk *trunk-id.subnumber*

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support *trunk-id.subnumber* parameter.

Parameters

Parameter	Description	Value
trunk-id	Specifies the ID of an Eth-Trunk.	The value is an integer. The value varies according to device model: ● SS1720GW-E, S1720GWR-E, S2730S-S, S5720I-SI, S5720-LI, and S5720S-LI: 0-119 ● S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735-S-I, S5735S-S, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S: 0-127 ● S5735S-H, S5736-S, S6720S-S: 0-249 On the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, S6730S-S, S6735-S, S6720-EI, and S6720S-EI, you can run the **assign trunk** command to set the value, and run the **display trunk configuration** command to check the configuration.
main	Displays the status and traffic statistics of an Eth-Trunk main interface.	-
trunk-id.subnumber	Specifies the number of an Eth-Trunk sub-interface.	The value is an integer that ranges from 1 to 4096.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display interface eth-trunk** command to view the status and weight of each Eth-Trunk member interface.

To monitor the status of an interface or locate an interface fault, you can use the **display interface eth-trunk** command to collect the status of and traffic statistics on the interface. You can collect traffic statistics and locate faults on the interface according to the command output.

Example

# Display status and traffic statistics about Eth-Trunk 10.

```
<HUAWEI> display interface Eth-Trunk 10
Eth-Trunk10 current state : UP
Line protocol current state : DOWN
Description:
Switch Port, Link-type : trunk(negotiated),
PVID :    1, Hash arithmetic : According to SIP-XOR-DIP,Maximal BW:
 2G, Current BW: 1000M, The Maximum Frame Length is 9216
IP Sending Frames' Format is PKTFMT_ETHNT_2, Hardware address is 00e0-fcd4-36f1
Current system time: 2013-01-14 19:38:12
Last 300 seconds input rate 0 bits/sec, 0 packets/sec
Last 300 seconds output rate 0 bits/sec, 0 packets/sec
Input:  0 packets, 0 bytes
  Unicast:                    0,  Multicast:                    0
  Broadcast:                  0,  Jumbo:                        0
  Discard:                    0,  Pause:                        0
  Frames:                     0

  Total Error:                0
  CRC:                        0,  Giants:                       0
  Jabbers:                    0,  Fragments:                    0
  Runts:                      0,  DropEvents:                   0
  Alignments:                 0,  Symbols:                      0
  Ignoreds:                   0

Output:  0 packets, 0 bytes
  Unicast:                    0,  Multicast:                    0
  Broadcast:                  0,  Jumbo:                        0
  Discard:                    0,  Pause:                        0

  Total Error:                0
  Collisions:                 0,  ExcessiveCollisions:          0
  Late Collisions:            0,  Deferreds:                    0
  Buffers Purged:             0

    Input bandwidth utilization  :    0%
    Output bandwidth utilization :    0%
-----------------------------------------------------
PortName                      Status      Weight
-----------------------------------------------------
GigabitEthernet0/0/1          DOWN        1
GigabitEthernet0/0/2          UP          1
-----------------------------------------------------
The Number of Ports in Trunk : 2
The Number of UP Ports in Trunk : 1
```

Table 5-25 Description of the **display interface eth-trunk** command output

Item	Description
Eth-Trunk10 current state	Eth-Trunk status: ● UP: The interface is Up. ● DOWN: The interface becomes faulty. ● UP(E-TRUNK-DOWN): The Eth-Trunk goes Down because of E-Trunk negotiation.

Item	Description
Line protocol current state	Link layer protocol status of the Eth-Trunk: ● DOWN: The link layer protocol of the interface fails or no IP address is assigned to the interface. ● UP: The link layer protocol of the interface is running properly.
Description	Description of the Eth-Trunk. To specify the parameter, run the **description** command.
Switch Port	The Eth-Trunk is a Layer 2 interface. Route Port is displayed if the Eth-Trunk is a Layer 3 interface.
Link-type	Link type of the Layer 2 interface. The parameter is displayed only in Layer 2 mode. The options are as follows: ● access (configured): The interface is manually configured as an access interface. ● hybrid: The interface is manually configured as a hybrid interface. ● trunk (configured): The interface is manually configured as a trunk interface. ● dot1q-tunnel: The interface is manually configured as a Dot1q-tunnel interface. ● access(negotiated): The interface is used as an access interface through negotiation. ● trunk(negotiated): The interface is used as a trunk interface through negotiation. To configure the link type of an interface, run the **port link-type** command.
PVID	Default VLAN ID of the Eth-Trunk.
Hash arithmetic	Hash algorithm used for load balancing among Eth-Trunk member interfaces. The hash algorithm depends on the load balancing mode configured by using the **load-balance** command. The SS1720GW-E, S1720GWR-E, S5720I-SI, S5720-LI, S5720S-LI, S5735S-H, S5736-S, and S6720S-S use the **src-dst-ip**, source TCP or UDP port number, and destination TCP or UDP port number in the hash algorithm for load balancing regardless of whether you configure this parameter.
Maximal BW	Maximum bandwidth.
Current BW	Current bandwidth.

Item	Description
The Maximum Frame Length	Maximum frame length allowed by the Eth-Trunk. To specify the parameter, run the **jumboframe enable** command.
IP Sending Frames' Format	Format of frames sent through the IP protocol, which can be PKTFMT_ETHNT_2, Ethernet_802.3, or Ethernet_SNAP.
Hardware address	Device MAC address.
Current system time	Current system time. If the time zone is configured and the daylight saving time is used, the time is in the format of YYYY/MM/DD HH:MM:SS±HH:MM.
Last 300 seconds input rate	Received packet rate (bits per second and packets per second) within the last 300 seconds.
Last 300 seconds output rate	Sent packet rate (bits per second and packets per second) within the last 300 seconds.
Input	Total number of received packets.
Output	Total number of sent packets.
Unicast	Number of unicast packets received or sent by an Eth-Trunk.
Multicast	Number of multicast packets received or sent by an Eth-Trunk.
Broadcast	Number of broadcast packets received or sent by an Eth-Trunk.
Jumbo	Number of jumbo frames received or sent by the Eth-Trunk.
Discard	Number of packets discarded by the Eth-Trunk during physical layer detection.
Pause	Pause frame.
Total Error	Number of error packets discovered by the Eth-Trunk during physical layer detection.
CRC	Number of CRC error packets received by the Eth-Trunk.
Giants	Number of jumbo frames with the correct FCS received by the Eth-Trunk.
Jabbers	Number of jumbo frames with incorrect FCS received by the Eth-Trunk.
Fragments	Number of fragments received by the Eth-Trunk.

Item	Description
Runts	Number of undersized frames with the correct FCS received by the Eth-Trunk.
DropEvents	Number of received packets that are discarded due to GBP full or back pressure.
Alignments	Number of received frames with alignment errors.
Symbols	Number of received frames with coding errors.
Ignoreds	Number of received MAC control frames in which the OpCode is not PAUSE.
Frames	Number of packets with the incorrect 802.3 length.
Collisions	Number of sent packets. During packet transmission, 1 to 15 conflict events were generated.
ExcessiveCollisions	Number of packets that fail to be sent. During packet transmission, 16 conflict events were generated.
Late Collisions	Number of delayed packets sent by the Eth-Trunk. During packet transmission, conflict events were generated.
Deferreds	Number of delayed packets sent by the Eth-Trunk. During packet transmission, no conflict event was generated.
Buffers Purged	Number of packets aged in the cache because packets sent by the Eth-Trunk have been stored in the queue buffer for a long time.
Input bandwidth utilization	Inbound bandwidth usage.
Output bandwidth utilization	Outbound bandwidth usage.
PortName	Name of the Eth-Trunk member interface.
Status	Status of the Eth-Trunk member interface. Manual mode: ● Up: indicates that the interface is properly started. ● Down: indicates that the interface becomes faulty. LACP mode: ● Up: indicates that the interface is selected. ● Down: indicates that the interface is not selected.
Weight	Weight of a member interface for load balancing.
The Number of Ports in Trunk	Number of Eth-Trunk member interfaces.

Item	Description
The Number of UP Ports in Trunk	Number of Eth-Trunk member interfaces in Up state.

5.2.14 display lacp brief

Function

The **display lacp brief** command displays brief LACP information, including the LACP system priority and system ID.

Format

display lacp brief

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

Devices at both ends of an Eth-Trunk compare LACP system priorities and system IDs to determine the Actor during LACP negotiation.

- By default, the LACP system priority is 32768, and the device with the smaller LACP system ID is used as the Actor.
- If LACP system priorities are changed using the **lacp priority** command, the device with the smaller LACP system priority is used as the Actor.

The **display eth-trunk** command can be used to check the LACP system priority and system ID only after an Eth-Trunk in LACP mode has been configured. This is inconvenient for network planning. To facilitate network planning, you can run the **display lacp brief** command to check the LACP system priority and system ID when no Eth-Trunk in LACP mode is configured.

Precautions

When two PEs join an E-Trunk, run the **lacp e-trunk system-id** command on the PEs to configure the same E-Trunk LACP system ID so that the CE considers the PEs to be one device. The E-Trunk LACP system ID configurations do not affect

LACP system IDs of Eth-Trunks in LACP mode. The LACP system ID of an Eth-Trunk in LACP mode is the MAC address of the Ethernet interface on the device.

E-Trunk is supported by only the following models: S5720I-SI, S5735-S, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6720S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S.

Example

# Display brief LACP information.

```
<HUAWEI> display lacp brief
System Priority:32768
System ID      :00e0-5958-ef00
```

Table 5-26 Description of the **display lacp brief** command output

Item	Description
System Priority	LACP system priority. To configure the LACP system priority, run the **lacp priority** command.
System ID	System ID, which is the bridge MAC address of the device.

5.2.15 display lacp statistics eth-trunk

Function

The **display lacp statistics eth-trunk** command displays statistics on received and sent Link Aggregation Control Protocol Data Units (LACPDUs) about an Eth-Trunk in LACP mode.

Format

display lacp statistics eth-trunk [*trunk-id* [**interface** *interface-type interface-number*]]

Parameters

Parameter	Description	Value
trunk-id	Specifies the ID of an Eth-Trunk.	The value is an integer. The value varies according to device model: ● SS1720GW-E, S1720GWR-E, S2730S-S, S5720I-SI, S5720-LI, and S5720S-LI: 0-119 ● S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735-S-I, S5735S-S, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S: 0-127 ● S5735S-H, S5736-S, S6720S-S: 0-249 On the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, S6730S-S, S6735-S, S6720-EI, and S6720S-EI, you can run the **assign trunk** command to set the value, and run the **display trunk configuration** command to check the configuration.
interface *interface-type interface-number*	Specifies the type and number of an interface. ● *interface-type* specifies the type of the interface. ● *interface-number* specifies the number of the interface.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

This command can be used only when the Eth-Trunk works in LACP mode. To change the working mode of an Eth-Trunk to the LACP mode, run the **mode lacp** command in the Eth-Trunk interface view.

To view the statistics on a specific Eth-Trunk, ensure that the Eth-Trunk has been created. To view the statistics on a specified Eth-Trunk member interface, ensure that the interface is added to the Eth-Trunk.

Example

# Display the statistics on LACPDUs sent and received by member interface GigabitEthernet0/0/1 of Eth-Trunk 4.

```
<HUAWEI> display lacp statistics eth-trunk 4
 Eth-Trunk4's PDU statistic is:
 -------------------------------------------------------------------------------
 Port                  LacpRevPdu   LacpSentPdu  MarkerRevPdu  MarkerSentPdu
 GigabitEthernet0/0/2    20683        830          0             0
 GigabitEthernet0/0/3    16356        677          0             0
 GigabitEthernet0/0/1    7213         7213         0             0
```

# Display the statistics on LACPDUs sent and received by member interface GigabitEthernet0/0/1 of Eth-Trunk 4.

```
<HUAWEI> display lacp statistics eth-trunk 4 interface gigabitethernet 0/0/1
 GigabitEthernet0/0/1's PDU statistic is:
 -------------------------------------------------------------------------------
 Port                  LacpRevPdu   LacpSentPdu  MarkerRevPdu MarkerSentPdu
 GigabitEthernet0/0/1    7673         7673         0            0
```

Table 5-27 Description of the **display lacp statistics eth-trunk** command output

Item	Description
Port	Current member interface of the Eth-Trunk.
LacpRevPdu	Number of received LACPDUs.
LacpSentPdu	Number of sent LACPDUs.
MarkerRevPdu	Number of received MARKER packets.
MarkerSentPdu	Number of sent MARKER packets.

5.2.16 display load-balance-profile

Function

The **display load-balance-profile** command displays detailed information about a specified load balancing profile.

NOTE

Only the S5735S-H, S5736-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6720S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Format

display load-balance-profile [*profile-name*]

Parameters

Parameter	Description	Value
profile-name	Specifies the name of a load balancing profile.	The value is a string of 1 to 31 characters.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

This command displays detailed information about a specified load balancing profile, including the load balancing mode of IPv4, IPv6, Layer 2, and MPLS packets.

Example

# Display detailed information about a specified load balancing profile.

```
<HUAWEI> display load-balance-profile abc
Load-balance-profile : abc
Packet    HashField
----------------------------------
IPV4      sip         dip
IPV6      sip         dip
L2        smac        l2-protocol vlan       sport
MPLS      top-label   2nd-label

Trunk interface
----------------------------------
Eth-Trunk100
```

Table 5-28 Description of the display load-balance-profile command output

Item	Description
Load-balance-profile	Load balancing profile. To specify the parameter, run the **load-balance-profile** command.
Packet	Packet type.
HashField	Load balancing mode in the load balancing profile. You can run the **ipv4 field**, **ipv6 field**, **l2 field**, and **mpls field** commands to configure the load balancing mode for IPv4, IPv6, Layer 2, and MPLS packets respectively.
Trunk interface	Eth-Trunk that uses the load balancing profile, configured by the **load-balance** command.

5.2.17 display load-distribution active-linknumber-change

Function

The **display load-distribution active-linknumber-change** command displays the configuration when the number of interfaces in an Eth-Trunk where load balancing calculation is performed is configured.

NOTE

Only the SS1720GW-E, S1720GWR-E, S5720-LI, S5720S-LI, and S5720I-SI support this command.

Format

display load-distribution active-linknumber-change [**interface Eth-Trunk** *trunk-id*]

Parameters

Parameter	Description	Value
interface Eth-Trunk *trunk-id*	Specifies the ID of an Eth-Trunk.	The ID of an Eth-Trunk must have been created.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After the **load-distribution active-linknumber-change** command is used to configure the number of interfaces in an Eth-Trunk where load balancing calculation is performed, you can run the **display load-distribution active-linknumber-change** command to check the configuration.

Example

# Display the configuration when the number of interfaces in an Eth-Trunk where load balancing calculation is performed is configured.

```
<HUAWEI> display load-distribution active-linknumber-change interface Eth-Trunk 3
-------------------------------------------------------------------------------
Interface    Pre-linknumber    Post-linknumber
-------------------------------------------------------------------------------
Eth-Trunk3       2                  4
-------------------------------------------------------------------------------
```

Table 5-29 Description of the **display load-distribution active-linknumber-change** command output

Item	Description
Interface	Name of the Eth-Trunk.
Pre-linknumber	Number of active interfaces in an Eth-Trunk when the number of interfaces in an Eth-Trunk where load balancing calculation is performed is configured. To configure the number of active interfaces in an Eth-Trunk when the number of interfaces in an Eth-Trunk where load balancing calculation is performed, run the **load-distribution active-linknumber-change** or **load-distribution active-linknumber-change global** command.
Post-linknumber	Number of interfaces in an Eth-Trunk where load balancing calculation is performed when the Eth-Trunk has active interfaces. To configure the number of interfaces in an Eth-Trunk where load balancing calculation is performed when the Eth-Trunk has active interfaces, run the **load-distribution active-linknumber-change** or **load-distribution active-linknumber-change global** command.

5.2.18 display trunk index-map

Function

The **display trunk index-map** command displays the mapping between Eth-Trunk IDs and internal indexes.

Format

display trunk index-map

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

An ID is manually allocated to an Eth-Trunk during Eth-Trunk creation. For example, the ID of Eth-Trunk 1 is 1. In addition, the device also allocates an internal number, also called the index, to each Eth-Trunk. When allocating indexes, the device traverses indexes in ascending order. The unallocated index is used as the index of an Eth-Trunk; therefore, the mapping between Eth-Trunk IDs and indexes is unordered. You can use **display trunk index-map** to check the mapping between Eth-Trunk IDs and indexes.

Example

# Display the mapping between Eth-Trunk IDs and internal indexes.

```
<HUAWEI> display trunk index-map
Index   Interface Name

-----------------------------
1       Eth-Trunk10
2       Eth-Trunk20
3       Eth-Trunk5
```

Table 5-30 Description of the **display trunk index-map** command output

Item	Description
Index	Index of the Eth-Trunk.
Interface Name	Name of the Eth-Trunk.

5.2.19 display trunk resource

Function

The **display trunk resource** command displays trunk resources that have been used on a device.

Format

display trunk resource

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

To view the number of trunk interfaces configured on a device and the number of member interfaces added to the trunk interfaces, run the **display trunk resource** command. The command output helps you learn about used trunk resources.

Example

# Display trunk resources used on a device.

```
<HUAWEI> display trunk resource
Number of configured trunk interfaces is : 4
Interface           Member Count
-------------------------------------------------------------
Eth-Trunk1           2
Eth-Trunk10          0
Eth-Trunk30          0
Eth-Trunk55          0
```

Table 5-31 Description of the **display trunk resource** command output

Item	Description
Number of configured trunk interfaces is	Number of configured trunk interfaces.
Interface	Trunk interface type: ● Eth-Trunk
Member Count	Number of member interfaces added to a trunk interface.

5.2.20 display trunkfwdtbl eth-trunk

Function

The **display trunkfwdtbl eth-trunk** command displays the forwarding table of an Eth-Trunk.

Format

display trunkfwdtbl eth-trunk *trunk-id*

Parameters

Parameter	Description	Value
trunk-id	Specifies the ID of an Eth-Trunk.	The value is an integer. The value varies according to device model: ● SS1720GW-E, S1720GWR-E, S2730S-S, S5720I-SI, S5720-LI, and S5720S-LI: 0-119 ● S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735-S-I, S5735S-S, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S: 0-127 ● S5735S-H, S5736-S, S6720S-S: 0-249 On the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, S6730S-S, S6735-S, S6720-EI, and S6720S-EI, you can run the **assign trunk** command to set the value, and run the **display trunk configuration** command to check the configuration.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

By default, an Eth-Trunk supports a maximum of eight physical member interfaces, which correspond to eight entries in the forwarding table. The eight entries correspond to HASH-KEY values 0 to 7. The system searches for outbound interfaces among active links based on HASH-KEY values.

NOTE

On the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, S6730S-S, S6735-S, S6720-EI, and S6720S-EI, you can run the **assign trunk** command to set the value, and run the **display trunk configuration** command to check the configuration.

Example

# Display the forwarding table of Eth-Trunk 1. Eth-Trunk 1 has three active links.

```
<HUAWEI> display trunkfwdtbl eth-trunk 1
 Eth-Trunk1's forwarding table is:
GigabitEthernet0/0/1
GigabitEthernet0/0/2
GigabitEthernet0/0/3
GigabitEthernet0/0/1
GigabitEthernet0/0/2
GigabitEthernet0/0/3
GigabitEthernet0/0/1
GigabitEthernet0/0/2
```

Table 5-32 Description of the **display trunkfwdtbl eth-trunk** command output

Item	Description
Eth-Trunk1's forwarding table	Forwarding entry of an Eth-Trunk.

5.2.21 display trunkmembership eth-trunk

Function

The **display trunkmembership eth-trunk** command displays information about Eth-Trunk member interfaces.

Format

display trunkmembership eth-trunk *trunk-id*

Parameters

Parameter	Description	Value
trunk-id	Specifies the ID of an Eth-Trunk.	The value is an integer. The value varies according to device model: ● SS1720GW-E, S1720GWR-E, S2730S-S, S5720I-SI, S5720-LI, and S5720S-LI: 0-119 ● S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735-S-I, S5735S-S, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S: 0-127 ● S5735S-H, S5736-S, S6720S-S: 0-249 On the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, S6730S-S, S6735-S, S6720-EI, and S6720S-EI, you can run the **assign trunk** command to set the value, and run the **display trunk configuration** command to check the configuration.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

After an Eth-Trunk is successfully configured, you can run the **display trunkmembership eth-trunk** command to view the configuration of the Eth-Trunk and its member interfaces.

To monitor the status of an interface or locate an interface fault, you can use the **display trunkmembership eth-trunk** command to view detailed information about an Eth-Trunk and its member interfaces. The command output helps you can troubleshoot faults and check the member interface configuration.

Prerequisites

An Eth-Trunk has been correctly configured. If the Eth-Trunk is not created, the system displays an error when you run the **display trunkmembership eth-trunk** command.

Precautions

Before running the **display trunkmembership eth-trunk** command to view the configuration of the Eth-Trunk in LACP mode, ensure that the Eth-Trunk has been configured to work in LACP mode using the **mode lacp** command.

Example

# Display information about member interfaces of Eth-Trunk 2.

```
<HUAWEI> display trunkmembership eth-trunk 2
Trunk ID: 2
Used status: VALID
TYPE: ethernet
Working Mode : Normal
Number Of Ports in Trunk = 2
Number Of Up Ports in Trunk = 2
Operate status: up
Interface GigabitEthernet0/0/1, valid, operate up, weight=1
Interface GigabitEthernet0/0/2, valid, operate up, weight=1
```

Table 5-33 Description of the display trunkmembership eth-trunk command output

Item	Description
Trunk ID	ID of the Eth-Trunk.
Used status	Whether the Eth-Trunk is available: ● VALID: The Eth-Trunk is available. ● INVALID: The Eth-Trunk is unavailable.
TYPE	Type of an Eth-Trunk. To specify the parameter, run the **port link-type** command.
Working Mode	Working mode of an Eth-Trunk. ● Normal: manual load balancing mode ● LACP: LACP mode To specify the parameter, run the **mode** command.
Number Of Ports in Trunk	Number of interfaces that are added to the Eth-Trunk.
Number Of Up Ports in Trunk	Number of Up interfaces that are added to the Eth-Trunk.
Operate status	Eth-Trunk status: ● up ● down

Item	Description
Interface, valid, operate, weight	Detailed information about a member interface: ● Interface: indicates the interface type and number. ● valid: indicates that the interface is available. ● operate: indicates the status of the interface. ● weight: indicates the weight of the interface for load balancing.

5.2.22 eth-trunk

Function

The **eth-trunk** command adds an interface to an Eth-Trunk.

The **undo eth-trunk** command removes an interface from an Eth-Trunk.

By default, an interface does not belong to any Eth-Trunk.

Format

eth-trunk *trunk-id* [**mode** { **active** | **passive** }]

undo eth-trunk

Parameters

Parameter	Description	Value
trunk-id	Indicates the ID of an Eth-Trunk.	The value is an integer that ranges from 0 to 249. The value is an integer. The value varies according to device model: ● SS1720GW-E, S1720GWR-E, S2730S-S, S5720I-SI, S5720-LI, and S5720S-LI: 0-119 ● S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735-S-I, S5735S-S, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S: 0-127 ● S5735S-H, S5736-S, S6720S-S: 0-249 On the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, S6730S-S, S6735-S, S6720-EI, and S6720S-EI, you can run the **assign trunk** command to set the value, and run the **display trunk configuration** command to check the configuration.

Parameter	Description	Value
mode { **active** | **passive** }	Indicates the mode in which an Eth-Trunk member interface sends packets. This parameter is valid for only the Eth-Trunk in LACP mode. By default, the mode an Eth-Trunk member interface sends packets is **active**. ● **active**: indicates that an Eth-Trunk member interface proactively sends negotiation packets. ● **passive**: indicates that an Eth-Trunk member interface sends packets to negotiate with its remote end only after receiving a packet from its remote end.	-

Views

Ethernet interface view, GE interface view, XGE interface view, MultiGE interface view, 40GE interface view, 100GE interface view, 25GE interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To improve the connection reliability and increase the bandwidth, you can use the **eth-trunk** command to bind multiple interfaces into an Eth-Trunk.

You can add an interface to an Eth-Trunk only after you run the **interface Eth-Trunk** command to create the Eth-Trunk.

An Eth-Trunk contains a maximum of 32 member interfaces on the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S, 16 member interfaces on the S5735S-H, S5736-S, and S6720S-S, and 8 member interfaces on all other models. Interfaces added to an Eth-Trunk are called member interfaces. On the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, S6730S-S, S6735-S, S6720-EI and S6720S-EI, you can run the **assign trunk** command to set the value, and run the **display trunk configuration** command to check the configuration.

When you add an Ethernet interface to an Eth-Trunk, the interface must use default settings of some attributes. Otherwise, the interface cannot be added to the Eth-Trunk. The attributes include:

- Link type
- VLAN that the interface belongs to
- VLAN mapping
- VLAN stacking
- QinQ protocol number
- Interface priority
- Whether the interface allows BPDUs to pass through
- MAC address learning
- Adding the interface to a multicast group statically
- Discarding broadcast packets
- Discarding unknown multicast packets
- Discarding unknown unicast packets
- Controllable multicast profile bound to the interface

The attributes on all member interfaces of an Eth-Trunk must be consistent and cannot be changed separately. If the preceding attributes of an Eth-Trunk are changed, the attributes of all the member interfaces are changed accordingly.

It is recommended that you run the **shutdown (interface view)** command to disable an interface before adding the interface to an Eth-Trunk. After adding interfaces at both ends of a link to an Eth-Trunk, run the **undo shutdown (interface view)** command to enable the interfaces. Otherwise, traffic interruption or broadcast storms may occur.

It is recommended that you run the **shutdown (interface view)** command to disable a member interface before running the **undo eth-trunk** command to remove the member interface from an Eth-Trunk.

The number of member interfaces of the Eth-Trunk on devices at both ends must be the same. The interfaces at both ends must be connected with straight-through cables.

Example

# Add GigabitEthernet0/0/1 to Eth-Trunk 2.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] eth-trunk 2
```

5.2.23 e-trunk (Eth-Trunk interface view)

Function

The **e-trunk** command adds an Eth-Trunk in LACP mode to a specified E-Trunk.

The **undo e-trunk** command deletes an Eth-Trunk from a specified E-Trunk.

NOTE

Only the S5720I-SI, S5735-S, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6720S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Format

e-trunk *e-trunk-id* [**remote-eth-trunk** *eth-trunk-id*]

undo e-trunk

Parameters

Parameter	Description	Value
e-trunk-id	Specifies the ID of an E-Trunk.	The value is an integer that ranges from 1 to 16.
remote-eth-trunk *eth-trunk-id*	Specifies the Eth-Trunk ID of the remote PE. If the ID of the Eth-Trunk created on a PE is different from the ID of the Eth-Trunk created on the other PE, you must configure **remote-eth-trunk** when adding different Eth-Trunks in LACP mode to an E-Trunk so that the E-Trunk can work properly.	The value is an integer that ranges from 0 to 4294967295.

Views

Eth-Trunk interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Only Eth-Trunks in LACP mode can be added to an E-Trunk, and an Eth-Trunk can be added to only one E-Trunk. If an Eth-Trunk is already added to an E-Trunk, you must delete it from the E-Trunk before adding it to another E-Trunk.

NOTE

At most 64 Eth-Trunks in LACP mode can be added to an E-Trunk.

Precautions

- Only Eth-Trunk interfaces in LACP mode can be added to an E-Trunk.
- After an Eth-Trunk interface is added to an E-Trunk, to add the Eth-Trunk interface to another E-Trunk or modify the remote Eth-Trunk ID, first run the **undo e-trunk** command to delete the Eth-Trunk interface from the current E-Trunk and then run the **e-trunk** command.
- If the master Eth-Trunk interface in an E-Trunk encounters a link failure, the backup Eth-Trunk interface goes Down after the master Eth-Trunk interface is removed from the E-Trunk.

Example

# Add Eth-Trunk 1 to E-Trunk 1.

```
<HUAWEI> system-view
[HUAWEI] interface Eth-Trunk 1
[HUAWEI-Eth-Trunk1] e-trunk 1
```

5.2.24 e-trunk mode

Function

The **e-trunk mode** command configures a working mode of an Eth-Trunk in an E-Trunk.

The **undo e-trunk mode** command restores the default working mode of an Eth-Trunk in an E-Trunk.

By default, an Eth-Trunk works in automatic mode in an E-Trunk.

NOTE

Only the S5720I-SI, S5735-S, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6720S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Format

e-trunk mode { **auto** | **force-master** | **force-backup** }

undo e-trunk mode

Parameters

Parameter	Description	Value
auto	Indicates the automatic mode.	-
force-master	Indicates the forcible master mode.	-
force-backup	Indicates the forcible backup mode.	-

Views

Eth-Trunk interface view, MultiGE interface view

Default Level

2: Configuration level

Usage Guidelines

The **e-trunk mode** command is valid only for the Eth-Trunks added to an E-Trunk. When the Eth-Trunk is deleted from the E-Trunk, the configuration is cancelled.

When the E-Trunk works properly, changing the interval for sending packets or timeout of hello packets will cause the E-Trunk to alternate between the master state and the backup state. You are advised to set the working mode of a member Eth-Trunk to forcible master/backup before changing the interval for sending packets or the timeout of hello packets. After the new configuration takes effect, restore the working mode to automatic.

Example

# Set the working mode of Eth-Trunk 1 in an E-Trunk to forcible master.

```
<HUAWEI> system-view
[HUAWEI] interface Eth-Trunk 1
[HUAWEI-Eth-Trunk1] e-trunk mode force-master
```

5.2.25 e-trunk port

Function

The **e-trunk port** command configures the UDP port number used to send and receive E-Trunk packets.

The **undo e-trunk port** command restores the default value.

By default, UDP port 1025 is used to send and receive E-Trunk packets.

NOTE

Only the S5720I-SI, S5735-S, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6720S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Format

e-trunk port *port-number*

undo e-trunk port

Parameters

Parameter	Description	Value
port-number	Specifies the UDP port number used to send and receive E-Trunk packets. If the UDP port number in the range of 1025 to 65535 is used by another protocol, the port number cannot be used to send or receive E-Trunk packets. **NOTE** UDP port numbers 49152 to 65535 are allocated randomly by the socket. Do not configure the UDP port number in this range; otherwise, the E-Trunk cannot work properly.	The value is an integer that ranges from 1025 to 65535.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

E-Trunk is a Huawei proprietary protocol. UDP port 1025 used to send and receive E-Trunk packets may conflict with the UDP port used by another protocol. To ensure that E-Trunk packets are forwarded correctly, run the **e-trunk port** command to change the UDP port number used to send and receive E-Trunk packets.

Precautions

The port numbers at both ends of an E-Trunk must be consistent. When the E-Trunk works properly, you must change the UDP port number within the timeout of E-Trunk negotiation.

If you change the UDP port number during E-Trunk running, devices at both ends of an E-Trunk may be unable to communicate. If E-Trunk negotiation times out, both devices in the E-Trunk may become master devices.

Example

# Configure the UDP port number used to send and receive E-Trunk packets.

```
<HUAWEI> system-view
[HUAWEI] e-trunk port 1026
```

5.2.26 e-trunk (system view)

Function

The **e-trunk** command creates an E-Trunk.

The **undo e-trunk** command deletes an E-Trunk.

NOTE

Only the S5720I-SI, S5735-S, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6720S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Format

e-trunk *e-trunk-id*

undo e-trunk *e-trunk-id*

Parameters

Parameter	Description	Value
e-trunk-id	Specifies the ID of an E-Trunk.	The value is an integer that ranges from 1 to 16.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

If the specified E-Trunk already exists, this command directly displays the view of the specified E-Trunk.

At most 16 E-Trunks can be created on a device.

After an E-Trunk is created, it does not send protocol packets until the remote IP address is configured.

Example

# Create an E-Trunk with the ID of 1.

```
<HUAWEI> system-view
[HUAWEI] e-trunk 1
[HUAWEI-e-trunk-1]
```

5.2.27 e-trunk track bfd-session

Function

The **e-trunk track bfd-session** command binds a BFD session to an E-Trunk.

The **undo e-trunk track bfd-session** command unbinds a BFD session from an E-Trunk.

By default, no BFD session is bound to an E-Trunk.

NOTE

Only the S5720I-SI, S5735-S, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6720S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Format

e-trunk track bfd-session session-name *bfd-session-name*

undo e-trunk track bfd-session

Parameters

Parameter	Description	Value
session-name *bfd-session-name*	Specifies the name of a BFD session.	The value is a string of 1 to 15 case-insensitive characters without spaces. When the string is enclosed with double quotation marks (""), spaces are allowed in the string.

Views

E-Trunk view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

PE1 and PE2 are connected through an E-Trunk. PE1 is in master state and PE2 is in slave state. When PE1 fails and PE2 does not receive any E-Trunk protocol packets from PE1 after the timer expires, PE2 switches from the slave state to the master state.

The status of PE2 changes after the timer expires. During the timeout, user traffic is interrupted. To enable PE2 to rapidly detect the fault and switch its status, run this command to bind a BFD session to an E-Trunk.

After the BFD session is bound to the E-Trunk, the BFD session can rapidly detect the link between PE1 and PE2. If the link fails, the BFD session becomes Down. PE2 then can detect the BFD session status and switch its status to master so that traffic is correctly forwarded.

NOTE

In this scenario, the Eth-Trunk on PE1 and PE2 supports only one member interface.

Prerequisites

Before using this command, pay attention to the following points:

- An E-Trunk and a BFD session must have been configured. BFD for IP must be used; otherwise, the E-Trunk cannot rapidly detect the fault through the BFD session.
- The IP addresses of both ends of the E-Trunk must be reachable; otherwise, the BFD session cannot go Up. That is, the BFD session cannot detect the link between PE1 and PE2.

Precautions

After a BFD session is bound to an E-Trunk and AC interfaces on both devices of the E-Trunk are associated with the BFD session, if the AC interface of the master device fails, the BFD session goes Down and traffic is switched to the standby link. If the AC interface recovers within 60 seconds, traffic is immediately switched back to the active link.

Example

# Bind a BFD session named **hello** to E-Trunk 1.

```
<HUAWEI> system-view
[HUAWEI] e-trunk 1
[HUAWEI-e-trunk-1] e-trunk track bfd-session session-name hello
```

5.2.28 interface eth-trunk

Function

The **interface eth-trunk** command displays the view of an existing Eth-Trunk or creates an Eth-Trunk and displays its view.

The **undo interface eth-trunk** command deletes an Eth-Trunk.

By default, no Eth-Trunk is created.

Format

interface eth-trunk *trunk-id*[.*subnumber*]

undo interface eth-trunk *trunk-id*[.*subnumber*]

Parameters

Parameter	Description	Value
trunk-id	Specifies the ID of an Eth-Trunk.	The value is an integer. The value varies according to device model: ● SS1720GW-E, S1720GWR-E, S2730S-S, S5720I-SI, S5720-LI, and S5720S-LI: 0-119 ● S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735-S-I, S5735S-S, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S: 0-127 ● S5735S-H, S5736-S, S6720S-S: 0-249 On the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, S6730S-S, S6735-S, S6720-EI, and S6720S-EI, you can run the **assign trunk** command to set the value, and run the **display trunk configuration** command to check the configuration.
subnumber	Specifies the ID of an Eth-Trunk sub-interface.	The value is an integer that ranges from 1 to 4096.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

If the specified Eth-Trunk already exists, the **interface eth-trunk** command directly displays the view of the specified Eth-Trunk.

You can delete an Eth-Trunk only when the Eth-Trunk does not contain any member interface.

NOTE

- Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support Ethernet sub-interfaces.
- Only hybrid and trunk interfaces on the preceding switches support Layer 2 Ethernet sub-interface configuration.
- After you run the **undo portswitch** command to switch Layer 2 interfaces on the preceding series of switches into Layer 3 interfaces, you can configure Layer 3 Ethernet sub-interfaces on the interfaces.
- After an interface is added to an Eth-Trunk, sub-interfaces cannot be configured on the interface.
- VLAN termination sub-interfaces cannot be created on a VCMP client.

Example

# Create Eth-Trunk 2.

```
<HUAWEI> system-view
[HUAWEI] interface eth-trunk 2
[HUAWEI-Eth-Trunk2]
```

5.2.29 ipv4 field

Function

The **ipv4 field** command configures a load balancing mode of IPv4 packets in a load balancing profile.

The **undo ipv4 field** command deletes a load balancing mode of IPv4 packets or restores the default load balancing mode of IPv4 packets.

By default, load balancing of IPv4 packets is based on the source IP address (**sip**) and destination IP address (**dip**).

NOTE

Only the S5735S-H, S5736-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6720S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Format

ipv4 field [**dip** | **l4-dport** | **l4-sport** | **protocol** | **sip** | **sport** | **vlan**] *

undo ipv4 field [**dip** | **l4-dport** | **l4-sport** | **protocol** | **sip** | **sport** | **vlan**] *

NOTE

Only **dip**, **sip**, and **sport** are supported on the S5736-S.

Parameters

Parameter	Description	Value
dip	Performs load balancing based on destination IP addresses in IPv4 packets.	-
l4-dport	Performs load balancing based on transport-layer destination port numbers in IPv4 packets.	-
l4-sport	Performs load balancing based on transport-layer source port numbers in IPv4 packets.	-
protocol	Performs load balancing based on protocol types in IPv4 packets.	-
sip	Performs load balancing based on source IP addresses in IPv4 packets.	-
sport	Performs load balancing based on physical-layer source port numbers in IPv4 packets.	-
vlan	Performs load balancing based on VLAN IDs in IPv4 packets.	-

Views

Load balancing profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **undo ipv4 field** command with no parameter specified restores the default load balancing mode of IPv4 packets. The **undo ipv4 field** command with a parameter specified deletes a specified load balancing mode of IPv4 packets.

Precautions

If you run the **ipv4 field** command multiple times, only the latest configuration takes effect.

On S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S switches, if **l4-dport** or **l4-sport** is specified for L2TP packets, load balancing is performed based on **session id** and **tunnel id** in L2TP packets rather than **l4-dport** and **l4-sport**.

On S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S switches, if **l4-dport** or **l4-sport** is specified for GTP packets, both outer and inner IP information are parsed when load balancing is performed for GTP packets; if another parameter is specified, only the outer IP information is parsed when load balancing is performed for GTP packets. For other switches, only the outer IP information of GTP packets is parsed when load balancing is performed.

Example

# In the load balancing profile **a**, set the load balancing mode of IPv4 packets to **sip** and **protocol**, that is, load balancing based on source IP addresses and protocol types of IPv4 packets.

```
<HUAWEI> system-view
[HUAWEI] load-balance-profile a
[HUAWEI-load-balance-profile-a] ipv4 field sip protocol
```

5.2.30 ipv6 field

Function

The **ipv6 field** command configures a load balancing mode of IPv6 packets in a load balancing profile.

The **undo ipv6 field** command deletes the load balancing mode of IPv6 packets or restores the default load balancing mode of IPv6 packets.

By default, load balancing of IPv6 packets is based on the source IP address (**sip**) and destination IP address (**dip**).

NOTE

Only the S5735S-H, S5736-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6720S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Format

ipv6 field [**dip** | **l4-dport** | **l4-sport** | **protocol** | **sip** | **sport** | **vlan**] *

undo ipv6 field [**dip** | **l4-dport** | **l4-sport** | **protocol** | **sip** | **sport** | **vlan**] *

NOTE

Only **dip**, **l4-dport**, **l4-sport**, **sip**, and **sport** are supported on the S5735S-H, S5736-S, andS6720S-S.

Parameters

Parameter	Description	Value
dip	Performs load balancing based on destination IP addresses in IPv6 packets.	-
l4-dport	Performs load balancing based on transport-layer destination port numbers in IPv6 packets.	-
l4-sport	Performs load balancing based on transport-layer source port numbers in IPv6 packets.	-
protocol	Performs load balancing based on protocol types in IPv6 packets.	-
sip	Performs load balancing based on source IP addresses in IPv6 packets.	-
sport	Performs load balancing based on physical-layer source port numbers in IPv6 packets.	-
vlan	Performs load balancing based on VLAN IDs in IPv6 packets.	-

Views

Load balancing profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **undo ipv6 field** command with no parameter specified restores the default load balancing mode of IPv6 packets. The **undo ipv6 field** command with a parameter specified deletes a specified load balancing mode of IPv6 packets.

Precautions

If you run the **ipv6 field** command multiple times, only the latest configuration takes effect.

On the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S switches, if **l4-dport** or **l4-sport** is specified for L2TP packets, load balancing is performed based on **session id** and **tunnel id** in L2TP packets rather than **l4-dport** and **l4-sport**.

Example

# In the load balancing profile **a**, set the load balancing mode of IPv6 packets to **sip** and **protocol**, that is, load balancing based on source IP addresses and protocol types of IPv6 packets.

```
<HUAWEI> system-view
[HUAWEI] load-balance-profile a
[HUAWEI-load-balance-profile-a] ipv6 field sip protocol
```

5.2.31 l2 field

Function

The **l2 field** command configures a load balancing mode of Layer 2 packets in a load balancing profile.

The **undo l2 field** command deletes the load balancing mode of Layer 2 packets or restores the default load balancing mode of Layer 2 packets.

By default, load balancing of Layer 2 packets is based on the source MAC address (**smac**) and destination MAC address (**dmac**).

NOTE

Only the S5735S-H, S5736-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6720S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Format

l2 field [**dmac** | **l2-protocol** | **smac** | **sport** | **vlan**] *

undo l2 field [**dmac** | **l2-protocol** | **smac** | **sport** | **vlan**] *

NOTE

Only **dmac**, **smac**, and **sport** are supported on the S5735S-H, S5736-S, and S6720S-S.

Parameters

Parameter	Description	Value
dmac	Performs load balancing based on destination MAC addresses in Layer 2 packets.	-

Parameter	Description	Value
l2-protocol	Performs load balancing based on protocol types in Layer 2 packets.	-
smac	Performs load balancing based on source MAC addresses in Layer 2 packets.	-
sport	Performs load balancing based on physical-layer source port numbers in Layer 2 packets.	-
vlan	Performs load balancing based on VLAN IDs in Layer 2 packets.	-

Views

Load balancing profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **undo l2 field** command with no parameter specified restores the default load balancing mode of Layer 2 packets. The **undo l2 field** command with a parameter specified deletes a specified load balancing mode of Layer 2 packets.

Precautions

If you run the **l2 field** command multiple times, only the latest configuration takes effect.

Example

# In the load balancing profile **a**, set the load balancing mode of Layer 2 packets to **l2-protocol**, that is, load balancing based on protocol types of Layer 2 packets.

```
<HUAWEI> system-view
[HUAWEI] load-balance-profile a
[HUAWEI-load-balance-profile-a] l2 field l2-protocol
```

5.2.32 lacp collector delay

Function

The **lacp collector delay** command configures the value of the **CollectorMaxDelay** field in an LACPDU.

The **undo lacp collector delay** command restores the default value of the **CollectorMaxDelay** field in an LACPDU.

The default value of the **CollectorMaxDelay** field is 0 in an LACPDU.

Format

lacp collector delay *delay-time*

undo lacp collector delay

Parameters

Parameter	Description	Value
delay-time	Specifies the value of the **CollectorMaxDelay** field in an LACPDU.	The value is an integer that ranges from 0 to 65535, in 10 microseconds.

Views

Eth-Trunk interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The default value of the **CollectorMaxDelay** field in LACPDUs sent by the device of different versions to the connected non-Huawei device is different. This may cause high CPU usage. You can run the **lacp collector delay** command to set the value of the **CollectorMaxDelay** field in LACPDUs.

Prerequisites

The Eth-Trunk has been configured to work in LACP mode using the **mode lacp** command.

Precautions

For a Huawei device, the valid value range of the **CollectorMaxDelay** field is 0 to 65535. Even though the member interfaces of the same Eth-Trunk receive LACPDUs with different **CollectorMaxDelay** values, the device can process the LACPDUs without deteriorating its CPU performance.

Example

# Set the value of the **CollectorMaxDelay** field to 65535.

```
<HUAWEI> system-view
[HUAWEI] interface eth-trunk 1
[HUAWEI-Eth-Trunk1] mode lacp
[HUAWEI-Eth-Trunk1] lacp collector delay 65535
```

5.2.33 lacp e-trunk priority

Function

The **lacp e-trunk priority** command sets the LACP priority of an E-Trunk.

The **undo lacp e-trunk priority** command cancels the configuration.

By default, the LACP priority of an E-Trunk is 32768.

NOTE

Only the S5720I-SI, S5735-S, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6720S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Format

lacp e-trunk priority *priority*

undo lacp e-trunk priority

Parameters

Parameter	Description	Value
priority	Specifies the LACP priority of an E-Trunk.	The value is an integer that ranges from 0 to 65535. A smaller value indicates a higher LACP priority.

Views

System view, Eth-Trunk interface view

Default Level

2: Configuration level

Usage Guidelines

The **lacp e-trunk priority** command sets the LACP priority of an E-Trunk. If the LACP priority is set, a member Eth-Trunk sends LACPDUs by using this LACP priority. If the LACP priority is not set, the default LACP priority 32768 is used.

The master and backup devices in an E-Trunk must use the same LACP priority.

When multiple E-Trunks are configured on the device, different LAGs can use different LACP priorities. You need to set the LACP priorities in the Eth-Trunk interface view.

The LACP priority configured in the system view is valid for all Eth-Trunks added to the E-Trunk. The LACP priority configured in the Eth-Trunk view takes effect only on the corresponding Eth-Trunk. If the LACP priorities are configured in both the Eth-Trunk interface view and system view, the LACP priority configured in the interface view takes effect.

NOTE

Ensure that the Eth-Trunk has been added to the E-Trunk before you run the **lacp e-trunk priority** command in the Eth-Trunk interface view.

Example

# Set the LACP priority of the E-Trunk to 1.

```
<HUAWEI> system-view
[HUAWEI] lacp e-trunk priority 1
```

5.2.34 lacp e-trunk system-id

Function

The **lacp e-trunk system-id** command sets the LACP system ID of an E-Trunk.

The **undo lacp e-trunk system-id** command cancels the configuration.

By default, the LACP system ID in the system view is the MAC address of the Ethernet interface.

NOTE

Only the S5720I-SI, S5735-S, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6720S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Format

lacp e-trunk system-id *mac-address*

undo lacp e-trunk system-id

Parameters

Parameter	Description	Value
system-id *mac-address*	Specifies the LACP system ID of an E-Trunk.	The value is in the format of H-H-H. An H contains 1 to 4 hexadecimal numbers, such as 00e0 and fc01. If you enter fewer than four digits, 0s are prefixed to the input digits. For example, if you enter e0, the system changes e0 to 00e0. The LACP system ID cannot be all 0s or all Fs.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

The **lacp e-trunk system-id** command sets the LACP system ID of an E-Trunk. If the system ID is set, a member Eth-Trunk sends LACPDUs by using this system ID. If the LACP system ID is not set, the MAC address of the Ethernet interface is used as the system ID.

The master and backup devices in an E-Trunk must use the same LACP system ID.

Example

# Set the LACP system ID of the E-Trunk to 00E0-FC00-0000.

```
<HUAWEI> system-view
[HUAWEI] lacp e-trunk system-id 00E0-FC00-0000
```

5.2.35 lacp force-switch

Function

The **lacp force-switch** command enables forcible switching when no preemption is configured for an Eth-Trunk interface in LACP mode or preemption is enabled but the delay is not reached.

By default, the switch does not enable forcible switching.

NOTE

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

Format

lacp force-switch

Parameters

None

Views

Eth-Trunk interface view

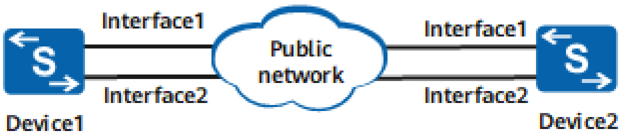
Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Figure 5-1 Eth-Trunk interface in LACP mode



As shown in **Figure 5-1**, when no service is bound to the MA (Maintenance Association), an Eth-Trunk interface in LACP mode is configured on two devices. interface1 where the MEP (Maintenance End Point) resides is the interface of the Eth-Trunk interface's primary link. When the **delay-measure two-way trigger if-down** or **loss-measure single-ended-synthetic trigger if-down** command is configured on interface1, interface1 is triggered to go ETHOAM down if Y.1731 detects that the primary link has poor quality. To ensure that services are not interrupted, run the **lacp track interface** command in the Eth-Trunk member interface view to increase the priority of the secondary member interface interface2. The secondary link then preempts the primary state, implementing an automatic primary/secondary link switchover.

When the primary link's quality recovers, run the **lacp force-switch** command to enable forcible switching if no preemption is configured or preemption is enabled but the delay is not reached.

Prerequisites

The **lacp track interface** command has been run to associate the secondary member interface of an Eth-Trunk interface in LACP mode with its primary member interface and to dynamically change the priority of the secondary member interface.

Precautions

An Eth-Trunk interface can have only two member interfaces. The maximum number of active links must be 1.

Example

# Enable forcible switching on Eth-Trunk 1.

```
<HUAWEI> system-view
[HUAWEI] interface eth-trunk 1
[HUAWEI-Eth-Trunk1] lacp force-switch
```

5.2.36 lacp force-forward

Function

The **lacp force-forward** command configures an Eth-Trunk member interface in Up state to forward data packets when the remote interface does not join the Eth-Trunk.

The **undo lacp force-forward** command restores the default setting.

By default, an Eth-Trunk member interface in Up state cannot forward data packets when the remote interface does not join the Eth-Trunk.

Format

lacp force-forward

undo lacp force-forward

Parameters

None

Views

Eth-Trunk interface view

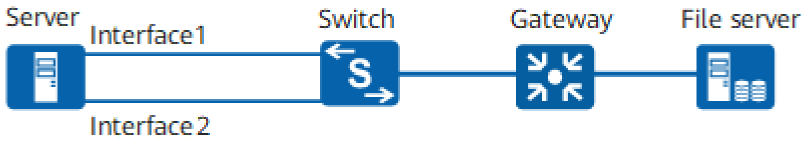
Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Figure 5-2 A switch directly connects to a server



In **Figure 5-2**, two interfaces of two network adapters on a server are directly connected to a switch. The switch is configured with an Eth-Trunk in LACP mode. The process on the server is as follows:

1. The server configures an IP address for Interface1 based the default configuration during startup, and sends a request to the remote file server through Interface1 and downloads the configuration file from the remote file server.

2. After the configuration file is downloaded successfully, the server aggregates two interfaces according to the configuration file. The server uses the two interfaces as Eth-Trunk member interfaces to perform LACP negotiation with the switch.

Before the server obtains the configuration file, Interface1 is an independent physical interface and is not configured with LACP. As a result, LACP negotiation on the switch interface fails. The switch does not forward traffic on the Eth-Trunk, and the server cannot download the configuration file through Interface1. In this case, the server cannot communicate with the switch.

To address this issue, run the **lacp force-forward** command on the Eth-Trunk of the switch. The Eth-Trunk member interface in Up state can still forward data packets even though the remote device is not enabled with LACP.

Prerequisites

The Eth-Trunk has been configured to work in LACP mode by using the **mode lacp** command.

Precautions

- With this command configured, an Eth-Trunk interface does not support Layer 3 forwarding and cannot be used to forward packets sent to the CPU. Only member interfaces in the ForceFwd state can forward Layer 2 traffic through hardware forwarding. The ForceFwd state is automatically set when LACP negotiation fails, and cannot be changed manually. You can use the **display eth-trunk** command to check the value of the Status field.
- This command applies to only the scenario where an Eth-Trunk joins a VLAN as an access, hybrid, trunk, and dot1q-tunnel interfaces.
- When a spanning tree protocol (for example, STP, RSTP, or MSTP) is used, the member interface in ForceFwd state cannot be blocked. That is, the member interface in ForceFwd state can continue to forward data packets. When other loop prevention protocols such as ERPS and RRPP are used, the member interface in ForceFwd state can be blocked. The blocked member interface in ForceFwd state cannot forward data packets.
- This command cannot be used with E-Trunk. That is, this command cannot be used on the Eth-Trunk that joins an E-Trunk.
- This command cannot be used with **max active-linknumber** or **least active-linknumber**.

Example

# Configure an Eth-Trunk member interface in Up state to forward data packets when the remote interface does not join the Eth-Trunk.

```
<HUAWEI> system-view
[HUAWEI] interface eth-trunk 1
[HUAWEI-Eth-Trunk1] mode lacp
[HUAWEI-Eth-Trunk1] lacp force-forward
```

5.2.37 lacp optimized-converge enable

Function

The **lacp optimized-converge enable** command enables optimized LACP convergence.

The **undo lacp optimized-converge enable** command disables optimized LACP convergence.

By default, optimized LACP convergence is disabled.

Format

lacp optimized-converge enable

undo lacp optimized-converge enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

When the working mode of an Eth-Trunk interface is set to LACP, Eth-Trunk member interfaces are configured to forward traffic after LACP negotiation and instruct services to reselect a route. Service traffic then can be properly forwarded. However, when multiple cards are restarted at the same time, Eth-Trunk member interfaces negotiate in preemption mode. As a result, Eth-Trunk member interfaces negotiate slowly, causing a large number of service packets to be lost.

After optimized LACP convergence is enabled using the **lacp optimized-converge enable** command, the device increases the LACP negotiation priority so that services can quickly detect Eth-Trunk member interface changes, accelerating Eth-Trunk traffic convergence.

Example

# Enable optimized LACP convergence.

```
<HUAWEI> system-view
[HUAWEI] lacp optimized-converge enable
```

5.2.38 lacp preempt delay

Function

The **lacp preempt delay** command sets the LACP preemption delay.

The **undo lacp preempt delay** command restores the default LACP preemption delay.

By default, the LACP preemption delay is 30 seconds.

Format

lacp preempt delay *delay-time*

undo lacp preempt delay

Parameters

Parameter	Description	Value
delay-time	Specifies the LACP preemption delay.	The value is an integer that ranges from 0 to 180 on the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S, 10 to 180 on other models, in seconds.

Views

Eth-Trunk interface view

Default Level

2: Configuration level

Usage Guidelines

To use this command, ensure that the following conditions are met:

- The Eth-Trunk has been configured to work in LACP mode using the **mode lacp** command in the Eth-Trunk interface view.
- Priority preemption has been enabled on the Eth-Trunk using the **lacp preempt enable** command in the Eth-Trunk interface view.

Link A replaces link B and becomes active after the preemption delay n the following situation:

1. LACP priority preemption is enabled and the **lacp preempt delay** command is used.

2. The faulty link (link A) with higher priority than that of the current active link (link B) recovers.
3. The number of current active links reaches the upper threshold.

If both devices of an Eth-Trunk use different preemption delays, a longer preemption delay is used. If priority preemption is enabled but the preemption delay is not set, the interface with a higher priority preempts the interface with a lower priority according to the default preemption delay.

Example

# Set the LACP preemption delay of Eth-Trunk 1 to 20 seconds.

```
<HUAWEI> system-view
[HUAWEI] interface eth-trunk 1
[HUAWEI-Eth-Trunk1] mode lacp
[HUAWEI-Eth-Trunk1] lacp preempt delay 20
```

5.2.39 lacp preempt enable

Function

The **lacp preempt enable** command enables priority preemption for an Eth-Trunk in LACP mode.

The **undo lacp preempt enable** command disables priority preemption for an Eth-Trunk in LACP mode.

By default, priority preemption is disabled.

Format

lacp preempt enable

undo lacp preempt enable

Parameters

None

Views

Eth-Trunk interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenarios

In LACP mode, when one of the active links fails, the system selects the link with the highest priority from backup links to replace the faulty one. When the faulty link recovers, the priority of this link is higher than the priority of the link that replaces itself, and priority preemption is enabled, the link becomes active again.

If priority preemption is disabled, the system does not re-select any active interface. The recovered link functions as the backup one.

When priority preemption is enabled, the system selects an active interface based on the LACP interface priority on the Actor.

Prerequisites

The LACP mode must have been configured using the **mode lacp** command in the Eth-Trunk interface view.

Precautions

To ensure that an Eth-Trunk works properly, enable or disable LACP preemption on both ends of the Eth-Trunk.

Example

# Enable priority preemption on Eth-Trunk 1.

```
<HUAWEI> system-view
[HUAWEI] interface eth-trunk 1
[HUAWEI-Eth-Trunk1] mode lacp
[HUAWEI-Eth-Trunk1] lacp preempt enable
```

5.2.40 lacp priority

Function

The **lacp priority** command sets the LACP system or interface priority.

The **undo lacp priority** command restores the default LACP system or interface priority.

By default, the LACP system or interface priority is 32768.

Format

lacp priority *priority*

undo lacp priority

Parameters

Parameter	Description	Value
priority	Specifies the LACP priority. A smaller value indicates a higher LACP priority.	The value is an integer that ranges from 0 to 65535.

Views

System view, Ethernet interface view, GE interface view, 25GE interface view, XGE interface view, MultiGE interface view, 40GE interface view, 100GE interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The LACP system priority is used to differentiate the local device and the remote device. The device of a higher LACP system priority is selected as the Actor of the link aggregate group (LAG), and active interfaces are selected according to interfaces of the Actor.

The LACP interface priority is used to differentiate interfaces on a device. The interface of a higher priority is selected as the active interface.

If devices at both ends of an Eth-Trunk are not configured with LACP system priorities, the devices use the default LACP system priority 32768 and the device with a smaller MAC address is selected as the Actor.

If priorities of different interfaces on a switch are not set, the default priority of interfaces is all 32768. Active interfaces are selected based on interface numbers and interfaces with smaller interface numbers are preferred.

Prerequisites

The interface has been added to the Eth-Trunk in LACP mode.

You can run the **mode lacp** command in the Eth-Trunk interface view to change the working mode of an Eth-Trunk to LACP.

Precautions

In LACP mode, active interfaces selected by devices at both ends of an Eth-Trunk link must be the same; otherwise, the link aggregation group cannot be set up.

If the **max active-linknumber** command is executed in LACP mode to set the upper threshold for the number of active interfaces, you need to determine the active interfaces when the number of interfaces manually added to an LAG exceeds the upper threshold. Setting the LACP interface priority ensures that interfaces with higher priorities become active ones in LACP mode.

If the **max active-linknumber** command is not used, the upper threshold for the number of active interfaces is 8. When the number of interfaces manually added to an LAG is smaller than 8, you do not need to select active interfaces because all interfaces are active.

If the **max active-linknumber** *link-number* command is run in the Eth-Trunk interface view, you need to run the **lacp preempt enable** command to enable LACP preemption on the current Eth-Trunk interface. Otherwise, interfaces with high LACP priorities may fail to be selected as active interfaces.

Example

# Set the LACP system priority to 1.

```
<HUAWEI> system-view
[HUAWEI] lacp priority 1
```

Set the LACP priority of GigabitEthernet0/0/1 to 1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet0/0/1
[HUAWEI-GigabitEthernet0/0/1] lacp priority 1
```

5.2.41 lacp priority-command-mode

Function

The **lacp priority-command-mode** command sets a Link Aggregation Control Protocol (LACP) system priority configuration mode.

The **undo lacp priority-command-mode** command restores the default LACP system priority configuration mode.

By default, the LACP system priority configuration mode is **default**.

Format

lacp priority-command-mode { **default** | **system-priority** }

undo lacp priority-command-mode

Parameters

Parameter	Description	Value
default	Sets the LACP system priority configuration mode to **default**. In **default** mode, the LACP system priority is configured using the **lacp priority** command in the system view.	-
system-priority	Sets the LACP system priority configuration mode to **system-priority**. In **system-priority** mode, the LACP system priority is configured using the **lacp system-priority** command in the system view.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A change in the LACP system priority will cause LACP renegotiation. During the renegotiation process, Eth-Trunk interfaces in LACP mode will go Down until the renegotiation succeeds, which may interrupt services. If the **lacp priority** command used to set the LACP interface priority is executed in the system view, the Eth-Trunk in LACP mode may alternate between Up and Down. To prevent this situation, run the **lacp priority-command-mode** command in the system view to set the configuration mode of the LACP system priority to **system-priority**. This mode can be used to differentiate the LACP system priority and LACP interface priority.

Precautions

When running the **lacp priority-command-mode** command, note the following points:

- If you specify **default** in the command, the LACP system priority and LACP interface priority configurations still use the same command (**lacp priority** *priority*).
- If you specify **system-priority** in the command, run the **lacp system-priority** *priority* command to configure the LACP system priority and run the **lacp priority** *priority* command to configure the LACP interface priority.

Example

# Set the LACP system priority configuration mode to **system-priority**.

```
<HUAWEI> system-view
[HUAWEI] lacp priority-command-mode system-priority
```

5.2.42 lacp selected

Function

The **lacp selected** command configures a mode for selecting active interfaces of an Eth-Trunk in LACP mode.

The **undo lacp selected** command restores the default mode for selecting active interfaces of an Eth-Trunk in LACP mode.

By default, active interfaces are selected based on the LACP interface priority.

Format

lacp selected { **priority** | **speed** }

undo lacp selected

Parameters

Parameter	Description	Value
priority	Indicates that active interfaces are selected based on the LACP interface priority. The interfaces with high priorities are preferentially selected as active interfaces.	-
speed	Indicates that active interfaces are selected based on the interface rate. High-speed interfaces are preferentially selected as active interfaces.	-

Views

Eth-Trunk interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

As defined in LACP, active interfaces are selected based on the LACP interface priority by default. If member interfaces of an Eth-Trunk in LACP mode work at different rates, low-speed interfaces may be selected as active interfaces. To enable the device to select high-speed interfaces as active interfaces, run the **lacp selected** command to set the mode of selecting active interfaces to **speed**.

To enable the device to select active interface based on the LACP interface priority, run the **lacp selected priority** command to set the mode of selecting active interfaces to **priority**.

Prerequisites

The Eth-Trunk has been configured to work in LACP mode using the **mode lacp** command in the Eth-Trunk interface view.

Precautions

Active interfaces are selected based on the LACP interface priority by default. Changing the mode for selecting active interfaces may cause service interruptions for a short time. You are advised not to change the mode for selecting active interfaces during service transmission.

You are advised not to bundle interfaces working at different rates into an Eth-Trunk in LACP mode because the priority preemption function may become ineffective.

Example

# Configure Eth-Trunk 1 in LACP mode and configure the device to select active interfaces based on the interface rate.

```
<HUAWEI> system-view
[HUAWEI] interface Eth-Trunk 1
[HUAWEI-Eth-Trunk1] mode lacp
[HUAWEI-Eth-Trunk1] lacp selected speed
```

5.2.43 lacp src-mac

Function

The **lacp src-mac** command configures an interface or system MAC address as an LACPDU's source MAC address.

The **undo lacp src-mac** command restores the default source MAC address.

By default, the system MAC address is used as an LACPDU's source MAC address.

Format

lacp src-mac { **bridge** | **port** }

undo lacp src-mac

Parameters

Parameter	Description	Value
bridge	Configures the system MAC address as an LACPDU's source MAC address.	-
port	Configures an interface MAC address as an LACPDU's source MAC address.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

When a Huawei device connects to a non-Huawei device through Eth-Trunk interfaces in static LACP mode, if the Huawei device uses the default system MAC address, whereas the non-Huawei device uses the MAC addresses of the Eth-Trunk member interfaces as LACPDUs' source MAC addresses, the non-Huawei device may consider the received LACPDUs with the same MAC address invalid and therefore discard them, leading to an LACP negotiation failure.

To ensure a successful LACP negotiation, run the **lacp src-mac port** command to configure the Huawei device to use interface MAC addresses as LACPDUs' source MAC addresses.

Example

# Configure interface MAC addresses as LACPDUs' source MAC addresses.

```
<HUAWEI> system-view
[HUAWEI] lacp src-mac port
```

5.2.44 lacp system-id

Function

The **lacp system-id** command configures a Link Aggregation Control Protocol (LACP) system ID for an Eth-Trunk.

The **undo lacp system-id** command restores the default configuration.

By default, the system bridge MAC address functions as the LACP system ID of an Eth-Trunk.

NOTE

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

Format

lacp system-id *mac-address*

undo lacp system-id [*mac-address*]

Parameters

Parameter	Description	Value
mac-address	Specifies the LACP system ID of an Eth-Trunk.	The value is in the format of H-H-H. Each H is a 4-digit hexadecimal number. You can enter 1 to 4 digits, such as 00e0 or fc01. If an H contains fewer than four digits, 0s are added ahead. For example, e0 is equal to 00e0. **NOTE** The LACP system ID of an Eth-Trunk cannot be all 0s.

Views

Eth-Trunk interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When multiple E-Trunks are configured on the device, the link aggregation groups can use different LACP system IDs. You need to run the **lacp system-id** *mac-address* command to set the LACP system ID.

The LACP system ID configured using the **lacp e-trunk system-id** command in the system view is valid for all Eth-Trunks that are added to the E-Trunk. The LACP system ID configured using the **lacp system-id** *mac-address* command in the Eth-Trunk interface view is valid for only the Eth-Trunk. If the LACP system ID is configured in both the Eth-Trunk interface view and system view, the system ID configured in the Eth-Trunk interface view takes effect.

Prerequisites

The Eth-Trunk has been configured to work in LACP mode using the **mode lacp** command.

Example

# Configure 00e0-fc00-0000 as the LACP system ID of Eth-Trunk 10.

```
<HUAWEI> system-view
[HUAWEI] interface eth-trunk 10
[HUAWEI-Eth-Trunk10] mode lacp
[HUAWEI-Eth-Trunk10] lacp system-id 00e0-fc00-0000
```

5.2.45 lacp system-priority

Function

The **lacp system-priority** command configures a Link Aggregation Control Protocol (LACP) system priority.

The **undo lacp system-priority** command restores the default LACP system priority.

The default LACP system priority is 32768.

Format

lacp system-priority *priority*

undo lacp system-priority

Parameters

Parameter	Description	Value
priority	Specifies an LACP system priority.	The value is an integer ranging from 0 to 65535. A smaller value indicates a higher LACP priority.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The system priority is set to differentiate the priority of the local device and the peer device. The system of a higher priority is selected as the Actor of the link aggregate group (LAG), and active interfaces are selected according to interfaces of the Actor.

If the devices on both ends of the Eth-Trunk are not configured with system priorities, the devices use the default priority 32768. In this case, the Actor is selected according to the system MAC. The system with a smaller MAC is selected as the Actor.

A change in the LACP system priority will cause LACP renegotiation. During the renegotiation process, Eth-Trunk interfaces in LACP mode will go Down until the renegotiation succeeds, which may interrupt services. If the **lacp priority** command used to set the LACP interface priority is executed in the system view, the Eth-Trunk in LACP mode may alternate between Up and Down. To prevent this situation, run the **lacp priority-command-mode** command in the system view to set the configuration mode of the LACP system priority to **system-priority**. This mode can be used to differentiate the LACP system priority and LACP interface priority.

When running the **lacp priority-command-mode** command, note the following points:

- If you specify **default** in the command, the LACP system priority and LACP interface priority configurations still use the same command (**lacp priority** *priority*).
- If you specify **system-priority** in the command, run the **lacp system-priority** *priority* command to configure the LACP system priority and run the **lacp priority** *priority* command to configure the LACP interface priority.

Prerequisites

The **lacp priority-command-mode system-priority** command has been executed in the system view to set the configuration mode of the LACP system priority to **system-priority**.

Example

# Set the LACP system priority to 10.

```
<HUAWEI> system-view
[HUAWEI] lacp priority-command-mode system-priority
[HUAWEI] lacp system-priority 10
```

5.2.46 lacp timeout

Function

The **lacp timeout** command configures the timeout interval for an Eth-Trunk in LACP mode to receive LACPDUs.

The **undo lacp timeout** command restores the default timeout interval.

By default, the timeout interval for an Eth-Trunk to receive LACPDUs is 90s.

Format

lacp timeout { **fast** [**user-defined** *user-defined*] | **slow** }

undo lacp timeout

Parameters

Parameter	Description	Value
fast	Indicates that the timeout interval for an Eth-Trunk in LACP mode to receive LACPDUs is 3 seconds. If **fast** is specified, the remote device sends an LACPDU every 1 second. In this mode, the local device can quickly respond to LACPDUs from the remote device but consumes more system resources compared with the **slow** mode.	-
user-defined *user-defined*	Specifies the timeout interval for an Eth-Trunk to receive LACPDUs when **fast** is specified.	The value is an integer that ranges from 3 to 90, in seconds.
slow	Indicates that the timeout interval for an Eth-Trunk in LACP mode to receive LACPDUs is 90 seconds. If **slow** is specified, the remote device sends an LACPDU every 30 seconds. In this mode, the local device responds to LACPDUs from the remote device slowly but consumes fewer system resources compared with the **fast** mode. The timeout interval on the two ends can be different. To facilitate maintenance, you are advised to set the same timeout interval at both ends.	-

Views

Eth-Trunk interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If two devices are connected through three GE interfaces at each end and the three GE interfaces are bundled into an Eth-Trunk, you can run the **mode lacp** command to configure the Eth-Trunk to work in LACP mode and run the **least active-linknumber** *link-number* command to set the lower threshold for the number of active interfaces to 2.

If the Eth-Trunk on the local device cannot detect a self-loop or fault that occurred on a member interface in the LAG on the remote device, the local Eth-Trunk still has three member interfaces in Up state and the three member interfaces still load balance data, causing packet loss. To ensure reliable data transmission, run the **lacp timeout** command to set the timeout interval for the Eth-Trunk to receive LACPDUs. If a local member interface does not receive any LACPDU within the configured timeout interval, it becomes Down immediately and no longer forwards data.

The number of Up member interfaces does not fall below the configured lower threshold for the number of active interfaces, so the Eth-Trunk is still Up. In this case, data is load balanced between the two member interfaces in Up state and reliably transmitted to the remote end.

Prerequisites

The Eth-Trunk has been configured to work in LACP mode using the **mode lacp** command in the Eth-Trunk interface view.

Precautions

After the timeout interval is successfully configured, pay attention to the following points:

- If **fast** is specified, the remote device sends an LACPDU every 1 second.
- If **slow** is specified, the remote device sends an LACPDU every 30 seconds.

The timeout interval configured on an Eth-Trunk takes effect on all its member interfaces.

Example

# Set the timeout interval for Eth-Trunk 1 to receive LACPDUs to 3 seconds.

```
<HUAWEI> system-view
[HUAWEI] interface eth-trunk 1
[HUAWEI-Eth-Trunk1] mode lacp
[HUAWEI-Eth-Trunk1] lacp timeout fast
```

5.2.47 lacp track interface

Function

The **lacp track interface** command associates the secondary member interface of an Eth-Trunk interface in LACP mode with its primary member interface and dynamically changes the priority of the secondary member interface.

The **undo lacp track interface** command restores the default configuration.

By default, the secondary member interface of an Eth-Trunk interface in LACP mode is not associated with its primary member interface.

NOTE

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

Format

lacp track interface *interface-type interface-number* **priority-reduced** *value*

undo lacp track interface *interface-type interface-number* **priority-reduced** *value*

Parameters

Parameter	Description	Value
interface-type interface-number	Specifies the type and number of an associated physical interface.	-
priority-reduced *value*	Specifies a value by which the priority is reduced. **NOTE** The new priority of the secondary member interface is the configured priority minus the value specified by **priority-reduced** *value*. The new priority of the secondary member interface must be less than the priority of the primary member interface.	The value is an integer ranging from 0 to 65535.

Views

Eth-Trunk member interface view

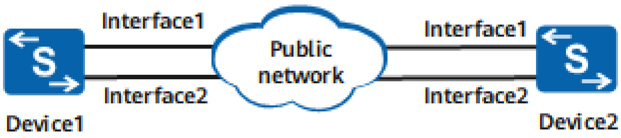
Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Figure 5-3 Eth-Trunk interface in LACP mode



As shown in **Figure 5-3**, when no service is bound to the MA, an Eth-Trunk interface in LACP mode is configured on two devices. interface1 where the MEP resides is the interface of the Eth-Trunk interface's primary link. When the **delay-measure two-way trigger if-down** or **loss-measure single-ended-synthetic trigger if-down** command is configured on interface1, interface1 is triggered to go ETHOAM down if Y.1731 detects that the primary link has poor quality.

To ensure that services are not interrupted, run the **lacp track interface** command in the Eth-Trunk member interface view to increase the priority of the secondary member interface interface2. The secondary link then preempts the primary state, implementing an automatic primary/secondary link switchover.

Prerequisites

An Eth-Trunk interface has been configured to work in LACP mode using the **mode lacp** command in the Eth-Trunk interface view.

Precautions

An Eth-Trunk interface can have only two member interfaces. The maximum number of active links must be 1.

The **lacp track interface** command must be configured on the secondary member interface of an Eth-Trunk interface's Actor.

The secondary member interface must not be associated with another interface.

If the **lacp track interface** command has been run and the primary link has poor quality, the primary interface is triggered to go ETHOAM down. If the secondary link also has poor quality, a primary/secondary switchover is also performed because Y.1731 performance detection is not configured for the secondary link.

If the **lacp track interface** command has been run and the primary link has poor quality, the primary interface is triggered to go ETHOAM down. If the **undo lacp track interface** command is run to delete the configuration, two links cannot be selected within the timeout period. As a result, traffic is interrupted. Services can be restored only after the timeout period elapses.

Example

# Associate the secondary member interface GE 0/0/1 of an Eth-Trunk interface in LACP mode with its primary member interface GE 0/0/2, and set a value by which the priority is reduced to 100 when the status of the primary member interface changes to ETHOAM down.

```
<HUAWEI> system-view
[HUAWEI] interface eth-trunk 1
[HUAWEI-Eth-Trunk1] mode lacp
[HUAWEI-Eth-Trunk1] trunkport GigabitEthernet 0/0/1 to 0/0/2
[HUAWEI-Eth-Trunk1] max active-linknumber 1
[HUAWEI-Eth-Trunk1] quit
[HUAWEI] interface GigabitEthernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] lacp track interface GigabitEthernet 0/0/2 priority-reduced 100
```

5.2.48 least active-linknumber

Function

The **least active-linknumber** command sets the lower threshold for the number of active interfaces in an Eth-Trunk.

The **undo least active-linknumber** command restores the default lower threshold for the number of active interfaces in an Eth-Trunk.

By default, the lower threshold for the number of active interfaces in an Eth-Trunk is 1.

Format

least active-linknumber *link-number*

undo least active-linknumber

Parameters

Parameter	Description	Value
link-number	Specifies the lower threshold for the number of active interfaces in an Eth-Trunk.	The value is an integer that ranges from 1 to 32 on the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S, 1 to 16 on the S5735S-H, S5736-S, and S6720S-S, and 1 to 8 on other models. On the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, S6730S-S, S6735-S, S6720-EI, and S6720S-EI, you can run the **assign trunk** command to set the value, and run the **display trunk configuration** command to check the configuration.

Views

Eth-Trunk interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The number of active interfaces in an Eth-Trunk affects the status and bandwidth of the Eth-Trunk. The bandwidth of an Eth-Trunk is equal to the total bandwidth of all member interfaces in Up state.

The number of Up member links affects the status and bandwidth of an Eth-Trunk. To ensure that the Eth-Trunk functions properly and is less affected by member link status changes, set the following thresholds.

- Lower threshold for the number of active interfaces

  When the number of active interfaces falls below this threshold, the Eth-Trunk goes Down. This guarantees the Eth-Trunk a minimum available bandwidth.

  For example, if the Eth-Trunk is required to provide a minimum bandwidth of 2 Gbit/s and each member link's bandwidth is 1 Gbit/s, the lower threshold for the number of active interfaces must be set to 2 or larger.

- Upper threshold for the number of active interfaces

  When the number of active interfaces reaches this threshold, the bandwidth of the Eth-Trunk will not increase even if more member links go Up. This guarantees higher network reliability.

  To set the upper threshold for the number of active interfaces, use the **max active-linknumber** command.

To delete the configured lower threshold or restore the default lower threshold, use the **undo least active-linknumber** or **least active-linknumber 1** command.

Prerequisites

The Eth-Trunk has been correctly configured.

Precautions

If you run the **least active-linknumber** command multiple times, only the latest configuration takes effect.

After the lower threshold for the number of active interfaces is configured, the following situations may occur:

- The Eth-Trunk goes Down when the number of active interfaces falls below the configured lower threshold.
- The Eth-Trunk goes Up when the number of active interfaces reaches the configured lower threshold.

If the **max active-linknumber** command has been configured before you run the **least active-linknumber** command, ensure that the lower threshold for the number of active interfaces is less than or equal to the upper threshold for the number of active interfaces.

Example

# Set the lower threshold for the number of active interfaces to 3.

```
<HUAWEI> system-view
[HUAWEI] interface eth-trunk 1
[HUAWEI-Eth-Trunk1] least active-linknumber 3
```

5.2.49 load-balance

Function

The **load-balance** command sets a load balancing mode of an Eth-Trunk.

The **undo load-balance** command restores the default load balancing mode of an Eth-Trunk.

The default load balancing mode is **src-dst-ip**.

Format

load-balance { **dst-ip** | **dst-mac** | **src-ip** | **src-mac** | **src-dst-ip** | **src-dst-mac** | **enhanced profile** *profile-name* }

undo load-balance

NOTE

Only S5735S-H, S5736-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6720S-S, S6730-H, S6730S-H, S6730-S and S6730S-S support **enhanced profile** *profile-name*.

Parameters

Parameter	Description	Value
dst-ip	Indicates load balancing based on destination IP addresses.	-
dst-mac	Indicates load balancing based on destination MAC addresses.	-
src-ip	Indicates load balancing based on source IP addresses.	-
src-mac	Indicates load balancing based on source MAC addresses.	-
src-dst-ip	Indicates load balancing based on source and destination IP addresses.	-
src-dst-mac	Indicates load balancing based on source and destination MAC addresses.	-
enhanced profile *profile-name*	Indicates the name of the profile used to configure enhanced load balancing.	The value is a string of 1 to 31 characters.

Views

Eth-Trunk interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To ensure proper load balancing between physical links of an Eth-Trunk and avoid link congestion, use the **load-balance** command to set the load balancing mode of the Eth-Trunk.

Load balancing is valid only for outgoing traffic; therefore, the load balancing modes for the interfaces at both ends of the link can be different and do not affect each other.

You can set the load balancing mode based on traffic models. When a parameter of traffic changes frequently, you can set the load balancing mode based on this parameter to ensure that the traffic is load balanced evenly. For example, if IP addresses in packets change frequently, use the load balancing mode based on **dst-ip**, **src-ip**, or **src-dst-ip** so that traffic can be properly load balanced among physical links. If MAC addresses in packets change frequently and IP addresses are fixed, use the load balancing mode based on **dst-mac**, **src-mac**, or **src-dst-mac** so that traffic can be properly load balanced among physical links.

After the **load-balance** command is run to configure the load balancing mode for an Eth-Trunk, the hash factors used to calculate the outbound interface vary according to the packet type and device model. For example, after you configure load balancing based on the source and destination IP addresses for an Eth-Trunk, Layer 2 packets are load balanced automatically based on the source and destination MAC addresses because Layer 2 packets do not contain the source and destination IP addresses. You can run the **display eth-trunk load-balance** command to check the hash factors used when the outbound interface is calculated.

Prerequisites

Ensure that the **load-balance-profile** *profile-name* command has been executed to create a load balancing profile before you run the **load-balance enhanced profile** *profile-name* command.

Precautions

If you run the **load-balance** command multiple times, only the latest configuration takes effect.

When an inter-device Eth-Trunk is configured in a stack and the local device has Eth-Trunk member interfaces and the member interfaces function properly, only the Eth-Trunk member interfaces on the local device participate in load balancing. To enable Eth-Trunk member interfaces on other devices participate in load balancing, run the **undo local-preference enable** command to configure the Eth-Trunk not to preferentially forward local traffic.

If the value of *member-number* configured for an Eth-Trunk using the **assign trunk** { **trunk-group** *group-number* | **trunk-member** *member-number* }* command is larger than 16 on the S6735-S, S6720-EI and S6720S-EI or larger than 32 on the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S, only the enhanced mode can be used for load balancing. If the enhanced mode is not used, problems such as packet loss and uneven load balancing may occur.

NOTE

The SS1720GW-E, S1720GWR-E, S5720I-SI, S5720-LI, S5720S-LI, S5735S-H, S5736-S, and S6720S-S use the **src-dst-ip**, source TCP or UDP port number, and destination TCP or UDP port number in the hash algorithm for load balancing regardless of whether you configure this parameter.

The S1720GW-E, S1720GWR-E, S5720I-SI, S5720-LI, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5720S-LI, S5735-S, S500, S5735S-S, S5735-S-I, S5735S-H, S5736-S, and S6720S-S support only one load balancing mode globally. If the load balancing mode of an Eth-Trunk is modified, the modification takes effect on all Eth-Trunks. If an Eth-Trunk is created, the load balancing mode of the Eth-Trunk is the same as that of the original Eth-Trunks on the switch.

On the S6735-S, S6720-EI and S6720S-EI, when the **load-balance** command is run to configure the load balancing mode for an Eth-Trunk, whether the TCP or UDP port number is involved in the hash operation depends on the **ecmp load-balance** command. If the default setting is used or the **port** parameter is specified in the **ecmp load-balance** command, the TCP or UDP port number is involved in the hash operation when the dst-ip, src-ip, or src-dst-ip load balancing mode is configured for an Eth-Trunk.

On the S5731-H, S5731-S, S5731S-S, S5731S-H, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S, when you run the **load-balance** { **dst-ip** | **dst-mac** | **src-ip** | **src-mac** | **src-dst-ip** | **src-dst-mac** } command to configure the load balancing mode for an Eth-Trunk, regardless of which parameter is specified, packets are load balanced based on physical-layer source port numbers in the packets.

Example

# Set the load balancing mode of Eth-Trunk 1 to **dst-mac**.

```
<HUAWEI> system-view
[HUAWEI] interface Eth-Trunk 1
[HUAWEI-Eth-Trunk1] load-balance dst-mac
```

5.2.50 load-balance-profile

Function

The **load-balance-profile** command creates a load balancing profile and displays the load balancing profile view.

The **undo load-balance-profile** command deletes a load balancing profile.

By default, there is not a load balancing profile on the device.

NOTE

Only the S5735S-H, S5736-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6720S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Format

load-balance-profile *profile-name*

undo load-balance-profile *profile-name*

Parameters

Parameter	Description	Value
profile-name	Specifies the name of a load balancing profile.	The value is a string of 1 to 31 characters.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Before setting the load balancing mode, create a load balancing profile.

Only one load balancing profile can be created.

NOTE

If VLAN mapping, VLAN stacking, or VLAN re-marking of the ACL is configured on an inbound interface, and a load balancing profile is configured on an inter-device Eth-Trunk outbound interface, you are advised not to choose the VLAN-based load balancing mode when running the **mpls field**, **l2 field**, **ipv4 field**, and **ipv6 field** commands.

Example

# Create a load balancing profile named **a**.

```
<HUAWEI> system-view
[HUAWEI] load-balance-profile a
[HUAWEI-load-balance-profile-a]
```

5.2.51 load-distribution active-linknumber-change

Function

The **load-distribution active-linknumber-change** command configures the number of interfaces in an Eth-Trunk where load balancing calculation is performed.

The **undo load-distribution active-linknumber-change** command cancels the configuration.

By default, the number of interfaces in an Eth-Trunk where load balancing calculation is performed is the number of active interfaces of the device.

NOTE

Only the SS1720GW-E, S1720GWR-E, S5720-LI, S5720S-LI, and S5720I-SI support this command.

Format

load-distribution active-linknumber-change *link-number1* **to** *link-number2*

undo load-distribution active-linknumber-change [*link-number1*]

Parameters

Parameter	Description	Value
link-number1	Specifies the number of active interfaces in an Eth-Trunk.	The value is an integer that ranges from 2 to 7.
link-number2	Specifies the number of interfaces in an Eth-Trunk where load balancing calculation is performed.	The value is an integer that ranges from 3 to 8. **NOTE** When this command is used, *link-number2* must be larger than *link-number1*.

Views

Eth-Trunk interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

By default, the number of interfaces in an Eth-Trunk where load balancing calculation is performed is the number of active interfaces of the device. If the number of active interfaces is smaller than 8 and traffic on an Eth-Trunk is unevenly load balanced, you can run the **load-distribution active-linknumber-change** command to increase the number of interfaces in the Eth-Trunk where load balancing calculation is performed so that traffic can be better load balanced among active links.

The **load-distribution active-linknumber-change** *link-number1* **to** *link-number2* command with different values of *link-number1* can be configured repeatedly. When the number of active interfaces is the same as the value of *link-number1*, the configuration takes effect. If the **load-distribution active-linknumber-change** *link-number1* **to** *link-number2* command with the same value of *link-number1* is configured, only the latest configuration takes effect.

Precautions

When an inter-device Eth-Trunk is configured in a iStack and the **local-preference enable** command is used to configure an Eth-Trunk to preferentially forward local traffic, the number of interfaces in the Eth-Trunk where load balancing calculation is performed is the number of active interfaces.

This command is effective only for known unicast packets.

Example

# Set the number of interfaces in Eth-Trunk 1 where load balancing calculation is performed to 8 when Eth-Trunk 1 has four active interfaces.

```
<HUAWEI> system-view
[HUAWEI] interface eth-trunk 1
[HUAWEI-Eth-Trunk1] load-distribution active-linknumber-change 4 to 8
```

5.2.52 load-distribution active-linknumber-change global

Function

The **load-distribution active-linknumber-change global** command specifies the number of Eth-Trunk interfaces participating in load balancing calculation in the system view.

The **undo load-distribution active-linknumber-change global** command cancels the configuration.

By default, the number of member interfaces that participate in load balancing calculation in all Eth-Trunks is the number of active interfaces in the Eth-Trunks.

NOTE

Only the SS1720GW-E, S1720GWR-E, S5720-LI, S5720S-LI, and S5720I-SI support this command.

Format

load-distribution active-linknumber-change *link-number1* **to** *link-number2* **global**

undo load-distribution active-linknumber-change [*link-number1*] **global**

Parameters

Parameter	Description	Value
link-number1	Specifies the number of active interfaces in an Eth-Trunk.	The value is an integer in the range from 2 to 7.
link-number2	Specifies the number of interfaces in an Eth-Trunk where load balancing calculation is performed.	The value is an integer in the range from 3 to 8. **NOTE** When this command is used, *link-number2* must be larger than *link-number1*.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

By default, the number of interfaces in an Eth-Trunk where load balancing calculation is performed is the number of active interfaces of the device. If the number of active interfaces is smaller than 8 and traffic on an Eth-Trunk is unevenly load balanced, you can run the **load-distribution active-linknumber-change global** command to set the number of Eth-Trunk interfaces participating in load balancing calculation to a larger value in the system view to better load balance traffic.

The **load-distribution active-linknumber-change** *link-number1* **to** *link-number2* **global** command with different values of *link-number1* can be configured repeatedly. When the number of active interfaces is the same as the value of *link-number1*, the configuration takes effect. If the **load-distribution active-linknumber-change** *link-number1* **to** *link-number2* **global** command with the same value of *link-number1* is configured, only the latest configuration takes effect.

Precautions

- When an inter-device Eth-Trunk is configured in an iStack and the **local-preference enable** command is used to configure an Eth-Trunk to preferentially forward local traffic, the number of interfaces in the Eth-Trunk where load balancing calculation is performed is the number of active interfaces.
- This command is effective only for known unicast packets.
- If the number of Eth-Trunk interfaces participating in load balancing calculation is configured in both the system view and Eth-Trunk interface view, the configuration in the Eth-Trunk interface view takes effect.

Example

# Set the number of Eth-Trunk interfaces participating in load balancing calculation to 8 when the Eth-Trunks have four active interfaces.

```
<HUAWEI> system-view
[HUAWEI] load-distribution active-linknumber-change 4 to 8 global
```

5.2.53 local-preference enable

Function

The **local-preference enable** command configures an Eth-Trunk to preferentially forward local traffic.

The **local-preference disable** command configures an Eth-Trunk not to preferentially forward local traffic.

The **undo local-preference enable** command configures an Eth-Trunk not to preferentially forward local traffic.

By default, an Eth-Trunk is enabled to preferentially forward local traffic.

NOTE

The S5735-S-I, S5720I-10X-PWH-SI-AC, and S5720I-6X-PWH-SI-AC do not support this configuration.

Format

local-preference { **enable** | **disable** }

undo local-preference enable

NOTE

The S2730S-S, 5735-L1, S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, and S5735S-S do not support the **local-preference disable**.

Parameters

None

Views

System view (S2730S-S, S5735-L-I, S5735-L1, S300, S5735-L, S5735S-L1, S5735S-L, S5735-S, S5735S-S, S5735S-L-M, S500)

Eth-Trunk interface view (Other models excluding the S2730S-S, S5735-L-I, S5735-L1, S300, S5735-L, S5735S-L1, S5735S-L, S5735-S, S5735S-L-M, S500)

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In a stack, an Eth-Trunk is configured to be the outbound interface of traffic to ensure reliable transmission. Member interfaces of the Eth-Trunk may be located on different devices. When the stack device forwards traffic, the Eth-Trunk may select an inter-device member interface based on the hash algorithm. This forwarding mode occupies bandwidth resources between devices and reduces traffic forwarding efficiency.

To solve the problem, run the **local-preference enable** command to enable the Eth-Trunk to preferentially forward local traffic. Then traffic arriving at the local device is preferentially forwarded through member interfaces of the local device. If there is no member interface on the local device, member interfaces on another device are used to forward traffic. This forwarding mode effectively saves inter-device bandwidth resources and improves traffic forwarding efficiency.

- When the local device has Eth-Trunk member interfaces and the member interfaces function properly, the Eth-Trunk forwarding table of the local device contains only local Eth-Trunk member interfaces. Therefore, the hash algorithm selects a local member interface, and traffic is forwarded through the local device.

- When the local device does not have any Eth-Trunk member interfaces or all member interfaces fail, the Eth-Trunk forwarding table of the local device contains all available Eth-Trunk member interfaces. The hash algorithm selects a member interface on another device, and traffic is forwarded through this device.

Precaution

Member interfaces of the local Eth-Trunk have sufficient bandwidth to forward local interface traffic, which prevents packet loss.

This function is only valid for known unicast packets, and is invalid for broadcast, unknown-unicast, and multicast (BUM) packets.

Example

# Configure an Eth-Trunk not to preferentially forward local traffic.

```
<HUAWEI> system-view
[HUAWEI] interface Eth-Trunk 10
[HUAWEI-Eth-Trunk10] undo local-preference enable
```

5.2.54 max active-linknumber

Function

The **max active-linknumber** command sets the upper threshold for the number of active interfaces in an Eth-Trunk.

The **undo max active-linknumber** command restores the default upper threshold for the number of active interfaces in an Eth-Trunk.

By default, the upper threshold for the number of active interfaces in an Eth-Trunk is 32 on the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S, 16 on the S5735S-H, S5736-S, and S6720S-S, and 8 on other models.

Format

max active-linknumber *link-number*

undo max active-linknumber

Parameters

Parameter	Description	Value
link-number	Specifies the upper threshold for the number of active interfaces.	The value is an integer that ranges from 1 to 32 on the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S, 1 to 16 on the S5735S-H, S5736-S, and S6720S-S, and 1 to 8 on other models. On the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, S6730S-S, S6735-S, S6720-EI, and S6720S-EI, you can run the **assign trunk** command to set the value, and run the **display trunk configuration** command to check the configuration.

Views

Eth-Trunk interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The number of active interfaces in an Eth-Trunk affects the status and bandwidth of the Eth-Trunk. The bandwidth of an Eth-Trunk is equal to the total bandwidth of all member interfaces in Up state.

The number of Up member links affects the status and bandwidth of an Eth-Trunk. To ensure that the Eth-Trunk functions properly and is less affected by member link status changes, set the following thresholds.

- Lower threshold for the number of active interfaces

  When the number of active interfaces falls below this threshold, the Eth-Trunk goes Down. This guarantees the Eth-Trunk a minimum available bandwidth.

  For example, if the Eth-Trunk is required to provide a minimum bandwidth of 2 Gbit/s and each member link's bandwidth is 1 Gbit/s, the minimum number of Up member links must be set to 2 or larger.

  To set the lower threshold for the number of active interfaces, run the **least active-linknumber** command.

- Upper threshold for the number of active interfaces

  When the number of active interfaces reaches this threshold, the bandwidth of the Eth-Trunk will not increase even if more member links go Up. The upper threshold is used to improve network reliability with assured bandwidth.

Prerequisites

The Eth-Trunk has been correctly configured.

Precautions

- If you run the **max active-linknumber** command multiple times, only the latest configuration takes effect.
- The **max active-linknumber** command is valid only in LACP mode.
- If the number of member interfaces added to an Eth-Trunk is less than the upper threshold, there is no backup interface.
- After you run this command, if the number of current active interfaces reaches the upper threshold, new member interfaces function as the backup interfaces.
- If the **least active-linknumber** command has been configured before you run the **max active-linknumber** command, ensure that the maximum number of active member links is greater than or equal to the minimum number of active member links.
- The upper thresholds configured by the **max active-linknumber** command on both ends must be the same; otherwise, the Eth-Trunk status flaps if an active interface fails.
- In the scenario where the Eth-Trunk in 1:N LACP mode is used, the upper threshold for the number of Eth-Trunk member links in Up state is 1. After the active link becomes Down and before the backup link switches to the active link, the Down event of the original active link is not reported to the Eth-Trunk. To prevent route re-calculation caused by the Eth-Trunk Down event, the Down event of the original active link is reported to the Eth-Trunk in any of the following situations:
  - The timeout interval (60s) for reporting the Down event has been expired.
  - The backup link goes Up and becomes the active link.
  - The backup link fails and cannot go Up.

  The preceding implementation is inapplicable to scenarios where association between Eth-Trunk in E-Trunk or LACP mode and VRRP is configured.
- When a Huawei switch connects to a non-Huawei device, if the maximum number of active links at both ends is smaller than the number of all active interfaces of the Eth-Trunk, a link is interrupted suddenly especially in 1:1 mode. As a result, LACP negotiation results at both ends are different and the Eth-Trunk in Down state cannot be restored. It is recommended that LACP preemption be enabled and the same preemption delay be set at both ends or the maximum number of active links be not set at both ends.

  NOTE

  The 1:1 mode indicates that the maximum number of active links at both ends of an Eth-Trunk is 1 and two member interfaces join an Eth-Trunk at both ends.

Example

# Set the upper threshold for the number of active interfaces in Eth-Trunk 1 to 3.

```
<HUAWEI> system-view
[HUAWEI] interface eth-trunk 1
[HUAWEI-Eth-Trunk1] mode lacp
[HUAWEI-Eth-Trunk1] max active-linknumber 3
```

5.2.55 mixed-rate link enable

Function

The **mixed-rate link enable** command adds interfaces with different interface types to the same Eth-Trunk.

The **undo mixed-rate link enable** command disables interfaces with different interface types from being added to the same Eth-Trunk.

By default, interfaces with different interface types are not allowed to be added to the same Eth-Trunk.

Format

mixed-rate link enable

undo mixed-rate link enable

Parameters

None

Views

Eth-Trunk interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can run the **mixed-rate link enable** command to add interfaces with different rates to the same Eth-Trunk. If a member interface of an Eth-Trunk is a GE interface and the transmission bandwidth needs to be increased, you can enable this function when the GE interface needs to be changed to an XGE interface. During switching, add the XGE interface to the Eth-Trunk and then delete the GE interface. In this way, the service interruption time during the switching process can be reduced.

Precautions

- In LACP mode, if the peer device does not support this function, interfaces with different rates cannot be successfully added to the same Eth-Trunk even if the local device has the function enabled.

- In LACP mode, when Eth-Trunk negotiation succeeds, modifying the configuration of this command triggers a renegotiation, which can cause an LACP flap.
- In manual mode, if the peer device allows only interfaces with the same rate to be added to the same Eth-Trunk, traffic forwarded by all interfaces of the local device can be received only by the interfaces with the same rate, but not by the other interfaces.
- When an Eth-Trunk performs load balancing calculation, the interface rate cannot be used as the calculation weight. When interfaces with different rates are added to the same Eth-Trunk, traffic is evenly load balanced on all the links. Therefore, the bandwidth of member interfaces is calculated by the minimum rate of the member interfaces in the Eth-Trunk. For example, when a GE interface and a 10GE interface are added to the same Eth-Trunk, the rate of the GE interface is used in calculation and the bandwidth of the Eth-Trunk is 2G.
- When the **undo mixed-rate link enable** command is executed, ensure that the Eth-Trunk does not contain member interfaces with different rates.

Example

# Set the Eth-Trunk 2 to allow interfaces with different interface types adding.

```
<HUAWEI> system-view
[HUAWEI] interface Eth-Trunk 2
[HUAWEI-Eth-Trunk2] mixed-rate link enable
```

5.2.56 mode

Function

The **mode** command configures a working mode of an Eth-Trunk.

The **undo mode** command restores the default working mode of an Eth-Trunk.

By default, an Eth-Trunk works in manual load balancing mode.

Format

mode { **lacp** | **manual load-balance** }

undo mode

Parameters

Parameter	Description	Value
lacp	Indicates the LACP mode.	-
manual load-balance	Indicates the manual load balancing mode.	-

Views

Eth-Trunk interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenarios

An Eth-Trunk can use the following working modes:

- LACP mode

  When the devices that are directly connected through an Eth-Trunk support LACP, you can run the **mode lacp** command to configure the Eth-Trunk to work in LACP mode. This mode can implement both load balancing and redundancy.

  In LACP mode, you must manually create an Eth-Trunk and add member interfaces to the Eth-Trunk. The difference between the LACP mode and manual load balancing mode is that active member interfaces are selected by sending LACP data units (LACPDUs). That is, when a group of interfaces are added to an Eth-Trunk, devices at both ends determine active and inactive interfaces by sending LACPDUs to each other.

- Manual load balancing mode

  When one of the devices at the two ends of an Eth-Trunk does not support LACP, run the **mode manual load-balance** command to configure the Eth-Trunk to work in manual load balancing mode. In addition, you can add multiple member interfaces to the Eth-Trunk to increase the bandwidth between the two devices and improve reliability.

  The manual load balancing mode is a basic link aggregation mode. In this mode, you must manually create an Eth-Trunk and add interfaces to the Eth-Trunk. LACP is not used.

  In manual load balancing mode, all active interfaces of the Eth-Trunk forward data and load balance traffic.

Precautions

If you run the **mode** command multiple times, only the latest configuration takes effect.

If an Eth-Trunk interface has member interfaces, you can switch the Eth-Trunk interface's working mode between manual mode and LACP mode. However, if the Eth-Trunk interface is added to an E-Trunk, you cannot change its working mode.

Example

# Configure Eth-Trunk 1 to work in LACP mode.

```
<HUAWEI> system-view
[HUAWEI] interface eth-trunk 1
[HUAWEI-Eth-Trunk1] mode lacp
```

5.2.57 mpls field

Function

The **mpls field** command configures a load balancing mode of MPLS packets in a load balancing profile.

The **undo mpls field** command deletes a specified load balancing mode of MPLS packets or restores the default load balancing modes of MPLS packets.

By default, load balancing of MPLS packets is based on the two outer labels (**top-label** and **2nd-label**) of each packet.

NOTE

Only the S5735S-H, S5736-S, S5731-H, S5731S-H, S5732-H, S5731-S, S5731S-S, S6730-S, S6730S-S, S6720-EI, S6720S-EI, S6720S-S, S6730S-H, and S6730-H support this command.

Format

mpls field [**2nd-label** | **3rd-label** | **dip** | **dmac** | **l4-dport** | **l4-sport** | **protocol** | **sip** | **smac** | **sport** | **top-label** | **vlan**] *

undo mpls field [**2nd-label** | **3rd-label** | **dip** | **dmac** | **l4-dport** | **l4-sport** | **protocol** | **sip** | **smac** | **sport** | **top-label** | **vlan**] *

Parameters

Parameter	Description	Value
2nd-label	Performs load balancing based on the second label of MPLS packets.	-
3rd-label	Performs load balancing based on the third label of MPLS packets.	-
dip	Performs load balancing based on destination IP addresses in MPLS packets.	-
dmac	Performs load balancing based on destination MAC addresses in MPLS packets.	-
l4-dport	Performs load balancing based on transport-layer destination port numbers in MPLS packets.	-

Parameter	Description	Value
l4-sport	Performs load balancing based on transport-layer source port numbers in MPLS packets.	-
protocol	Performs load balancing based on protocol types in MPLS packets.	-
sip	Performs load balancing based on source IP addresses in MPLS packets.	-
smac	Performs load balancing based on source MAC addresses in MPLS packets.	-
sport	Performs load balancing based on physical-layer source port numbers.	-
top-label	Performs load balancing based on the top label of MPLS packets.	-
vlan	Performs load balancing based on VLAN IDs.	-

Views

Load balancing profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **undo mpls field** command with no parameter specified restores the default load balancing modes of MPLS packets. The **undo mpls field** command with a parameter specified deletes a specified load balancing mode of MPLS packets.

The **mpls field 3rd-label** command implements flow label-based load balancing on L2VPN networks.

Precautions

- If you run the **mpls field** command multiple times, only the latest configuration takes effect.

- Only the S5731-H, S5731S-H, S5732-H, S6730S-H, and S6730-H support the **3rd-label**, **l4-dport**, **l4-sport**, and **protocol** load balancing mode.
- Only **2nd-label**, **dmac**, **smac**, **sport**, and **top-label** are supported on the S5735S-H, S5736-S, and S6720S-S.
- Load balancing based on MPLS labels takes effect for only labeled packets on the ingress.
- For the S5731-H, S5731S-H, S5732-H, S5731-S, S5731S-S, S6730-S, S6730S-S, S6730S-H, and S6730-H, MPLS packets can be load balanced based on source or destination IP addresses on the P and tunnel egress on an L2VPN network. If original data packets are Layer 2 packets and the **sip** or **dip** parameter is specified, MPLS packets are load balanced based on source or destination MAC addresses. For other models, load balancing based on source or destination IP addresses for MPLS packets does not take effect on the P and tunnel egress on an L2VPN network. You are advised to configure the **2nd-label**, **3rd-label**, or **top-label** load balancing mode.

Example

# In the load balancing profile **a**, set the load balancing mode of MPLS packets to **2nd-label**, that is, load balancing based on the second label of MPLS packets.

```
<HUAWEI> system-view
[HUAWEI] load-balance-profile a
[HUAWEI-load-balance-profile-a] mpls field 2nd-label
```

5.2.58 peer-address source-address

Function

The **peer-address source-address** command configures the local and remote IP addresses of an E-Trunk.

The **undo peer-address** command cancels the configuration.

NOTE

Only the S5720I-SI, S5735-S, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6720S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Format

peer-address *peer-ip-address* **source-address** *source-ip-address*

undo peer-address

Parameters

Parameter	Description	Value
peer-address *peer-ip-address*	Specifies the remote IP address of an E-Trunk.	The value is in dotted decimal notation.

Parameter	Description	Value
source-address *source-ip-address*	Specifies the local IP address of an E-Trunk.	The value is in dotted decimal notation.

Views

E-Trunk view

Default Level

2: Configuration level

Usage Guidelines

The remote IP address of the local device is the local IP address of the remote device. For example, an E-Trunk is created between device A and device B. On device A, the remote IP address is 10.2.2.2 and the local IP address is 10.1.1.1. On device B, the remote IP address is 10.1.1.1 and the local IP address is 10.2.2.2.

When changing the local or remote IP address on a device, you must change the corresponding address on the remote device. Otherwise, LACPDUs are discarded.

Example

# Set the remote IP address of E-Trunk 1 to 10.2.2.2 and the local IP address to 10.1.1.1.

```
<HUAWEI> system-view
[HUAWEI] e-trunk 1
[HUAWEI-e-trunk-1] peer-address 10.2.2.2 source-address 10.1.1.1
```

5.2.59 priority (E-Trunk view)

Function

The **priority** command sets the priority of an E-Trunk.

The **undo priority** command restores the default priority of an E-Trunk.

By default, the priority of an E-Trunk is 100.

NOTE

Only the S5720I-SI, S5735-S, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6720S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Format

priority *priority*

undo priority

Parameters

Parameter	Description	Value
priority *priority*	Specifies the priority of an E-Trunk.	The value is an integer that ranges from 1 to 254. The default value is 100. A smaller value indicates a higher priority.

Views

E-Trunk view

Default Level

2: Configuration level

Usage Guidelines

An E-Trunk determines the master/backup status of the two devices according to the priority and system ID. The device with a higher priority is the master.

If the two devices have the same priority, the device with a smaller system ID is the master.

If the two devices have the same priority and system ID, the E-Trunk considers the configuration incorrect and discards LACPDUs.

Example

# Set the priority of E-Trunk 1 to 10.

```
<HUAWEI> system-view
[HUAWEI] e-trunk 1
[HUAWEI-e-trunk-1] priority 10
```

5.2.60 reset e-trunk packet-statistics

Function

The **reset e-trunk packet-statistics** command clears packet statistics about an E-Trunk.

NOTE

Only the S5720I-SI, S5735-S, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6720S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Format

reset e-trunk packet-statistics [**e-trunk-id** *e-trunk-id*]

Parameters

Parameter	Description	Value
e-trunk-id *e-trunk-id*	Specifies the ID of an E-Trunk.	The value is an integer that ranges from 1 to 16.

Views

User view

Default Level

3: Management level

Usage Guidelines

Before collecting packet statistics about an E-Trunk in a given period, run the **reset e-trunk packet-statistics** command to clear the existing statistics. Then run **display e-trunk** command to view packet statistics.

Example

# Clear packet statistics about E-Trunk 1.

```
<HUAWEI> reset e-trunk packet-statistics e-trunk-id 1
```

5.2.61 reset lacp statistics eth-trunk

Function

The **reset lacp statistics eth-trunk** command clears statistics about LACPDUs on all Eth-Trunks in LACP mode, a specified Eth-Trunk in LACP mode, or a specified member interface.

Format

reset lacp statistics eth-trunk [*trunk-id* [**interface** *interface-type interface-number*]]

Parameters

Parameter	Description	Value
trunk-id	Specifies the ID of an Eth-Trunk.	The value is an integer. The value varies according to device model: ● SS1720GW-E, S1720GWR-E, S2730S-S, S5720I-SI, S5720-LI, and S5720S-LI: 0-119 ● S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735-S-I, S5735S-S, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S: 0-127 ● S5735S-H, S5736-S, S6720S-S: 0-249 On the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, S6730S-S, S6735-S, S6720-EI, and S6720S-EI, you can run the **assign trunk** command to set the value, and run the **display trunk configuration** command to check the configuration.
interface *interface-type interface-number*	Specifies an Eth-Trunk member interface. *interface-type*: specifies the type of the interface. *interface-number*: specifies the number of the interface.	-

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

Before collecting statistics about LACPDUs on a specific interface within a given period of time, you need to run the **reset lacp statistics eth-trunk** command to clear the existing statistics about LACPDUs on the interface.

When using the **reset lacp statistics eth-trunk** command, pay attention to the following points:

- If no parameter is specified, statistics about LACPDUs on all Eth-Trunks in LACP mode are cleared.
- If only *trunk-id* is specified, statistics about LACPDUs on the specified Eth-Trunk in LACP mode are cleared.
- If both *trunk-id* and **interface** *interface-type interface-number* are specified, statistics about LACPDUs on the specified member interface of the specified Eth-Trunk in LACP mode are cleared.

Prerequisites

- The Eth-Trunk has been created and configured to work in LACP mode.
- Member interfaces have been added to the Eth-Trunk.

Precautions

The **reset lacp statistics eth-trunk** command clears statistics about sent and received LACPDUs on all Eth-Trunks in LACP mode, a specified Eth-Trunk in LACP mode, or a specified member interface. The cleared statistics cannot be restored. Exercise caution when you run this command.

Example

# Clear statistics about LACPDUs on all Eth-Trunks in LACP mode.

```
<HUAWEI> reset lacp statistics eth-trunk
```

# Clear the statistics about LACPDUs on the member interface GigabitEthernet0/0/1 of Eth-Trunk 1 in LACP mode.

```
<HUAWEI> reset lacp statistics eth-trunk 1 interface gigabitethernet 0/0/1
```

5.2.62 revert disable

Function

The **revert disable** command disables revertive switching on an E-Trunk.

The **undo revert disable** command enables revertive switching on an E-Trunk.

By default, revertive switching is enabled on an E-Trunk and the revertive switching delay is 120s.

NOTE

Only the S5720I-SI, S5735-S, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6720S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Format

revert disable

undo revert disable

Parameters

None

Views

E-Trunk view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On devices of an E-Trunk, when the faulty master device recovers, to prevent loss of traffic that is switched back, run the **revert disable** command to disable revertive switching on the E-Trunk.

Prerequisites

The E-Trunk has been correctly configured.

Follow-up Procedure

Run the **undo revert disable** command to enable revertive switching on an E-Trunk. When the faulty master device recovers, services are switched back to the original active device after 120s by default. Run the **timer revert delay** *delay-value* command to set the revertive switching delay.

Example

# Disable revertive switching on the E-Trunk.

```
<HUAWEI> system-view
[HUAWEI] e-trunk 1
[HUAWEI-e-trunk-1] revert disable
```

5.2.63 security-key

Function

The **security-key** command sets an encrypted password for an E-Trunk.

The **undo security-key** command restores the default password of an E-Trunk.

By default, no encryption password is configured.

NOTE

Only the S5720I-SI, S5735-S, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6720S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Format

security-key { **simple** *simple-key* | **cipher** *cipher-key* }

undo security-key

Parameters

Parameter	Description	Value
simple *simple-key*	Indicates the password in plain text.	The value is a string of 1 to 255 case-sensitive characters without spaces and question mark (?). When double quotation marks are used around the string, spaces are allowed in the string.

Parameter	Description	Value
cipher *cipher-key*	Indicates the password in cipher text.	The value is a case-sensitive character string without spaces and question mark (?). When double quotation marks are used around the string, spaces are allowed in the string. When the cipher text is used, the password can be entered in plain or cipher text. The length depends on the input mode: ● The password in plain text is a string of 1 to 255 characters, but the cipher-text password of 32 to 392 characters is displayed during query. ● The password in plain text is a string of 24 or 32 to 392 characters. **NOTE** ● It is recommended that the password in plain text be used. If the password in cipher text is used, the password must comply with the encryption algorithm. ● If the cipher-text password of 24 characters is supported before upgrade, the password is compatible during upgrade.

Views

E-Trunk view

Default Level

2: Configuration level

Usage Guidelines

NOTICE

If **simple** is specified, the password is saved in the configuration file in plain text. This brings security risks. Therefore, it is recommended that you specify **cipher** to save the password in cipher text.

You can encrypt the password with the plain text or cipher text.

- When the password is encrypted in plain text, it can be displayed in the configuration file.
- When the password is encrypted in cipher text, it is displayed as unidentifiable characters.

An encrypted password must be configured to enhance the system security. The encrypted passwords configured on the two devices of an E-Trunk must be the same.

Example

# Set the password of E-Trunk 1 to YsHsjx_202206 and encrypt the password in cipher mode.

```
<HUAWEI> system-view
[HUAWEI] e-trunk 1
[HUAWEI-e-trunk-1] security-key cipher YsHsjx_202206
```

5.2.64 sequence enable

Function

The **sequence enable** command enables the E-Trunk sequence number check function.

The **undo sequence enable** command disables the E-Trunk sequence number check function.

By default, the E-Trunk sequence number check function is disabled.

NOTE

Only the S5720I-SI, S5735-S, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6720S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Format

sequence enable

undo sequence enable

Parameters

None

Views

E-Trunk view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If the master device in an E-Trunk fails, an attacker can obtain the E-Trunk packet sent by the master device and attack the backup device, causing service interruptions. To resolve this problem, run the **sequence enable** command to enable the E-Trunk sequence number check function.

Configuration Impact

After the E-Trunk sequence number check function is enabled, the E-Trunk sequence number of packets is checked to protect against attacks and enhance E-Trunk security.

Precautions

The **sequence enable** command must be run on both the master and backup devices in an E-Trunk. Otherwise, the E-Trunk sequence number check function fails, causing dual master devices in the E-Trunk.

Example

# Enable the E-Trunk sequence number check function on E-Trunk 1.

```
<HUAWEI> system-view
[HUAWEI] e-trunk 1
[HUAWEI-e-trunk-1] sequence enable
```

5.2.65 timer hello (E-Trunk view)

Function

The **timer hello** command sets the interval at which an E-Trunk sends hello packets.

The **undo timer hello** command restores the default interval for sending hello packets.

By default, the value of *hello-times* is 10, in 100 ms. That is, the default interval for sending hello packets is 1s.

NOTE

Only the S5720I-SI, S5735-S, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6720S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Format

timer hello *hello-times*

undo timer hello

Parameters

Parameter	Description	Value
hello *hello-times*	Specifies the interval for sending hello packets.	The value is an integer that ranges from 5 to 100. The unit is 100 ms. The default value is 10.

Views

E-Trunk view

Default Level

2: Configuration level

Usage Guidelines

The **timer hello** command sets the interval at which the master and backup devices of an E-Trunk send hello packet. If the backup device receives no hello packet from the master device after certain number of intervals (specified by the **timer hold-on-failure multiplier** command for detecting hello packets), the backup device becomes the master.

Configuring a timeout period longer than 5 minutes is recommended, so that the Eth-Trunk packets can be sent to the peer device within the timeout period when a master/backup switchover is performed.

Example

# Set the interval for sending hello packets to 9.

```
<HUAWEI> system-view
[HUAWEI] e-trunk 1
[HUAWEI-e-trunk-1] timer hello 9
```

5.2.66 timer hold-on-failure multiplier

Function

The **timer hold-on-failure multiplier** command sets the time multiplier for an E-Trunk to detect hello packets.

The **undo timer hold-on-failure multiplier** command restores the default time multiplier.

By default, the time multiplier for detecting hello packets is 20.

NOTE

Only the S5720I-SI, S5735-S, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6720S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Format

timer hold-on-failure multiplier *multiplier*

undo timer hold-on-failure multiplier

Parameters

Parameter	Description	Value
multiplier *multiplier*	Specifies the time multiplier for detecting hello packets.	The value is an integer that ranges from 3 to 300. The default value is 20.

Views

E-Trunk view

Default Level

2: Configuration level

Usage Guidelines

After the time multiplier for detecting hello packets is set, the local device is triggered to send hello packets. The remote device checks the timeout of the local device according to the timeout interval in the received packet. If the remote device is the backup device and does not receive hello packets from the local device within the timeout interval, the remote device becomes the master device.

Timeout interval = Interval for sending hello packets x Time multiplier

It is recommended that you set the time multiplier to 3 or larger.

The timeout interval configured on the local device is used by the remote device to check the timeout of the local device. If the hello packet from the remote device does not contain the timeout interval, the timeout interval of the local device is used.

Example

# Set the time multiplier for detecting hello packets to 3.

```
<HUAWEI> system-view
[HUAWEI] e-trunk 1
[HUAWEI-e-trunk-1] timer hold-on-failure multiplier 3
```

5.2.67 timer revert delay

Function

The **timer revert delay** command sets the revertive switching delay of an E-Trunk.

The **undo timer revert delay** command restores the default revertive switching delay of an E-Trunk.

By default, the revertive switching delay of an E-Trunk is 120 seconds.

NOTE

Only the S5720I-SI, S5735-S, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6720S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Format

timer revert delay *delay-value*

undo timer revert delay

Parameters

Parameter	Description	Value
delay-value	Specifies the revertive switching delay of an E-Trunk.	The value is an integer that ranges from 0 to 3600, in seconds.

Views

E-Trunk view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the member Eth-Trunk on the master device goes Down, the member Eth-Trunk on the remote device becomes Up after LACP negotiation. Then the remote device becomes the master device, and the local device becomes the backup device. When the local device recovers, it becomes the master device again in the subsequent LACP negotiation.

If an E-Trunk works with other services, after the master device recovers from a fault, the status of the member Eth-Trunk on the master device may be restored before other services are restored. If traffic is immediately switched back to the master device, service traffic will be interrupted. To solve this problem, you need to set the revertive switching delay for the E-Trunk.

After you run the **timer revert delay** command to set the revertive switching delay for an E-Trunk, the local Eth-Trunk can become Up only after the delay timer times out. This delays the revertive switching of the service traffic, ensuring nonstop services.

Precautions

The revert delay of an E-Trunk must be greater than the PW recovery time. This ensures that services are not interrupted when traffic is reverted back to the master device.

In E-Trunk B2B scenarios where there are four PE devices and an E-Trunk is configured between each two PEs, to ensure that services can be switched back to the master device when a fault is rectified, configure the master device in one E-Trunk to immediately switch traffic back and the master device in the other E-Trunk to switch traffic back after a delay.

Example

# Set the revertive switching delay of E-Trunk 1 to 100 seconds.

```
<HUAWEI> system-view
[HUAWEI] e-trunk 1
[HUAWEI-e-trunk-1] timer revert delay 100
```

5.2.68 trunkport

Function

The **trunkport** command adds a member interface in the Eth-Trunk interface view.

The **undo trunkport** command deletes a member interface in the Eth-Trunk interface view.

By default, no member interface is added to an Eth-Trunk.

Format

trunkport *interface-type* { *interface-number1* [**to** *interface-number2*] } &<1-16> [**mode** { **active** | **passive** }]

undo trunkport *interface-type* { *interface-number1* [**to** *interface-number2*] } &<1-16>

Parameters

Parameter	Description	Value
interface-type interface-number1 [**to** *interface-number2*]	Specifies the type and number of an interface. ● *interface-type* specifies the interface type. ● *interface-number1* specifies the number of the first interface. ● *interface-number2* specifies the number of the last interface. The value of *interface-number2* must be larger than the value of *interface-number1*. *interface-number1* and *interface-number2* specify the range of interfaces. If **to** *interface-number2* is not specified, only one interface is specified.	-
mode { **active** | **passive** }	Indicates the mode in which an Eth-Trunk member interface sends packets. This parameter is valid for only the Eth-Trunk in LACP mode. By default, the mode an Eth-Trunk member interface sends packets is **active**. ● **active**: indicates that an Eth-Trunk member interface proactively sends negotiation packets. ● **passive**: indicates that an Eth-Trunk member interface sends packets to negotiate with its remote end only after receiving a packet from its remote end.	-

Views

Eth-Trunk interface view

Default Level

2: Configuration level

Usage Guidelines

An Eth-Trunk contains a maximum of 32 member interfaces on the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S, 16 member interfaces on the S5735S-H, S5736-S, and S6720S-S and 8 member interfaces on other models.

NOTE

On the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, S6730S-S, S6735-S, S6720-EI, and S6720S-EI, you can run the **assign trunk** command to set the value, and run the **display trunk configuration** command to check the configuration.

Example

# Add GigabitEthernet0/0/1 to Eth-Trunk 1.

```
<HUAWEI> system-view
[HUAWEI] interface eth-trunk 1
[HUAWEI-Eth-Trunk1] trunkport gigabitethernet 0/0/1
```

5.2.69 unknown-unicast load-balance

Function

The **unknown-unicast load-balance** command configures a load balancing mode for broadcast, unknown-unicast, and multicast (BUM) traffic.

The **undo unknown-unicast load-balance** command restores the default load balancing mode for BUM traffic.

By default, BUM traffic is load balanced based on source and destination MAC addresses of packets.

NOTE

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

Format

unknown-unicast load-balance { **dmac** | **smac** | **smacxordmac** | **enhanced** [**lbid**] }

undo unknown-unicast load-balance

Parameters

Parameter	Description	Value
dmac	Load balances the BUM traffic based on destination MAC addresses of packets.	-
smac	Load balances BUM traffic based on source MAC addresses of packets.	-
smacxordmac	Load balances BUM traffic based on source and destination MAC addresses of packets.	-
enhanced [**lbid**]	Load balances BUM traffic based on the enhanced load balancing profile. **NOTE** Only the S6735-S, S6720-EI and S6720S-EI support the **lbid** parameter.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

If the traffic policy contains a traffic behavior that defines the action of re-marking destination MAC addresses of packets, load balancing of BUM traffic must be based on source MAC addresses of packets.

On a VPLS network or a VXLAN network, when the S6735-S, S6720-EI or S6720S-EI switches form a stack, if the outbound interface of BUM traffic is an inter-device Eth-Trunk interface, you need to configure run the **unknown-unicast load-balance enhanced lbid** to configure the load balancing mode. Otherwise, packet loss may occur or there may be duplicate packets.

Example

# Configure the device to load balance BUM traffic based on source MAC addresses of packets.

```
<HUAWEI> system-view
[HUAWEI] unknown-unicast load-balance smac
```

5.2.70 unicast load-balance enhanced

Function

The **unicast load-balance enhanced** command configures a load balancing mode for known unicast packets based on the inner or outer IP address.

The **undo unicast load-balance enhanced** commands restores the default loading balancing mode for known unicast packets.

By default, load balancing for known unicast packets is based on the outer IP address.

NOTE

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

Format

unicast load-balance enhanced { **inner-ip** | **outer-ip** } *

undo unicast load-balance enhanced

Parameters

Parameter	Description	Value
inner-ip	Indicates that load balancing for known unicast packets is based on the inner IP address.	-
outer-ip	Indicates that load balancing for known unicast packets is based on the outer IP address.	-

Views

Eth-Trunk interface view

Default Level

2: Configuration level

Usage Guidelines

When configuring enhanced Eth-Trunk load balancing, you can run the **unicast load-balance enhanced** command to configure known unicast packets, such as GRE packets, to be load balanced based on the inner IP address, outer IP address, or both.

- In IPv4 over GRE or IPv6 over GRE scenarios, if **inner-ip** is specified, known unicast packets are load balanced based on the inner source IP address, inner destination IP address, or both. Similarly, you can configure known unicast packets to be load balanced based on the outer source IP address, outer destination IP address, or both. Additionally, known unicast packets can be load balanced based on the inner and outer source IP addresses, inner and outer destination IP addresses, or both.

- In Ethernet over GRE scenarios, if **inner-ip** is specified, known unicast packets are load balanced based on the inner source MAC address, inner destination MAC address, or both. If **outer-ip** is specified, known unicast packets are load balanced based on the outer source IP address, outer destination IP address, or both. If both **inner-ip** and **outer-ip** are specified, known unicast packets are load balanced based on the outer source IP address and inner source MAC address, outer destination IP address and inner destination MAC address, or both.
- In PPPoE scenarios, if **inner-ip** is specified, known unicast packets are load balanced based on the inner source IP address, inner destination IP address, or both. If **outer-ip** is specified, known unicast packets are load balanced based on the outer source MAC address, outer destination MAC address, or both. If both **inner-ip** and **outer-ip** are specified, known unicast packets are load balanced based on the inner source IP address and outer source MAC address, inner destination IP address and outer destination MAC address, or both.

Example

# Configure an Eth-Trunk interface to perform load balancing for known unicast packets based on the inner IP address.

```
<HUAWEI> system-view
[HUAWEI] interface eth-trunk 1
[HUAWEI-Eth-Trunk1] unicast load-balance enhanced inner-ip
```

5.3 VLAN Configuration Commands

5.3.1 Command Support

Commands provided in this section and all the parameters in the commands are supported by all switch models (except the S5731-L and S5731S-L), unless otherwise specified. For details, see specific commands.

5.3.2 damping time

Function

The **damping time** command sets the VLAN damping time on a VLANIF interface, that is, the delay before reporting a VLAN Down event to the VLANIF interface.

The **undo damping time** command restores the default damping time.

The default damping time on a VLANIF interface is 0 seconds. That is, the VLANIF interface is notified immediately after the VLAN becomes Down.

Format

damping time *delay-time*

undo damping time

Parameters

Parameter	Description	Value
delay-time	Specifies the delay before reporting the VLAN Down event to a VLANIF interface.	The value ranges from 0 to 20, in seconds. The default value is 0.

Views

VLANIF interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Software upgrade or active/standby switchover on the switch may cause frequent status changes on VLANIF interfaces. To prevent network flapping, run the **damping time** command on VLANIF interfaces to configure the VLAN damping function.

When all interfaces in a VLAN become Down, the switch waits for a period specified by *delay-time* and then reports the VLAN Down event to the VLANIF interface.

Precautions

If any interface in the VLAN becomes Up within the delay time, the VLANIF interface remains Up.

You can use the **display interface vlanif** command to view the VLAN damping time.

If you run the **damping time** command multiple times in the same VLANIF interface view, only the latest configuration takes effect.

Example

# Set the VLAN damping time on VLANIF 10 to 10 seconds.

```
<HUAWEI> system-view
[HUAWEI] vlan 10
[HUAWEI-vlan10] quit
[HUAWEI] interface vlanif 10
[HUAWEI-Vlanif10] damping time 10
```

5.3.3 description (VLAN view)

Function

The **description** command sets the description of a VLAN.

The **undo description** command restores the default description of a VLAN.

By default, the description of a VLAN shows the VLAN ID. For example, the description of VLAN 2 is "VLAN 0002".

Format

description *description*

undo description

Parameters

Parameter	Description	Value
description	Specifies the description of a VLAN.	It is a string of 1 to 80 characters. The characters are case sensitive. It can contain blanks but cannot contain the question mark (?).

Views

VLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **description** command is used to set the description of a VLAN, which is convenient for identifying, memorizing, and maintaining the VLAN.

The **display vlan** *vlan-id* **verbose** command can display the description of a specified VLAN.

Precautions

Set different descriptions for VLANs to distinguish.

If you run the **description** command multiple times in the same VLAN view, only the last configuration takes effect.

Example

# Set the description of VLAN 2 as "huawei".

```
<HUAWEI> system-view
[HUAWEI] vlan 2
[HUAWEI-vlan2] description huawei
```

5.3.4 description (VLANIF interface view)

Function

The **description** command set the description of a VLANIF interface.

The **undo description** command restores the default description of a VLANIF interface.

Format

description *description*

undo description

Parameters

Parameter	Description	Value
description	Specifies the description of a VLANIF interface.	The value is a string of 1 to 242 characters. The character string is case sensitive. It can contain blanks but cannot contain the question mark (?).

Views

VLANIF interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To manage VLANIF interfaces conveniently, use the **description** command to set VLANIF interface descriptions. The description of a VLANIF interface helps you identify the VLANIF interface and know its functions.

You can use the **display interface vlanif** command to view the description of a VLANIF interface.

Precautions

The description of a VLANIF interface should provide useful information.

Set different descriptions for VLANIF interfaces to distinguish VLANIF interfaces.

If you run the **description** command multiple times in the same VLANIF interface view, only the latest configuration takes effect.

Example

# Set the description of VLANIF 2 to huawei.

```
<HUAWEI> system-view
[HUAWEI] vlan 2
[HUAWEI-vlan2] quit
[HUAWEI] interface vlanif 2
[HUAWEI-Vlanif2] description huawei
```

5.3.5 display default-parameter vlan

Function

The **display default-parameter vlan** command displays the default parameters of a VLAN.

Format

display default-parameter vlan *vlan-id*

Parameters

Parameter	Description	Value
vlan-id	Displays the default parameters of a specified VLAN.	The value is an integer ranging from 1 to 4094.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

A great number of VLANs are created on a device, and different features are configured for every VLAN. To know the default parameters of a VLAN, run the **display default-parameter vlan** command to specify the VLAN and view its default parameters.

Prerequisites

The specified VLAN has been created.

Precautions

The default parameters of a VLAN do not change with the VLAN configuration.

Example

# Display the default parameters of VLAN 10.

```
<HUAWEI> display default-parameter vlan 10
  VLAN ID              : 10
  Type                 : Common
  Status               : undo shutdown
  Broadcast            : Forward
  Unknown-Multicast    : Forward
  Unknown-Unicast      : Forward
  Statistics           : Disable
  MAC learning         : Enable
  Property             : Default
  Description          : VLAN 0010
```

Table 5-34 Description of the **display default-parameter vlan** command output

Item	Description
VLAN ID	VLAN ID.
Type	VLAN type. The value can be: Common: indicates an ordinary VLAN.
Status	VLAN status. The value can be: undo shutdown: The VLAN is enabled.
Broadcast	Method to deal with broadcast packets. Forward: forwards broadcast packets.
Unknown-Multicast	Method to deal with unknown multicast packets. Forward: forwards unknown multicast packets.
Unknown-Unicast	Method to deal with unknown unicast packets. Forward: forwards unknown unicast packets.
Statistics	Whether collecting statistics about VLAN packets is enabled. The value can be: Disable: Collecting statistics about VLAN packets is disabled.
MAC learning	Whether MAC address learning is enabled. The value can be: Enable: MAC address learning is enabled.
Property	VLAN attribute. The value can be: Default: indicates an ordinary VLAN.
Description	Description of a VLAN.

5.3.6 display interface vlanif

Function

The **display interface vlanif** command displays the status and configuration of a VLANIF interface.

Format

display interface vlanif [*vlan-id* | **main**]

Parameters

Parameter	Description	Value
vlan-id	Specifies the ID of a VLAN.	The value is an integer and the value range depends on the range of existing VLANIF interfaces. You can enter the question mark (?) to obtain the range of VLAN IDs.
main	Displays status and traffic statistics about a VLANIF interface. A VLANIF interface has no sub-interfaces. Status and traffic statistics about a VLANIF interface are displayed whether you specify the **main** parameter or not.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

To monitor an interface or locate an interface fault, you can use the **display interface vlanif** command to view the interface status, interface configuration, and traffic statistics on the interface.

Prerequisites

The specified VLANIF interface has been created.

Precautions

If *vlan-id* is not specified, the **display interface vlanif** command displays information about all VLANIF interfaces in the system.

Example

# Display the status and configuration of VLANIF 3.

```
<HUAWEI> display interface vlanif 3
Vlanif3 current state : UP
Line protocol current state : UP
Last line protocol up time : 2012-08-03 03:54:16
Description:
Route Port,The Maximum Transmit Unit is 1500
Internet Address is 192.168.1.1/24
IP Sending Frames' Format is PKTFMT_ETHNT_2, Hardware address is 00e0-fc12-3456
Current system time: 2012-02-10 11:24:14
Last 300 seconds input rate 0 bits/sec, 0 packets/sec
Last 300 seconds output rate 0 bits/sec, 0 packets/sec
Input:  0 packets, 0 bytes
Output:  0 packets, 0 bytes
    Input bandwidth utilization  : --
    Output bandwidth utilization : --
```

Table 5-35 Description of the display interface vlanif command output

Item	Description
current state	Status of a VLANIF interface. The value is UP or Down.
Line protocol current state	Status of the link-layer protocol on a VLANIF interface. The value is UP or Down.
Last line protocol up time	The last time the line protocol is up.
Description	Description of a VLANIF interface. To specify the parameter, run the **description** command.
Route Port	Indicates that the interface is a Layer 3 interface.
The Maximum Transmit Unit	Specifies the MTU of a VLANIF interface. To specify the parameter, run the **mtu** command.
Internet Address	IP address of a VLANIF interface. If the VLANIF interface does not have an IP address, the system displays "Internet protocol processing: disabled." To specify the parameter, run the **ip address** command.
IP Sending Frames' Format	Encapsulation format of IP packets, which can be PKTFMT_ETHNT_2, Ethernet_802.3, or Ethernet_SNAP.
Hardware address	MAC address of the VLANIF interface.

Item	Description
Last 300 seconds input/output rate	Rates of incoming and outgoing packets in the last 300 seconds, expressed in bytes per second and packets per second. **NOTE** On the SS1720GW-E, S1720GWR-E, S5720I-SI, S5720-LI, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5720S-LI, S5735-S, S500, S5735S-S, S5735-S-I, S5735S-H, S5736-S, and S6720S- this field is displayed only when the traffic statistics function is enabled on the VLAN view using the **statistic enable** command. On other models, this field is displayed only when the traffic statistics function is enabled on the VLANIF interface using the **statistic enable** command.
Current system time	Indicates the current system time. If the system is configured with a time zone and is in the summer time, the time is displayed in the format of YYYY/MM/DD HH:MM:SS±HH:MM.
Input/Output	Number of bytes and packets sent and received by the VLANIF interface. **NOTE** On the SS1720GW-E, S1720GWR-E, S5720I-SI, S5720-LI, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5720S-LI, S5735-S, S500, S5735S-S, S5735-S-I, S5735S-H, S5736-S, and S6720S- this field is displayed only when the traffic statistics function is enabled on the VLAN view using the **statistic enable** command. On other models, this field is displayed only when the traffic statistics function is enabled on the VLANIF interface using the **statistic enable** command.
Input/Output bandwidth utilization	Inbound/outbound bandwidth utilization on an interface.

5.3.7 display ip-subnet-vlan vlan

Function

The **display ip-subnet-vlan vlan** command displays information about IP subnets associated with VLANs.

Format

display ip-subnet-vlan vlan { **all** | *vlan-id1* [**to** *vlan-id2*] }

Parameters

Parameter	Description	Value
all	Displays IP subnets associated with all VLANs.	-
vlan-id1 [**to** *vlan-id2*]	Displays IP subnets associated with specified VLANs. ● *vlan-id1* specifies the start VLAN ID. ● **to** *vlan-id2* specifies the end VLAN ID. The value of *vlan-id2* must be greater than or equal to the value of *vlan-id1*. If **to** *vlan-id2* is not specified, only the IP subnet associated with *vlan-id1* is displayed.	● The value of *vlan-id1* is an integer that ranges from 1 to 4094. ● The value of *vlan-id2* is an integer that ranges from 1 to 4094.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

After configuring IP subnet-based VLAN assignment, you can run the **display ip-subnet-vlan vlan** command to verify the configuration.

This command displays the VLAN ID, IP subnet index, IP subnet address, IP subnet mask, and 802.1p priority of the VLAN mapping an IP subnet.

When using the **display ip-subnet-vlan vlan** command, pay attention to the following points:

- If **all** is specified, IP subnets associated with all VLANs are displayed.
- If **vlan** *vlan-id* is specified, the IP subnet associated with the specified VLAN is displayed.
- If *vlan-id1* **to** *vlan-id2* is specified, IP subnets associated with the specified VLANs are displayed.

Precautions

If no VLAN is associated with any IP subnet by using the **ip-subnet-vlan** command, the **display ip-subnet-vlan vlan** command does not display any information.

Example

# Display information about IP subnets associated with all VLANs.

```
<HUAWEI> display ip-subnet-vlan vlan all
-----------------------------------------------------------------
 Vlan    Index   IpAddress           SubnetMask         Priority
 -----------------------------------------------------------------
 2       12      192.168.1.1         255.255.255.0      3
 -----------------------------------------------------------------
 ip-subnet-vlan count: 1                  total count: 1
```

Table 5-36 Description of the **display ip-subnet-vlan vlan** command output

Item	Description
Vlan	ID of an IP subnet-based VLAN. To specify the parameter, run the **ip-subnet-vlan** command.
Index	Index of an IP subnet. To specify the parameter, run the **ip-subnet-vlan** command.
IpAddress	IP subnet address. To specify the parameter, run the **ip-subnet-vlan** command.
SubnetMask	IP subnet mask. To specify the parameter, run the **ip-subnet-vlan** command.
Priority	802.1p priority of the VLAN associated with an IP address or subnet. To specify the parameter, run the **ip-subnet-vlan** command.

5.3.8 display lnp

Function

The **display lnp interface** command displays LNP negotiation information on a Layer 2 Ethernet interface.

Format

display lnp { **interface** *interface-type interface-number* | **summary** }

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Displays LNP negotiation information on a specified Layer 2 Ethernet interface.	-
summary	Displays LNP negotiation information on all Ethernet interfaces of a Layer 2 device.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

If you want to check the link type and traffic statistics of a Layer 2 Ethernet interface after enabling LNP negotiation, run the **display lnp** command.

To monitor the status of or locate the fault on an LNP-enabled Layer 2 Ethernet interface, run the **display lnp** command to obtain the status information and statistics about user packets. This information provides a basis for fault locating.

Example

# Display LNP negotiation information on a specified Layer 2 Ethernet interface.

```
<HUAWEI> display lnp interface gigabitethernet0/0/1
LNP information for GigabitEthernet0/0/1:
  Port link type: trunk
  Negotiation mode: desirable
  Hello timer expiration(s): 19
  Negotiation timer expiration(s): 0
  Trunk timer expiration(s): 289
  FSM state: trunk

  Packets statistics
  4 packets received
    0 packets dropped
      bad version: 0, bad TLV(s): 0, bad port link type: 0,
      bad negotiation state: 0, other: 0
  5 packets output
    0 packets dropped
      other: 0
```

Table 5-37 Description of the display lnp interface command output

Item	Description
LNP information for	Layer 2 Ethernet interface on which LNP negotiation information is displayed

Item	Description
Port link type	Link-type of the Layer 2 Ethernet interface ● Trunk ● Access ● Hybrid ● dot1q-tunnel
Negotiation mode	Negotiation mode on the Layer 2 Ethernet interface, which can be configured using the **port link-type** command ● desirable ● auto ● on ● off
Hello timer expiration(s)	Timeout period for the Hello timer
Negotiation timer expiration(s)	Timeout period for the negotiation timer
Trunk timer expiration(s)	Timeout period for the Trunk timer
FSM state	Status of the LNP state machine
Packets statistics	Statistics about LNP packets
packets received	Number of received LNP packets
packets dropped	Number of dropped LNP packets
bad version	Number of LNP packets dropped due to incorrect versions
bad TLV(s)	Number of LNP packets dropped due to incorrect TLVs
bad port link type	Number of LNP packets dropped due to incorrect negotiation results
bad negotiation state	Number of LNP packets dropped due to incorrect negotiation states
other	Number of LNP packets dropped due to other causes
packets output	Number of sent LNP packets

# Display LNP negotiation information on all Ethernet interfaces of a Layer 2 device.

```
<HUAWEI> display lnp summary
Global LNP : Negotiation enable
-------------------------------------------------------------------------------
C: Configured; N: Negotiated; *: Negotiation disable;
Port        link-type(C)   link-type(N)   InDropped   OutDropped  FSM
-------------------------------------------------------------------------------
```

```
GE0/0/1     access       access             0          0  off
GE0/0/2     desirable     access             0          0  off
GE0/0/3     desirable     access             0          0  off
GE0/0/4     desirable     access             0          0  off
GE0/0/6     desirable     access             0          0  off
GE0/0/7     desirable     access             0          0  off
GE0/0/8     desirable     access             0          0  off
GE0/0/9     desirable     access             0          0  off
GE0/0/10     desirable     access             0          0  off
```

Table 5-38 Description of the display lnp summary command output

Item	Description
Global LNP	Whether LNP is enabled globally, which can be configured using the **lnp disable** command
Port	Layer 2 Ethernet interface on which LNP negotiation information is displayed
link-type(C)	Negotiation mode on the Layer 2 Ethernet interface, which can be configured using the **port link-type** command
link-type(N)	Negotiation result on the Layer 2 Ethernet interface
InDropped	Number of incoming LNP packets that are dropped on the Layer 2 Ethernet interface
OutDropped	Number of outgoing LNP packets that are dropped on the Layer 2 Ethernet interface
FSM	Status of the LNP state machine ● access ● trunk ● on ● off

5.3.9 display mac-vlan

Function

Using the **display mac-vlan** command, you can view the configuration of MAC address-based VLAN assignment.

Format

display mac-vlan { **mac-address** { **all** | *mac-address* [*mac-address-mask* | *mac-address-mask-length*] } | **vlan** *vlan-id* }

Parameters

Parameter	Description	Value
all	Displays VLANs associated with all MAC addresses.	-
mac-address *mac-address*	Displays the VLAN associated with a specified MAC address.	The value is in H-H-H format. H is a hexadecimal number of 1 to 4 digits.
mac-address-mask	Specifies the mask of a MAC address.	The value is in H-H-H format. H is a hexadecimal number of 1 to 4 digits. The default value is FFFF-FFFF-FFFF.
mac-address-mask-length	Specifies the mask length of a MAC address.	The value is an integer that ranges from 1 to 48. The default value is 48.
vlan *vlan-id*	Displays the configuration of a specified MAC address-based VLAN.	The value is an integer that ranges from 1 to 4094.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

After configuring MAC address-based VLAN assignment, you can run the **display mac-vlan** command to verify the configuration.

When using the **display mac-vlan** command, pay attention to the following points:

- If **mac-address** *mac-address* is specified, the VLAN associated with the specified MAC address is displayed.
- If **mac-address all** is specified, all VLANs associated with MAC addresses are displayed.
- If **vlan** *vlan-id* is specified, configuration of the specified MAC address-based VLAN is displayed.

Example

# Display the configuration of all MAC address-based VLANs.

```
<HUAWEI> display mac-vlan mac-address all
----------------------------------------------------------------
MAC Address     MASK            VLAN    Priority
----------------------------------------------------------------
00e0-fc12-0006  ffff-ffff-ffff  200     0

Total MAC VLAN address count: 1
```

Table 5-39 Description of the display mac-vlan command output

Item	Description
MAC Address	MAC address associated with a VLAN. To specify the parameter, run the **mac-vlan mac-address** command.
MASK	Mask of a MAC address. To specify the parameter, run the **mac-vlan mac-address** command.
VLAN	ID of the VLAN associated with a MAC address. To specify the parameter, run the **mac-vlan mac-address** command.
Priority	802.1p priority of the VLAN associated with the MAC address. To specify the parameter, run the **mac-vlan mac-address** command.

5.3.10 display policy-vlan

Function

Using the **display policy-vlan** command, you can view the configuration of policy-based VLAN assignment.

Format

display policy-vlan { **all** | **vlan** *vlan-id* }

Parameters

Parameter	Description	Value
all	Displays the configuration of all policy-based VLANs.	-

Parameter	Description	Value
vlan *vlan-id*	Displays the configuration of a specified policy-based VLAN.	The value is an integer that ranges from 1 to 4094.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

After associating MAC address and IP address binding policies to VLANs, you can use the **display policy-vlan** command to verify the configuration. The command displays the source MAC address, source IP address, interface where a policy-based VLAN is configured, VLAN ID, and VLAN priority.

When using the **display policy-vlan** command, pay attention to the following points:

- If **all** is specified, configuration of all policy-based VLANs is displayed.
- If **vlan** *vlan-id* is specified, configuration of the specified policy-based VLAN is displayed.

Precautions

If no policy-based VLAN is configured by using the **policy-vlan** command, the **display policy-vlan** does not display any information.

Example

# Display configuration of policy-based VLAN assignment.

```
<HUAWEI> display policy-vlan all
 ----------------------------------------------------------------------
 MacAddress     IPAddress       Port                    Vlan   Priority
 ----------------------------------------------------------------------
 00e0-fc03-0003  10.2.2.2       GigabitEthernet0/0/1  6       4
 00e0-fc02-0002  10.1.1.1       NA                    8       6
 ----------------------------------------------------------------------
Total Policy-VLAN count: 2
```

Table 5-40 Description of the display policy-vlan command output

Item	Description
MacAddress	Source MAC address bound to a policy-based VLAN. To specify the parameter, run the **policy-vlan** command.
IPAddress	Source IP address bound to a policy-based VLAN. To specify the parameter, run the **policy-vlan** command.
Port	Interface where the MAC address and IP address are bound. To specify the parameter, run the **policy-vlan** command.
Vlan	ID of a policy-based VLAN. To specify the parameter, run the **policy-vlan** command.
Priority	802.1p priority of a policy-based VLAN. To specify the parameter, run the **policy-vlan** command.

5.3.11 display port vlan

Function

The **display port vlan** command displays information about interfaces of the VLAN.

Format

display port vlan [*interface-type interface-number* | **active**] *

Parameters

Parameter	Description	Value
interface-type interface-number	Specifies the type and number of an interface in the VLAN. If this parameter is not specified, information about all interfaces in the VLAN is displayed.	-

Parameter	Description	Value
active	Indicates the interface information of dynamic entries in the VLAN. The dynamic mappings between VLANs and ports are identified by services such as voice VLAN service or protocols such as GARP VLAN registration protocol (GVRP).	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

You can run the **display port vlan** command to view information about interfaces of the VLAN and check whether the VLAN is assigned by the command, protocols, or services. If a fault occurs on an interface, you can locate the fault based on the information about the interface and VLAN.

Prerequisite

A VLAN has been created and the Layer 2 interface has joined the VLAN.

Precautions

If a large number of mappings between interfaces and VLANs exist on the device, you are advised to specify the interface or **active** to filter the command output. Otherwise, the following problems may occur due to excessive output information:

- The displayed information is repeatedly refreshed, causing required information to fail to be obtained.
- The system does not respond because of long-time information traverse and search.

Example

# Display information about interfaces that belong to each VLAN on the device.

```
<HUAWEI> display port vlan
Port                    Link Type    PVID  Trunk VLAN List
-------------------------------------------------------------------------------
GigabitEthernet0/0/1        hybrid       1     -
GigabitEthernet0/0/2        hybrid       1     -
```

Display information about all dynamic entries.

```
<HUAWEI> display port vlan active
T=TAG U=UNTAG
-------------------------------------------------------------------------------
Port            Link Type    PVID    VLAN List
-------------------------------------------------------------------------------
GE0/0/3          hybrid       2       T: 10
GE0/0/4          trunk        10      T: 100
```

NOTE

When the stack is set up through service interfaces and service interfaces are configured as physical member interfaces, the physical member interfaces are not displayed in **display port vlan** and **display port vlan active** command outputs.

Table 5-41 Description of the display port vlan command output

Item	Description
Port	Indicates the type and number of the interface.
Link Type	Types of the interface link: ● access ● trunk ● hybrid ● dot1q-tunnel ● desirable ● auto To specify the parameter, run the **port link-type** command. **NOTE** For the Eth-Trunk member interface, the value is displayed as -.
PVID	Indicates the default VLAN ID of the interface. By default, VLAN 1 is the default VLAN of all interfaces. For interfaces of the access and dot1q types and those interfaces negotiated as the access type, you can run the **port default vlan** command to configure the default VLAN. For interfaces of the hybrid type, you can run the **port hybrid pvid vlan** command to configure the default VLAN. For interfaces of the trunk type and those interfaces negotiated as the trunk type, you can run the **port trunk pvid vlan** command to configure the default VLAN. **NOTE** For the Eth-Trunk member interface, the value is displayed as 0.
Trunk VLAN List	Indicates the VLAN IDs of packets that are statically configured to pass through an interface.

Item	Description
VLAN List	● Indicates the VLAN IDs that are dynamically added by an interface. ● Indicates the VLAN IDs of packets that are statically configured to pass through an interface.

5.3.12 display protocol-vlan interface

Function

The **display protocol-vlan interface** command displays the protocol-based VLAN configuration on a specified interface or all interfaces.

Format

display protocol-vlan interface { **all** | *interface-type interface-number* }

Parameters

Parameter	Description	Value
all	Displays the protocol-based VLANs configured on all interfaces.	-
interface-type interface-number	Displays the protocol-based VLAN configured on a specified interface. ● *interface-type* specifies the type of an interface. ● *interface-number* specifies the number of an interface.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

After associating an interface with a protocol-based VLAN, you can use the **display protocol-vlan interface** command to verify the configuration.

Precautions

If no protocol-based VLAN is configured by using the **protocol-vlan vlan** command, the **display protocol-vlan interface** command displays no information.

Example

# Display the protocol-based VLAN associated with GE0/0/1.

```
<HUAWEI> display protocol-vlan interface gigabitethernet 0/0/1
-------------------------------------------------------------------------------
 Interface              VLAN    Index       Protocol Type          Priority
-------------------------------------------------------------------------------
 GigabitEthernet0/0/1     2       2          ipv4                  4
```

Table 5-42 Description of the display protocol-vlan interface command output

Item	Description
Interface	Interface associated with a protocol-based VLAN. To specify the parameter, run the **protocol-vlan vlan** command.
VLAN	ID of a protocol-based VLAN. To specify the parameter, run the **protocol-vlan vlan** command.
Index	Index of a protocol. To specify the parameter, run the **protocol-vlan vlan** command.
Protocol Type	Type of a protocol. To specify the parameter, run the **protocol-vlan** command.
Priority	802.1p priority of the VLAN associated with a protocol. To specify the parameter, run the **protocol-vlan** command.

5.3.13 display protocol-vlan vlan

Function

The **display protocol-vlan vlan** command displays the types and indexes of the protocols associated with VLANs.

Format

display protocol-vlan vlan { **all** | *vlan-id1* [**to** *vlan-id2*] }

Parameters

Parameter	Description	Value
all	Displays the protocols associated with all VLANs.	-
vlan-id1 [**to** *vlan-id2*]	Displays the protocols associated with specified VLANs. ● *vlan-id1* specifies the start VLAN ID. ● *vlan-id2* specifies the end VLAN ID.	The value of *vlan-id1* is an integer that ranges from 1 to 4094. *vlan-id2* is an integer that ranges from 1 to 4094. The value of *vlan-id2* must be greater than or equal to the value of *vlan-id1*.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After configuring protocol-based VLANs, you can use the **display protocol-vlan vlan** command to verify the configuration.

Example

# Display types and indexes of protocols associated with VLANs.

```
<HUAWEI> display protocol-vlan vlan all
-------------------------------------------------------------------------------
 VLAN          Protocol Index    Protocol Type
-------------------------------------------------------------------------------
 2             2                 ipv4
```

Table 5-43 Description of the display protocol-vlan vlan command output

Item	Description
VLAN	ID of a protocol-based VLAN. To specify the parameter, run the **protocol-vlan** command.
Protocol Index	Index of a protocol. To specify the parameter, run the **protocol-vlan** command.

Item	Description
Protocol Type	Type of a protocol. To specify the parameter, run the **protocol-vlan** command.

5.3.14 display vlan

Function

The **display vlan** command displays information about VLANs.

Format

display vlan [*vlan-id* [**verbose** \| **statistics** [**slot** *slot-id*] \| **port-info**]]

display vlan [*vlan-id1* [**to** *vlan-id2*]]

display vlan summary [**slot** *slot-id*]

display vlan vlan-name *vlan-name* [**statistics** \| **verbose**]

Parameters

Parameter	Description	Value
vlan-id	Specifies the ID of a VLAN.	The value is an integer that ranges from 1 to 4094.
vlan-id1 [**to** *vlan-id2*]	Specifies a range of VLAN IDs. ● *vlan-id1* specifies the first VLAN ID. ● **to** *vlan-id2* specifies the last VLAN ID. The value of *vlan-id2* must be greater than or equal to the value of *vlan-id1*. If **to** *vlan-id2* is not specified, only information about the VLAN specified by *vlan-id1* is displayed.	● The value of *vlan-id1* is an integer that ranges from 1 to 4094. ● The value of *vlan-id2* is an integer that ranges from 1 to 4094.

Parameter	Description	Value
statistics	Displays traffic statistics on interfaces in a specified VLAN. If traffic statistics is enabled in the VLAN view, the **display vlan** *vlan-id* **statistics** command can be used to view VLAN traffic statistics.	-
slot *slot-id*	Displays VLAN traffic statistics or summary in a specified slot.	The value is an integer and must be the slot ID of a running card.
summary	Displays summary of all VLANs.	-
verbose	Displays detailed information about a specified VLAN. If **verbose** is not specified, only brief information about the VLAN is displayed.	-
vlan-name *vlan-name*	Specifies a VLAN name.	The name is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
port-info	Displays information about all interfaces in a specified VLAN.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

The **display vlan** command displays VLAN configuration or packet statistics on interfaces in a VLAN.

The **display vlan** *vlan-id* command displays the ports that actually take effect, and the **display vlan** *vlan-id* **verbose** command displays the configured ports.

Prerequisites

Before using the **display vlan** *vlan-id* **statistics** command, run the **statistic enable (vlan view)** command in the corresponding VLAN view to enable the traffic statistics function in the VLAN.

Precautions

If no parameter is specified, brief information about all VLANs is displayed.

Example

# Display brief information about all VLANs.

```
<HUAWEI> display vlan
The total number of VLANs is : 3
--------------------------------------------------------------------------------
U: Up;         D: Down;         TG: Tagged;         UT: Untagged;
MP: Vlan-mapping;               ST: Vlan-stacking;
#: ProtocolTransparent-vlan;    *: Management-vlan;
--------------------------------------------------------------------------------

VID  Type    Ports
--------------------------------------------------------------------------------
1    common  UT:GE0/0/1(D)
9    common  TG:GE0/0/2(D)      Eth-Trunk1(D)
40   common

VID  Status  Property      MAC-LRN Statistics Description
--------------------------------------------------------------------------------
1    enable  default       enable  disable    VLAN 0001
9    enable  default       enable  disable    VLAN 0009
40   enable  default       enable  disable    VLAN 0040
```

# Display detailed information about VLAN 100.

```
<HUAWEI> display vlan 100 verbose
* : Management-VLAN
---------------------
  VLAN ID                     : 100
  VLAN Name                   :
  VLAN Type                   : Common
  Description                 : VLAN 0100
  Status                      : Enable
  Broadcast                   : Enable
  MAC Learning                : Enable
  Smart MAC Learning          : Disable
  Current MAC Learning Result : Enable
  Statistics                  : Disable
  Property                    : Default
  VLAN State                  : Down
  ----------------
  Tagged        Port: GigabitEthernet0/0/1
  ----------------
  Active  Tag   Port: GigabitEthernet0/0/1
-------------------
Interface            Physical
GigabitEthernet0/0/1                  DOWN
```

# Display interface traffic statistics in VLAN 10 on S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S. If no interface is added to VLAN 10, **Slot** information is not displayed.

```
<HUAWEI> display vlan 10 statistics
 Total
 VLAN : 10
 -------------------------------------------------------------------------------
 Item                                   Packets                    Bytes
                                         pps                      bps
 -------------------------------------------------------------------------------
 Inbound                                      0                      0
                                         0                      0
 Outbound                                      0                      0
                                         0                      0
 -------------------------------------------------------------------------------
 Slot : 0                                                                           VLAN :
10
-------------------------------------------------------------------------------
Item                                   Packets
Bytes                                                                        pps
bps
-------------------------------------------------------------------------------
Inbound                                      0
0                                                                          0
0                                         Outbound                              0
0                                                                          0
0                                         -------------------------------------------------------------------------------
```

# Display interface traffic statistics in VLAN 10 on other devices except the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S. If no interface is added to VLAN 10, **Slot** information is not displayed.

```
<HUAWEI> display vlan 10 statistics
 Total
 VLAN : 10
 -------------------------------------------------------------------------------
 Item                                   Packets                    Bytes
                                         pps                      bps
 -------------------------------------------------------------------------------
 Inbound                                      0                      -
                                         0                      -
 Outbound                                      0                      -
                                         0                      -
 Inbound unknown-unicast                          -                      -
                                         -                      -
 Inbound multicast                               0                      -
                                         0                      -
 Inbound broadcast                                0                      -
                                         0                      -
 Inbound drop                                  -                      -
                                         -                      -
 -------------------------------------------------------------------------------
 Inbound drop-percentage                         -                      -
 -------------------------------------------------------------------------------
 Slot : 0                                                                           VLAN :
10
-------------------------------------------------------------------------------
Item                                   Packets
Bytes                                                                        pps
bps
-------------------------------------------------------------------------------
Inbound                                      0
-                                                                          0
-                                         Outbound                              0
-                                                                          0
-                                         Inbound unknown-unicast                         -
-                                                                          -
-                                         Inbound multicast                          0
-                                                       0
-                           Inbound broadcast                  0
-                                                       0
-                           Inbound drop                           -
-                                                       -
-
--------------------------------------------------------------------------------
Inbound drop-percentage              -              -
--------------------------------------------------------------------------------
```

# Display summary of all VLANs.

```
<HUAWEI> display vlan summary
Static VLAN:
Total 3 static VLAN.
  1 9 to 10

Dynamic VLAN:
Total 0 dynamic VLAN.

Reserved VLAN:
Total 5 reserved VLAN.
  Rrpp reserved:
  3000 to 3001
  Sep reserved:
  3100

Stack-VLAN:   212 to 213
```

# Display interface information of a specific VLAN.

```
<HUAWEI> display vlan 1 port-info
VLAN  Interface              PHY      Auto-Neg   Duplex  Bandwidth
1     GigabitEthernet0/0/1   UP       enable     full    1000M
1     GigabitEthernet0/0/2   DOWN     enable     full    1000M
1     GigabitEthernet0/0/3   DOWN     disable    full    1000M
```

Table 5-44 Description of the display vlan command output

Item	Description
VID, VLAN, or VLAN ID	ID of a VLAN.
Type or VLAN Type	Type of a VLAN: ● mux: principal VLAN used in the MUX VLAN function ● mux-sub: subordinate VLAN used in the MUX VLAN function ● super: super-VLAN used for VLAN aggregation ● sub: sub-VLAN used for VLAN aggregation ● Common: common VLAN ● *Common: management VLAN ● dynamic: dynamic VLAN
Ports	Interfaces in a VLAN.
VLAN Name	Name of a VLAN.
Description	Description of a VLAN.

Item	Description
Status	Status of a VLAN. The value is always **Enable**.
Broadcast	Whether the broadcast function is enabled in a VLAN: ● Disable: The broadcast function is disabled. ● Enable: The broadcast function is enabled.
MAC Learning/MAC-LRN	Whether MAC address learning is enabled: ● Disable: MAC address learning is disabled. ● Enable: MAC addresses learning is enabled.
Smart MAC Learning	Whether smart MAC address learning is enabled: ● Disable: Smart MAC address learning is disabled. ● Enable: Smart MAC addresses learning is enabled.
Current MAC Learning Result	MAC address learning result.
Statistics	Whether the traffic statistics function is enabled in a VLAN: ● Disable: Traffic statistics function is disabled. ● Enable: Traffic statistics function is enabled.
Property	Property of a VLAN: ● Default: default VLAN ● MulticastVlan: multicast VLAN ● UserVlan: user VLAN
VLAN State	Status of the VLAN: ● Up ● Down The status of a VLAN is determined by the status of member interfaces in the VLAN. A VLAN is Up only when at least one member interface in the VLAN is Up.
Tagged/Untagged Port	Interfaces that are manually added to a VLAN in tagged or untagged mode.
Active Tag/Active Untag Port	Active interfaces that join a VLAN in tagged or untagged mode.
Inbound	Total incoming traffic volume.
Outbound	Total outgoing traffic volume.
Inbound unknown-unicast	Number of incoming unknown unicast packets.

Item	Description
Inbound multicast	Number of incoming multicast packets.
Inbound broadcast	Number of incoming broadcast packets.
Inbound drop	Number of discarded incoming packets. **NOTE** For the S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735S-S, S5735-S-I, if the **statistic enable** command is configured in a VLAN and the **port discard tagged-packet** command is configured on an interface and the interface is configured to allow packets from the specified VLAN to pass through, this item does not take effect.
Inbound drop-percentage	Percentage of discarded incoming packets. **NOTE** For the S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735S-S, S5735-S-I, if the **statistic enable** command is configured in a VLAN and the **port discard tagged-packet** command is configured on an interface and the interface is configured to allow packets from the specified VLAN to pass through, this item does not take effect.
Static VLAN	VLANs that are created manually.
Dynamic VLAN	VLANs that are learned dynamically.
Reserved VLAN	VLANs that are reserved for certain functions.
Rrpp reserved	VLANs used by the Rapid Ring Protection Protocol (RRPP). This field is displayed only when RRPP is configured on the switch.
Sep reserved	VLANs used by the Smart Ethernet Protocol (SEP). This field is displayed only when SEP is configured on the switch.
Stack-VLAN	VLANs configured in a stack. This field is displayed only when the switch is in a stack.
Interface	The name and number of an interface. All interfaces are displayed in the alphabetical order.
PHY	The physical status of the interface, including: ● UP: The physical layer of this interface works properly. ● DOWN: The physical layer of this interface becomes faulty.

Item	Description
Auto-Neg	Indicates whether auto-negotiation is enabled on the interface. The value can be: ● enable: indicates that the interface is enabled with auto-negotiation. ● disable: indicates that the interface is disabled with auto-negotiation.
Duplex	Duplex mode of the interface: ● half: The interface works in half-duplex mode. ● full: The interface works in full-duplex mode. ● auto: The interface works in auto-negotiation mode.
Bandwidth	Indicates the bandwidth of the interface.

5.3.15 interface vlanif

Function

The **interface vlanif** command creates a VLANIF interface and displays the VLANIF interface view.

The **undo interface vlanif** command deletes a VLANIF interface.

By default, VLANIF interfaces are not created.

Format

interface vlanif *vlan-id*

undo interface vlanif *vlan-id*

Parameters

Parameter	Description	Value
vlan-id	Specifies the ID of the VLAN that a VLANIF interface belongs to.	● S2710-SI/S5710-C-LI: 1 ● S2700-SI/S2700-EI/S5710-X-LI: 8 ● S2720-EI (V200R006C10, V200R009C00, V200R010C00): 8 ● S2720-EI (V200R011C10, V200R012C00, V200R013C00, V200R019C00, V200R019C10): 1024 ● S2730S-S: 1024 ● S3700-SI/S3700-EI/S3700-HI/S5700-SI/S5700-EI: 256 ● S5700-HI/S5730-SI/S5735S-H/S5736-S/S5730S-EI/S5720-EI/S5731-S/S5731S-S/S5710-HI/S5720I-SI/S5720-SI/S5720S-SI/S5720-LI/S5720S-LI/S6730-S/S6730S-S/S6720-LI/S6720S-LI/S6720-SI/S6720S-S/S6720S-SI/S6735-S/S6720-EI/S6720S-EI: 1024 ● S5720-HI/S5730-HI/S5731-H/S5731S-H/S5732-H/S6720-HI/S6730-H/S6730S-H: 1024 in versions earlier than V200R019C10 and 4096 in V200R019C10 and later versions ● S5735-L/S5735S-L/S5735S-L-M/S5735-S/S5735-S-I/S5735S-S: 1019 in versions earlier than V200R019C10 and

Parameter	Description	Value
		1024 in V200R019C10 and later versions ● S5735-L-I/S5735-L1/S5735S-L1/S500/S300: 1024 **NOTE** On the S500, S5735-S, S300, S5735-L, S5735S-L, S5735-S-I, S5735S-L-M, S5735S-S, S5735-L1, S5735-L-I and S5735S-L1 running V200R020C10 or a later version, if the resource allocation mode is set to **enhanced-mac**, a maximum of eight VLANIF interfaces can be configured. ● S2750-EI/S5700-LI/S5700S-LI: 1 in versions earlier than V200R005 and 8 in V200R005 and later versions ● S5710-EI/S6700-EI: 256 in versions earlier than V200R005 and 1024 in V200R005

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When a device needs to communicate with devices at the network layer, you can create a logical interface based on a VLAN on the device, namely, a VLANIF interface. A VLANIF interface is a network layer interface and can be configured with an IP address. The device then users the VLANIF interface to communicate with devices at the network layer.

Follow-up Procedure

Run the **ip address** to assign an IP address to the VLANIF interface.

Precautions

- A VLANIF interface goes Up only after the following conditions are met:
  - The corresponding VLAN must have been created.
  - A physical interface or Eth-Trunk in Up state has been added to the corresponding VLAN.
- After a VLANIF interface is configured, the corresponding VLAN cannot be configured as a VLAN for Dot1q termination sub-interfaces or an outer VLAN for QinQ termination sub-interfaces.
- If the specified VLANIF interface exists, the **interface vlanif** command displays the VLANIF interface view directly.
- When a VLANIF interface is used as a management VLANIF interface where you can telnet to the device, the user VLAN ID cannot be the same as the management VLAN ID; otherwise, you will fail to telnet to the device.
- For the S500, S5735-S, S300, S5735-L, S5735S-L, S5735-S-I, S5735S-L-M, S5735S-S, S5735-L-I, S5735-L1,and S5735S-L1, if the resource allocation mode is set to **enhanced-mac** using the **assign resource-mode enhanced-mac global** command, a maximum of eight VLANIF interfaces can be created; if the device has already more than eight VLANIF interfaces configured, after the **enhanced-mac** resource allocation mode is configured, only the eight VLANIF interfaces with the smallest VLAN IDs are reserved.

Example

# Create VLANIF 2 and enter the VLANIF interface view.

```
<HUAWEI> system-view
[HUAWEI] vlan 2
[HUAWEI-vlan2] quit
[HUAWEI] interface vlanif 2
[HUAWEI-Vlanif2]
```

5.3.16 ip-subnet-vlan

Function

Using the **ip-subnet-vlan** command, you can associate an IP subnet with a VLAN.

Using the **undo ip-subnet-vlan** command, you can disassociate an IP subnet from a VLAN.

By default, a VLAN is not associated with any IP subnet.

Format

ip-subnet-vlan [*ip-subnet-index*] **ip** *ip-address* { *mask* | *mask-length* } [**priority** *priority*]

undo ip-subnet-vlan { *ip-subnet-index* [**to** *ip-subnet-end*] | **all** }

Parameters

Parameter	Description	Value
ip-subnet-index	Specifies the index of an IP subnet. It can be set manually or automatically generated by the system according to the order in which IP subnets were associated with a VLAN.	The value is an integer that ranges from 1 to 12.
ip *ip-address* { *mask* | *mask-length* }	Specifies the source IP address or network segment associated with a VLAN. ● *ip-address* specifies the source IP address or IP subnet. ● *mask* specifies the subnet mask. ● *mask-length* specifies the mask length.	● *ip-address* is in dotted decimal notation. ● *mask* is in dotted decimal notation. ● *mask-length* is an integer that ranges from 0 to 32.
priority *priority*	Specifies the 802.1p priority of the VLAN associated with an IP address or subnet.	The value is an integer that ranges from 0 to 7. A larger value indicates a higher priority. The default value is 0.
to *ip-subnet-end*	Specifies the end subnet index.	The value is an integer that ranges from 1 to 12 and must be greater than or equal to *ip-subnet-index*.
all	Disassociates all the IP subnets from a VLAN.	-

Views

VLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **ip-subnet-vlan** command associates IP subnets with VLANs so that packets from different subnets are transmitted in different VLANs. On a network, if only one service is deployed on each subnet, you can associate IP subnets with VLANs to simplify VLAN configuration. In addition, you can add, modify, and move users on subnets without changing the VLAN configuration.

Follow-up Procedure

Add an interface to the VLAN and enable IP subnet-based VLAN assignment on the interface.

Precautions

On the S1720GW-E, S1720GWR-E, S5720I-SI, S5720-LI, and S5720S-LI, when the **ip error-packet-check disable** command is used to disable IP packet check, IP subnet-based VLAN assignment and policy-based VLAN assignment do not take effect.

If you run the **ip-subnet-vlan** command multiple times in the same VLAN view, all the specified IP subnets are associated with the VLAN.

NOTE

- The control VLAN of an RRPP ring cannot be associated with IP subnets.
- The IP subnet or the IP address associated with a VLAN cannot be a multicast network segment or multicast address.

Example

# Associate VLAN 3 with network segment 10.10.10.0/24 so that the packets originated from this segment can be transmitted in VLAN 3.

```
<HUAWEI> system-view
[HUAWEI] vlan 3
[HUAWEI-vlan3] ip-subnet-vlan ip 10.10.10.0 255.255.255.0
```

5.3.17 ip-subnet-vlan enable

Function

The **ip-subnet-vlan enable** command enables IP subnet-based VLAN assignment on an interface.

The **undo ip-subnet-vlan enable** command disables IP subnet-based VLAN assignment on an interface.

By default, IP subnet-based VLAN assignment is disabled on an interface.

Format

ip-subnet-vlan enable

undo ip-subnet-vlan enable

Parameters

None

Views

Ethernet interface view, GE interface view, XGE interface view, 40GE interface view, 100GE interface view, MultiGE interface view, port group view, Eth-Trunk interface view, 25GE interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

IP subnets can be associated with VLANs so that packets from different subnets are transmitted in different VLANs. On a network, if only one service is deployed on each subnet, you can associate IP subnets with VLANs to simplify VLAN configuration. In addition, you can add, modify, and move users on subnets without changing the VLAN configuration.

If IP subnet-based VLAN assignment is enabled on an interface:

- When receiving an untagged packet, the interface searches for the VLAN entry matching the source IP address of the packet. If a matching entry is found, the interface forwards the packet based on the matching VLAN ID and priority. If no matching entry is found, the interface uses other matching rules to forward the packet.
- When receiving a tagged packet, the interface forwards the packet based on the port-based VLAN configuration.

Precautions

On the S1720GW-E, S1720GWR-E, S5720I-SI, S5720-LI, and S5720S-LI, when the **ip error-packet-check disable** command is used to disable IP packet check, IP subnet-based VLAN assignment and policy-based VLAN assignment do not take effect.

On access and trunk interfaces, IP subnet-based VLAN assignment can be used only when the IP subnet-based VLAN is the same as the PVID. It is recommended that IP subnet-based VLAN assignment be configured on hybrid interfaces.

When multiple VLAN assignment methods are configured on the device, the device assigns VLANs based on priorities of these methods.

Example

# Enable IP subnet-based VLAN assignment.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] port link-type hybrid
[HUAWEI-GigabitEthernet0/0/1] ip-subnet-vlan enable
```

5.3.18 lnp disable

Function

The **lnp disable** command disables LNP negotiation on a device.

The **undo lnp disable** command enables LNP negotiation on a device.

By default, LNP negotiation is enabled on all interfaces of a device.

Format

lnp disable

undo lnp disable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

By default, LNP negotiation is enabled for all interfaces on a Layer 2 device. If an LNP-capable Layer 2 device is connected to an LNP-incapable Layer 2 device, the LNP-capable device keeps sending LNP packets, wasting bandwidth resources. To disable LNP negotiation on all interfaces of a Layer 2 device, run the **lnp disable** or **undo lnp enable** command.

To disable LNP negotiation on a Layer 2 Ethernet interface, run the **port negotiation disable** command in the interface view.

Precautions

- When the switch is upgraded from an earlier version of V200R005C00 to V200R005C00 or later, the link type auto-negotiation function is automatically disabled globally.
- By default, LNP negotiation is enabled for all interfaces on a Layer 2 device. If you run the **lnp disable** command in the system view to disable LNP negotiation on all interfaces of a Layer 2 device. LNP negotiation cannot be enabled on a Layer 2 Ethernet interface by running the **undo port negotiation disable** command in the interface view.
- The **lnp disable** command has no impact on services before the device restarts. However, after the device restarts, Layer 2 forwarding can be performed only for the manually configured VLANs. The **port default vlan 1**

command is configured by default, so only packets of VLAN 1 can be forwarded at Layer 2.

- For LNP negotiation to take effect, LNP negotiation must be enabled on both the device and Layer 2 Ethernet interfaces.
- This command is not supported in NETCONF mode.

Example

# Disable LNP negotiation on a device.

```
<HUAWEI> system-view
[HUAWEI] lnp disable
```

5.3.19 mac-learning smart vlan enable

Function

The **mac-learning smart vlan enable** command enables flexible MAC address learning in a specified VLAN.

The **undo mac-learning smart vlan enable** command disables flexible MAC address learning in a specified VLAN.

By default, flexible MAC address learning is disabled in a VLAN.

Format

mac-learning smart vlan { *vlan-id1* [**to** *vlan-id2*] } &<1-10> **enable**

undo mac-learning smart vlan { *vlan-id1* [**to** *vlan-id2*] } &<1-10> **enable**

Parameters

Parameter	Description	Value
vlan-id1	Specifies the start VLAN ID.	The value is an integer ranging from 1 to 4094.
to *vlan-id2*	Specifies the end VLAN ID.	The value is an integer ranging from 1 to 4094. The value of *vlan-id2* must be greater than the value of *vlan-id1*.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Enterprises usually adopt the ring or tree network topology to construct enterprise networks. Both network topologies require that devices at the convergence layer be able to learn a large number of MAC addresses in the case of enormous number of attached users.

As the number of attached users keeps growing, the specification of MAC entries supported by the devices cannot meet the need. As a result, MAC addresses of some users cannot be learned, and the packets of these users are broadcast in the VLAN, wasting network bandwidth and affecting the network performance.

To prevent the preceding problem, you can run the **mac-learning smart vlan enable** command in the system view to enable flexible MAC address learning in a VLAN. When less than three interfaces in the VLAN are Up, the system automatically disables MAC address learning in the VLAN, avoiding unnecessary resource consumption due to MAC address learning.

Prerequisites

The command takes effect only when the following operations are complete.

1. Run the **vlan** command to create a VLAN. If the device supports the dynamic VLAN function, you do not need to run the **vlan** command to create the VLAN.
2. Run the **undo mac-address learning disable** command in the VLAN view to enable MAC address learning.

Precautions

The system will delete the MAC entries after enabling flexible MAC address learning in the specified VLAN. When the number of Up interfaces in the VLAN exceeds 2, the system automatically enables MAC address learning in the VLAN. If a VLAN is configured as a MUX VLAN or is used as the outer VLAN in VLAN stacking or VLAN mapping configuration, flexible MAC address learning does not take effect in the VLAN.

If the **mac-learning smart vlan** command is run more than once, all configurations take effect.

Example

# Configure the system to automatically disable MAC address learning in VLAN 10.

```
<HUAWEI> system-view
[HUAWEI] undo mac-learning smart vlan 10 enable
```

5.3.20 mac-vlan enable

Function

The **mac-vlan enable** command enables MAC address-based VLAN assignment on an interface.

The **undo mac-vlan enable** command disables MAC address-based VLAN assignment on an interface.

By default, MAC address-based VLAN assignment is disabled on an interface.

Format

mac-vlan enable

undo mac-vlan enable

Parameters

None

Views

Ethernet interface view, GE interface view, XGE interface view, 40GE interface view, 100GE interface view, MultiGE interface view, port group view, Eth-Trunk interface view, 25GE interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If user devices move frequently on a network, you can use the **mac-vlan mac-address** command to associate MAC addresses with VLANs. When a user moves, you do not need to assign a VLAN to the user again. This improves security and access flexibility on the network. To enable an interface to forward packets based on associations between MAC addresses and VLANs, you must run the **mac-vlan enable** command to enable MAC address-based assignment on the interface.

If MAC address-based assignment is enabled on an interface:

- When receiving an untagged packet, the interface searches for the VLAN entry matching the source MAC address of the packet. If a matching entry is found, the interface forwards the packet using the VLAN ID and priority in the entry. If no matching entry is found, the interface uses other matching rules to forward the packet.
- When receiving a tagged packet, the interface forwards the packet based on the port-based VLAN configuration.

Precautions

On access and trunk interfaces, MAC address-based VLAN assignment can be used only when the MAC address-based VLAN is the same as the PVID. It is recommended that MAC address-based VLAN assignment be configured on hybrid interfaces.

The MUX VLAN function and MAC address-based VLAN assignment cannot be enabled on the same interface.

MAC address-based VLAN assignment and MAC address authentication cannot be enabled on the same interface.

When multiple VLAN assignment methods are configured on the switch, the switch assigns VLANs based on priorities of these methods.

MAC address-based VLAN assignment on an interface and NAC conflict on an interface; therefore, the **mac-vlan enable** and **mac-authen**, **dot1x enable**, **web-auth-server** or **authentication-profile** commands cannot be used on the same interface.

Example

# Enable MAC address-based VLAN assignment on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] port link-type hybrid
[HUAWEI-GigabitEthernet0/0/1] mac-vlan enable
```

5.3.21 mac-vlan mac-address

Function

The **mac-vlan mac-address** command associates a MAC address with a VLAN.

The **undo mac-vlan mac-address** command cancels the association between MAC addresses and VLANs.

By default, the MAC addresses are not associated with VLANs.

Format

mac-vlan mac-address *mac-address* [*mac-address-mask* | *mac-address-mask-length*] [**priority** *priority*]

undo mac-vlan mac-address { **all** | *mac-address* [*mac-address-mask* | *mac-address-mask-length*] }

Parameters

Parameter	Description	Value
mac-address	Specifies the MAC address to be associated with a VLAN.	The value is in H-H-H format. H is a hexadecimal number of 4 digits, for example, 00e0 and fc01. If you enter less than four digits, 0s are prefixed to the input digits. For example, if you enter e0, the system changes e0 to 00e0. The MAC address cannot be 0000-0000-0000, FFFF-FFFF-FFFF, or a multicast MAC address.
mac-address-mask	Specifies the mask of a MAC address.	The value is in H-H-H format. H is a hexadecimal number of 1 to 4 digits. The default value is FFFF-FFFF-FFFF.

Parameter	Description	Value
mac-address-mask-length	Specifies the length of a MAC address mask.	The value is an integer that ranges from 1 to 48. The default value is 48.
priority *priority*	Specifies the 802.1p priority of the VLAN to be associated with a MAC address.	The value is an integer that ranges from 0 to 7. A larger value indicates a higher priority. The default value is 0.
all	Specifies all the MAC addresses associated with a VLAN.	-

Views

VLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If user devices move frequently on a network, you can use the **mac-vlan mac-address** command to associate MAC addresses with VLANs. The switch then assigns VLANs to packets based on source MAC addresses of packets. Before forwarding a packet, the switch tags the packet with the VLAN associated with the source MAC address. When a user device moves, you do not need to assign a VLAN to the user device again. This improves security and access flexibility on the network.

You can specify the 802.1p priority of the VLAN to be associated with the specific MAC address. In this manner, when the switching device is congested, the switching device preferentially sends frames with high priorities.

Follow-up Procedure

Add an interface to the VLAN and enable MAC address-based VLAN assignment on the interface.

Precautions

- When the **mac-vlan mac-address** command with the same MAC address specified is executed multiple times, MAC-VLAN entries take effect according to the longest match principle. On the S6735-S, S6720-EI and S6720S-EI, MAC-VLAN entries take effect according to the longest match principle only when the subnet mask has 47 bits or less than 47 bits. A MAC-VLAN entry with a 48-bit subnet mask has the lowest priority.
- After a MAC address is associated with a VLAN, it cannot be associated with other VLANs.

- If you run the **mac-vlan mac-address** command multiple times in the same VLAN view, all the specified MAC addresses are associated with the VLAN.
- The total number of MAC-VLAN entries is the number of configured MAC-VLAN entries multiplied by the number of interfaces where MAC-VLAN entries are delivered. On different models, the number of MAC-VLAN entries is different:
  - The S5720I-SI, S5735-S, S5735S-S, S5735-S-I, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support a maximum of 1024 MAC-VLAN entries and a maximum of 64 MAC-VLAN entries with the mask.
  - The SS1720GW-E, S1720GWR-E, S500S5720S-LI, S5735S-H, S5736-S, S6720S-S, S5720-LI, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, and S5735S-L-M support a maximum of 512 MAC-VLAN entries and a maximum of 64 MAC-VLAN entries with the mask.
  - Other models support a maximum of 512 MAC-VLAN entries and a maximum of 32 MAC-VLAN entries with the mask.

Example

# Associate MAC address 22-33-44 with VLAN 100.

```
<HUAWEI> system-view
[HUAWEI] vlan 100
[HUAWEI-vlan100] mac-vlan mac-address 22-33-44
```

5.3.22 management-vlan

Function

Using the **management-vlan** command, you can configure a VLAN as a management VLAN.

Using the **undo management-vlan** command, you can cancel the configuration.

By default, no VLAN is configured as a management VLAN.

Format

management-vlan

undo management-vlan

Parameters

None

Views

VLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To use a network management system to manage multiple devices, create a VLANIF interface on each device and configure a management IP address for the VLANIF interface. You can then log in to a device and manage it using its management IP address. If a user-side interface is added to the VLAN, users connected to the interface can also log in to the device. This brings security risks to the device.

After a VLAN is configured as a management VLAN, no access interface or dot1q-tunnel interface can be added to the VLAN. An access interface or a dot1q-tunnel interface is connected to users. The management VLAN forbids users connected to access and dot1q-tunnel interfaces to log in to the device, improving device performance.

Follow-up Procedure

Create a VLANIF interface corresponding to the VLAN and configure a management IP address on the VLANIF interface.

Precautions

VLAN 1 cannot be configured as a management VLAN.

You can run the **display vlan** command to view the management VLAN configuration. In the command output, the VLAN marked with a * is the management VLAN.

After a VLAN is configured as a management VLAN, only trunk and hybrid interfaces can be added to the VLAN.

VCMP will be disabled if a managedment VLAN is configured.

Example

# Configure VLAN 100 as a management VLAN.

```
<HUAWEI> system-view
[HUAWEI] vlan 100
[HUAWEI-vlan100] management-vlan
```

5.3.23 name (VLAN view)

Function

The **name** command configures a name for a VLAN.

The **undo name** command deletes a configured VLAN name.

By default, a VLAN does not have a name.

Format

name *vlan-name*

undo name

Parameters

Parameter	Description	Value
vlan-name	Specifies the VLAN name.	The name is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Views

VLAN view

Default Level

2: Configuration level

Usage Guidelines

If a device is configured with multiple VLANs for transmitting different services, you can name the VLANs in their corresponding VLAN views to facilitate service management. In this manner, you can check the deployed services of a VLAN by the VLAN name.

After VLANs are named, you can run the **vlan vlan-name** command in the system view to enter the view of a specific VLAN, and then check or modify the configuration of the VLAN.

Example

# Create VLAN 2, which is used to transmit voice services, and name it as voice.

```
<HUAWEI> system-view
[HUAWEI] vlan 2
[HUAWEI-vlan2] name voice
```

5.3.24 ping mac

Function

The **ping mac** command enables the system to monitor connectivity between the local device and the destination device. This detection is called GMAC ping.

Format

ping mac *mac-address* **vlan** *vlan-id* [**interface** *interface-type interface-number* | **-c** *count* | **-s** *packetsize* | **-t** *timeout* | **-p** *priority-value*] *

Parameters

Parameter	Description	Value
mac-address	Specifies the MAC address of the destination node. An MP's MAC address can be a bridge MAC address or the MAC address of the interface where the MP is configured. The MAC address depends on the configured MP address model: ● If the shared MP address model is configured, an MP uses a bridge MAC address as its own MAC address. ● If the independent MP address model is configured, an MP uses the MAC address of the interface where the MP is configured.	The destination node can be a MEP or a MIP. The value is in H-H-H format. An H is a hexadecimal number of 1 to 4 digits. The value cannot be a broadcast or multicast MAC address.
vlan *vlan-id*	Specifies the ID of a VLAN.	The value is an integer that ranges from 1 to 4094.
interface *interface-type interface-number*	Specifies the outbound interface on the local device for sending ping packets. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number. If this parameter is specified and the interface is in the specified VLAN, the device sends ping packets through the interface. If this parameter is not specified, the device searches the MAC address table based on the specified destination MAC address and VLAN ID. ● If the forwarding entry is found, the device sends ping packets according to the entry. ● If the forwarding entry is not found, the device broadcasts ping packets in the VLAN.	-

Parameter	Description	Value
-c *count*	Specifies the number of ping attempts.	The value is an integer that ranges from 1 to 4294967295. The default value is 5.
-s *packetsize*	Specifies the size of a ping packet. On the device running IEEE 802.1ag Draft 7, the value does not contain the length of the Layer 2 packet header. On the device running IEEE Standard 802.1ag-2007, the value is the size of a ping packet.	The value is an integer that ranges from 95 to 9000, in bytes. The default value is 95.
-t *timeout*	Specifies the timeout interval for waiting for a response packet.	The value is an integer that ranges from 1 to 65535, in milliseconds. The default value is 2000 ms.
-p *priority-value*	Specifies the priority of ping packets.	The value is an integer that ranges from 0 to 7. The default value is 7.

Views

All views

Default Level

0: Visit level

Usage Guidelines

Usage Scenario

To use GMAC ping to detect connectivity, use the **ping mac** command.

Prerequisites

GMAC ping has been enabled using the **ping mac enable** command.

Precautions

A MEP is not required to initiate GMAC ping. The destination node can be not a MEP or MIP. You can perform GMAC ping without configuring the MD, MA, or MEP on the source device, intermediate device, and destination device. You must specify the VLAN on which the destination node resides.

NOTE

The two devices must be configured with IEEE 802.1ag of the same version. If the local device is configured with IEEE 802.1ag Draft 7 and the peer device is configured with IEEE Standard 802.1ag-2007, the **ping mac** command does not take effect. That is, the local device cannot ping the peer device.

Example

# Ping the device with the MAC address of 00e0-fc00-0204. Send two ping packets with the size of 112 bytes each. The device is in VLAN 10.

```
<HUAWEI> system-view
[HUAWEI] ping mac enable
[HUAWEI] ping mac 00e0-fc00-0204 vlan 10 -c 2 -s 112
Pinging 00e0-fc00-0204 with 112 bytes of data:
Reply from 00e0-fc00-0204: byte = 112 time = 9ms
Reply from 00e0-fc00-0204: byte = 112 time = 11ms
Packets: Sent = 2, Received = 2, Lost = 0 (0% Loss)
Minimum = 9ms, Maximum = 11ms, Average = 10ms
```

Table 5-45 Description of the ping mac command output

Item	Description
Reply from 00e0-fc00-0204: byte = 112 time = 9ms	Size and response time of ping packets returned from the destination device. When the response time is less than 1 ms, "time < 1ms" is displayed.
Packets: Sent = 2, Received = 2, Lost = 0 (0% Loss)	Number of sent ping packets, number of received reply packets, and number and percentage of discarded packets.
Minimum	Minimum round-trip time (RTT).
Maximum	Maximum RTT.
Average	Average RTT.

5.3.25 ping mac enable

Function

The **ping mac enable** command enables GMAC ping.

The **undo ping mac enable** command disables GMAC ping.

By default, GMAC ping is disabled.

Format

ping mac enable

undo ping mac enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To implement the following functions, use the **ping mac enable** command:

- Implement GMAC ping.
- Enable the device to respond to received GMAC ping packets.

Example

# Enable GMAC ping.

```
<HUAWEI> system-view
[HUAWEI] ping mac enable
```

5.3.26 policy-vlan

Function

The **policy-vlan** command configures policy-based VLAN assignment by associating a MAC address and IP address binding policy to a VLAN and setting the 802.1p priority of the VLAN.

The **undo policy-vlan** command disassociates a MAC address and IP address binding policy from a VLAN.

By default, a VLAN is not associated with any MAC address and IP address binding policy.

Format

policy-vlan mac-address *mac-address* **ip** *ip-address* [**interface** *interface-type interface-number*] [**priority** *priority*]

undo policy-vlan { **all** | **mac-address** *mac-address* **ip** *ip-address* [**interface** *interface-type interface-number*] }

Parameters

Parameter	Description	Value
mac-address *mac-address*	Specifies the source MAC address associated with a VLAN.	The value is in H-H-H format. H is a hexadecimal number of 4 digits, for example, 00e0 and fc01. If you enter fewer than four digits, 0s are prefixed to the input digits. For example, if you enter e0, the system changes e0 to 00e0. The MAC address cannot be 0000-0000-0000, FFFF-FFFF-FFFF, or a multicast MAC address.
ip *ip-address*	Specifies the IP address associated with a VLAN.	The value is in dotted decimal notation.
interface *interface-type interface-number*	Specifies the interface where the MAC address and IP address binding policy is applied. ● *interface-type* specifies the type of an interface. ● *interface-number* specifies the number of an interface. If this parameter is not specified, the binding policy is applied to all the interfaces in the VLAN. If this parameter is specified, the binding policy is applied to the specified interface.	-
priority *priority*	Specifies the 802.1p priority of the VLAN associated with the MAC address and IP address.	The value is an integer that ranges from 0 to 7. A larger value indicates a higher priority. The default value is 0.
all	Disassociates all MAC address and IP address binding policies from a VLAN.	-

Views

VLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Policy-based VLAN assignment is a method to assign VLANs based on source MAC addresses and IP addresses of packets. This method is applicable to networks where high security is required and user devices move frequently.

When receiving an untagged packet, an interface matches the source IP address and source MAC address of the packet with the entries in the policy-based VLAN table.

- If a matching entry is found, the interface forwards the packet based on the matching VLAN ID and priority.
- If no matching entry is found, the interface uses other matching rules to forward the packet.

Policy-based VLAN assignment takes effect only for untagged packets, whereas tagged packets are forwarded based on port-based VLANs.

Precautions

On the S1720GW-E, S1720GWR-E, S5720I-SI, S5720-LI, and S5720S-LI, when the **ip error-packet-check disable** command is used to disable IP packet check, IP subnet-based VLAN assignment and policy-based VLAN assignment do not take effect.

After a MAC address or IP address is associated with a VLAN, it cannot be associated with other VLANs.

If you run the **policy-vlan** command multiple times in the same VLAN view, all the specified IP addresses and MAC addresses are associated with the VLAN.

Example

# Bind MAC address 0-1-1 and IP address 10.1.1.1 to VLAN 2, and set the 802.1p priority of the VLAN to 7.

```
<HUAWEI> system-view
[HUAWEI] vlan 2
[HUAWEI-vlan2] policy-vlan mac-address 0-1-1 ip 10.1.1.1 priority 7
```

5.3.27 port

Function

The **port** command configures a VLAN as the default VLAN of an interface and adds the interface to the VLAN.

The **undo port** command restores the default VLAN of an interface to the default setting.

By default, VLAN 1 is the default VLAN of all interfaces.

Format

port *interface-type* { *interface-number1* [**to** *interface-number2*] } &<1-10>

undo port *interface-type* { *interface-number1* [**to** *interface-number2*] } &<1-10>

Parameters

Parameter	Description	Value
interface-type { *interface-number1* [**to** *interface-number2*] }	Configures the default VLAN for multiple interfaces. ● *interface-type* specifies the type of interfaces. ● *interface-number1* specifies the number of the first interface. ● *interface-number2* specifies the number of the last interface. The value of *interface-number2* must be greater than the value of *interface-number1*. The *interface-number1* and *interface-number2* parameters identify a range of interfaces. If **to** *interface-number2* is not specified, only one interface is specified. You can specify 10 interface ranges at one time.	-

Views

VLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

All frames sent from a user device are untagged, and frames sent from a remote device may also be untagged. However, the device processes only tagged frames. Therefore, the device adds a tag to each untagged frame received by an interface. The default VLAN ID of the interface can be added to untagged frames so that these frames are forwarded in the default VLAN.

After the default VLAN is specified for an access interface or a QinQ interface, packets passing through the interface are processed as follows:

- When the interface receives an untagged frame, it tags the frame with the default VLAN ID.
- When the interface receives a tagged packet:
  - If the interface is an access interface, it compares the VLAN ID of the packet with the default VLAN ID. If they are the same, the interface forwards the packets; otherwise, the interface discards the packets.
  - If the interface is a QinQ interface, it adds an outer tag with the default VLAN ID to the packet.
- Before forwarding tagged packets, access and QinQ interfaces remove VLAN tags from the packets.

Prerequisites

The link-type of specified interfaces cannot be hybrid or trunk before you run the **port** command.

Precautions

A super VLAN cannot be configured as the default VLAN of interfaces.

The **undo port** command deletes the default VLAN of the specified interfaces only if the current VLAN is the default VLAN of these interfaces.

If you run the **port** command multiple times in the same VLAN view, the VLAN is configured as the default VLAN of all the specified interfaces.

You can also run the **port default vlan** command in the interface view to configure the default VLAN for an interface. The two commands have the same function.

Example

# Configure VLAN 3 as the default VLAN of interfaces GE0/0/1 to GE0/0/4.

```
<HUAWEI> system-view
[HUAWEI] vlan 3
[HUAWEI-vlan3] port gigabitethernet 0/0/1 to 0/0/4
```

5.3.28 port default vlan

Function

The **port default vlan** command configures the default VLAN of an interface and adds the interface to the VLAN.

The **undo port default vlan** command restores the default VLAN of an interface to the default setting.

By default, VLAN 1 is the default VLAN of all interfaces.

Format

port default vlan *vlan-id* [**step** *step-number* [**increased** | **decreased**]]

undo port default vlan

Parameters

Parameter	Description	Value
vlan-id	Specifies the ID of the default VLAN.	The value is an integer that ranges from 1 to 4094.

Parameter	Description	Value
step *step-number* [**increased** | **decreased**]	Specifies that the interface added to an interface group can be bound to VLANs starting from the one identified by *vlan-id* in an ascending or descending order at a step specified by *step-number*. **increased** specifies an increase in the values of VLAN IDs starting from the one identified by *vlan-id* at a step specified by *step-number* to add the interfaces to the VLANs. Whereas **decreased** specifies a decrease in the values of VLAN IDs starting from the one identified by *vlan-id* at a step specified by *step-number* to add the interfaces to the VLANs. For example, you can configure **increased**, and set *vlan-id* to 10 and *step-number* to 20 in the **port default vlan** command. After this configuration, interface 1 joins VLAN 10; interface 2 joins VLAN 30... By analogy, interface 10 joins VLAN 190. **NOTE** ● This parameter can only be used in the port group view. ● When using **step** and *vlan-id* in the command, ensure that all interfaces added to the VLAN are available. ● If this parameter is not specified, all interfaces in an interface group are added into the same VLAN, that is, VLAN *vlan-id*.	The value is an integer that ranges from 1 to 4093.

Views

Ethernet interface view, GE interface view, XGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, MultiGE interface view, VE interface view, Eth-Trunk interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

All frames sent from a user device are untagged, and frames sent from a remote device may also be untagged. However, the device processes only tagged frames. Therefore, the device adds a tag to each untagged frame received by an interface. The default VLAN ID of the interface can be added to untagged frames so that these frames are forwarded in the default VLAN.

After the default VLAN is specified for an access interface or a QinQ interface, packets passing through the interface are processed as follows:

- When the interface receives an untagged frame, it tags the frame with the default VLAN tag.
- When the interface receives a tagged packet:
  - If the interface is an access interface, it compares the VLAN ID of the packet with the default VLAN ID. If they are the same, the interface forwards the packet; otherwise, the interface discards the packet.
  - If the interface is a QinQ interface, it adds an outer tag with the default VLAN ID to the packet.
- Before forwarding tagged packets, access and QinQ interfaces remove VLAN tags from the packets.

Prerequisites

The interface type is negotiation-desirable, negotiation-auto, access or QinQ. If not, run the **port link-type** command to change the interface type. The interface where **negotiation-desirable** or **negotiation-auto** is configured must be negotiated as an access interface so that the default VLAN configured by the **port default vlan** command takes effect.

Precautions

- If the ID of a nonexistent VLAN is configured as the PVID, VLAN 1 is added to the untagged packets. After the PVID is configured globally, the PVID of the interface is changed to the configured one.
- You can also run the **port** command in the VLAN view to configure the default VLAN of an interface. The two commands have the same function.
- A super VLAN cannot be configured as the default VLAN of interfaces.
- This command is invalid on a member interface of an Eth-Trunk.

- If you run the **port default vlan** command multiple times in the same interface view, only the latest configuration takes effect.

Example

# Configure VLAN 3 (an existing VLAN) as the default VLAN of GE0/0/1 (an access interface).

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] port link-type access
[HUAWEI-GigabitEthernet0/0/1] port default vlan 3
```

5.3.29 port discard tagged-packet

Function

The **port discard tagged-packet** command configures an interface to discard incoming tagged frames.

The **undo port discard tagged-packet** command configures an interface not to discard incoming tagged frames.

By default, an interface does not discard incoming tagged frames.

Format

port discard tagged-packet

undo port discard tagged-packet

Parameters

None

Views

Ethernet interface view, GE interface view, XGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, MultiGE interface view, VE interface view, Eth-Trunk interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

All frames sent from user devices are untagged, so user-side interfaces on a switch should not receive tagged frames. If a user connects a switching device to a user-side interface without permission, the user-side interface may receive tagged frames. The **port discard tagged-packet** command enables the user-side interface to discard untagged frames, preventing unauthorized access.

Precautions

The **port discard tagged-packet** command cannot function when dot1q-tunnel interfaces are configured on switches except the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S.

Use this command only on interfaces connected to user devices. If you run this command on a network-side interface, users in the same VLAN may fail to communicate.

Example

# Configure GE0/0/1 to discard incoming tagged frames.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] port discard tagged-packet
```

5.3.30 port hybrid pvid vlan

Function

The **port hybrid pvid vlan** command specifies the default VLAN ID of a hybrid interface.

The **undo port hybrid pvid vlan** command restores the default VLAN ID of a hybrid interface to the default setting.

By default, VLAN 1 is the default VLAN ID of all interfaces.

Format

port hybrid pvid vlan *vlan-id*

undo port hybrid pvid vlan

Parameters

Parameter	Description	Value
vlan-id	Specifies the default VLAN ID of a hybrid interface.	The value is an integer that ranges from 1 to 4094.

Views

Ethernet interface view, GE interface view, XGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, MultiGE interface view, VE interface view, Eth-Trunk interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

An interface may receive untagged and tagged frames, but the device processes only tagged frames. Therefore, the device adds a tag to each untagged frame received by an interface. The default VLAN ID of the interface can be added to untagged frames so that these frames are forwarded in the default VLAN.

A hybrid interface processes Ethernet frames as follows:

- When the interface receives an untagged frame, it tags the frame with the default VLAN ID. If the default VLAN ID is allowed by the interface, the interface accepts the frame. Otherwise, the interface discards the frame.
- When the interface receives a tagged frame, it accepts the frame if the VLAN ID of the frame is in the list of allowed VLAN IDs. Otherwise, the interface discards the frame.
- If the VLAN ID of a frame is allowed by the interface, the interface forwards the frame.

Prerequisites

If an interface is not a hybrid interface, run the **port link-type hybrid** command to change the interface type to hybrid.

Precautions

- If the ID of a nonexistent VLAN is configured as the PVID, VLAN 1 is added to the untagged packets. After the PVID is configured globally, the PVID of the interface is changed to the configured one.
- This command is invalid on a member interface of an Eth-Trunk.
- The **port hybrid pvid vlan** command only specifies the default VLAN for an interface but does not add the interface to the default VLAN.
- If you run the **port hybrid pvid vlan** command multiple times in the same interface view, only the latest configuration takes effect.

Example

# Specify VLAN 5 as the default VLAN of GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] vlan 5
[HUAWEI-vlan5] quit
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] port link-type hybrid
[HUAWEI-GigabitEthernet0/0/1] port hybrid pvid vlan 5
```

5.3.31 port hybrid tagged vlan

Function

The **port hybrid tagged vlan** command adds a hybrid interface to the specified VLANs. Frames of the VLANs then pass through the hybrid interface in tagged mode.

The **undo port hybrid vlan** command removes a hybrid interface from the specified VLANs.

By default, a hybrid interface is added to VLAN 1 in untagged mode.

Format

port hybrid tagged vlan { { *vlan-id1* [**to** *vlan-id2*] }&<1-10> | **all** }

undo port hybrid [**tagged**] **vlan** { { *vlan-id1* [**to** *vlan-id2*] }&<1-10> | **all** }

(Port group view) **port hybrid tagged vlan** *vlan-id3* [**step** *step-number* [**increased** | **decreased**]]

(Port group view) **undo port hybrid vlan** *vlan-id3* [**step** *step-number* [**increased** | **decreased**]]

Parameters

Parameter	Description	Value
vlan-id1 [**to** *vlan-id2*]	Adds a hybrid interface to specified VLANs. ● *vlan-id1* specifies the start VLAN ID. ● **to** *vlan-id2* specifies the end VLAN ID. The value of *vlan-id2* must be greater than or equal to the value of *vlan-id1*.	The value of *vlan-id1* is an integer that ranges from 1 to 4094. The value of *vlan-id2* is an integer that ranges from 1 to 4094.
all	Adds a hybrid interface to all VLANs.	-
vlan-id3	Specifies the ID of the start VLAN to be bound to the member port of a port group.	The value is an integer that ranges from 1 to 4094.

Parameter	Description	Value
step *step-number*	Specifies the step for the increase or decrease in the value of the VLAN ID. With this parameter specified, the member ports in a port group can be bound to VLANs starting from the one identified by *vlan-id3* in an ascending or descending order at a step specified by *step-number*. This facilitates the subsequent user configuration. For example: A port group has 10 member ports. You can configure **increased**, and set *vlan-id3* to 1 and *step-number* to 1 in the **port hybrid tagged vlan** command. After this configuration, member port 1 joins VLAN 1; member port 2 joins VLAN 2... By analogy, member port 10 joins VLAN 10.	The value is an integer that ranges from 1 to 4093.
increased	Specifies an increase in the values of VLAN IDs starting from the one identified by *vlan-id3* at a step specified by *step-number* to bind the VLANs to the member ports of a port group.	By default, Layer 2 ports are bound to the VLANs in an ascending order.

Parameter	Description	Value
decreased	Specifies a decrease in the values of VLAN IDs starting from the one identified by *vlan-id3* at a step specified by *step-number* to bind the VLANs to the member ports of a port group. When setting **decreased**, ensure that the value of *vlan-id3* is greater than or equal to the number of the member ports of the port group.	-

Views

Ethernet interface view, GE interface view, XGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, MultiGE interface view, VE interface view, Eth-Trunk interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A hybrid interface can connect to either a user device or a switch. This command adds a hybrid interface to VLANs in tagged mode so that the hybrid interface allows frames from the VLANs to pass.

After a hybrid interface is added to VLANs in tagged mode, the interface forwards frames without removing VLAN tags of frames.

Prerequisites

If an interface is not a hybrid interface, run the **port link-type hybrid** command to change the interface type to hybrid.

Precautions

- This command is invalid on a member interface of an Eth-Trunk.
- A super VLAN cannot be specified in the command.
- If you run the **port hybrid tagged vlan** command multiple times in the same interface view, the interface is added to all the specified VLANs.
- Running the **undo port hybrid tagged vlan** command on a hybrid interface removes the interface from specific VLANs it joins using the **port hybrid tagged vlan** command.

Example

# Add GE0/0/1 to VLAN 3 to VLAN 5 in tagged mode.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] port link-type hybrid
[HUAWEI-GigabitEthernet0/0/1] port hybrid tagged vlan 3 to 5
```

5.3.32 port hybrid untagged vlan

Function

The **port hybrid untagged vlan** command adds a hybrid interface to the specified VLANs. Frames of the VLANs then pass through the hybrid interface in untagged mode.

The **undo port hybrid vlan** command removes a hybrid interface from the specified VLANs.

By default, a hybrid interface is added to VLAN 1 in untagged mode.

Format

port hybrid untagged vlan { { *vlan-id1* [**to** *vlan-id2*] }&<1-10> | **all** }

undo port hybrid [**untagged**] **vlan**{ { *vlan-id1* [**to** *vlan-id2*] }&<1-10> | **all** }

(Port group view) **port hybrid untagged vlan** *vlan-id3* [**step** *step-number* [**increased** | **decreased**]]

(Port group view) **undo port hybrid vlan** *vlan-id3* [**step** *step-number* [**increased** | **decreased**]]

Parameters

Parameter	Description	Value
vlan-id1 [**to** *vlan-id2*]	Adds a hybrid interface to specified VLANs. ● *vlan-id1* specifies the start VLAN ID. ● **to** *vlan-id2* specifies the end VLAN ID. The value of *vlan-id2* must be greater than or equal to the value of *vlan-id1*.	The value of *vlan-id1* is an integer that ranges from 1 to 4094. The value of *vlan-id2* is an integer that ranges from 1 to 4094.
all	Adds a hybrid interface to all VLANs.	-

Parameter	Description	Value
vlan-id3	Specifies the ID of the start VLAN to be bound to the member port of a port group.	The value is an integer that ranges from 1 to 4094.
step *step-number*	Specifies the step for the increase or decrease in the value of the VLAN ID. With this parameter specified, the member ports in a port group can be bound to VLANs starting from the one identified by *vlan-id3* in an ascending or descending order at a step specified by *step-number*. This facilitates the subsequent user configuration. For example: A port group has 10 member ports. You can configure **increased**, and set *vlan-id3* to 1 and *step-number* to 1 in the **port hybrid untagged vlan** command. After this configuration, member port 1 joins VLAN 1; member port 2 joins VLAN 2... By analogy, member port 10 joins VLAN 10.	The value is an integer that ranges from 1 to 4093.
increased	Specifies an increase in the values of VLAN IDs starting from the one identified by *vlan-id3* at a step specified by *step-number* to bind the VLANs to the member ports of a port group.	By default, Layer 2 ports are bound to the VLANs in an ascending order.

Parameter	Description	Value
decreased	Specifies a decrease in the values of VLAN IDs starting from the one identified by *vlan-id3* at a step specified by *step-number* to bind the VLANs to the member ports of a port group. When setting **decreased**, ensure that the value of *vlan-id3* is greater than or equal to the number of the member ports of the port group.	-

Views

Ethernet interface view, GE interface view, XGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, MultiGE interface view, VE interface view, Eth-Trunk interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A hybrid interface can connect to either a user device or a switch. When a hybrid interface is connected to a user device, it must be added to VLANs in untagged mode so that it sends untagged frames. When a hybrid interface is connected to a switch, it can receive and forward frames with the same VLAN tag (in the tagged VLAN or untagged VLAN list) from the switch.

After a hybrid interface is added to VLANs in untagged mode, the interface removes VLAN tags of frames before sending frames.

Prerequisites

The link type of the interface has been changed to hybrid using the **port link-type hybrid** command.

Precautions

- This command is invalid on a member interface of an Eth-Trunk.
- A super VLAN cannot be specified in the command.
- If you run the **port hybrid untagged vlan** command multiple times in the same interface view, the interface is added to all the specified VLANs.

- Running the **undo port hybrid untagged vlan** command on a hybrid interface removes the interface from specific VLANs it joins using the **port hybrid untagged vlan** command.

Example

# Add GE0/0/1 to VLAN 3 to VLAN 5 in untagged mode.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] port link-type hybrid
[HUAWEI-GigabitEthernet0/0/1] port hybrid untagged vlan 3 to 5
```

5.3.33 port hybrid vlan 1

Function

The **port hybrid vlan 1** command adds a Hybrid port to VLAN 1 in untagged mode.

The **undo port hybrid vlan 1** command deletes a Hybrid port from VLAN 1.

Format

port hybrid vlan 1

undo port hybrid vlan 1

Parameters

None

Views

Ethernet interface view, GE interface view, XGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, MultiGE interface view, VE interface view, Eth-Trunk interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

All interfaces on the device join VLAN 1 by default, and the hybrid interface joins VLAN 1 in untagged mode by default. When there are unknown unicast packets, multicast packets, or broadcast packets of VLAN 1, broadcast storms may occur. For the hybrid interface that does not need to join VLAN 1, you need to run the **undo port hybrid vlan 1** command to delete the hybrid interface from VLAN 1 to prevent loops. When the network changes and the hybrid interface needs to join VLAN 1 in untagged mode, run the **port hybrid vlan 1** command.

Prerequisites

If an interface is not a hybrid interface, run the **port link-type hybrid** command to change the interface type to hybrid.

Precautions

This command cannot be used for a physical interface that has been added to an Eth-Trunk interface.

Example

# Add GE 0/0/1 to VLAN 1 in Untagged mode.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] port link-type hybrid
[HUAWEI-GigabitEthernet0/0/1] port hybrid vlan 1
```

5.3.34 port link-type

Function

The **port link-type** command sets the link type of an interface.

The **undo port link-type** command restores the default link type of an interface.

By default, the link type of an interface on the SS1720GW-E, S1720GWR-E, S5720I-SI, S5720-LI, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5720S-LI, S5735-S, S500, S5735S-S, S5735-S-I, S5735S-H, and S5736-S, S6720S-S is **negotiation-auto**, and the link type of an interface on other models is **negotiation-desirable**.

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S support VE interfaces. You can configure the link type for a VE interface only after the VE interface is switched to Layer 2 mode using the **portswitch** command. The default link type is hybrid.

Format

port link-type { **access** | **dot1q-tunnel** | **hybrid** | **trunk** | **negotiation-desirable** | **negotiation-auto** }

undo port link-type

Parameters

Parameter	Description	Value
access	Sets the link type of an interface to access.	-
dot1q-tunnel	Sets the link type of an interface to QinQ.	-
hybrid	Sets the link type of an interface to hybrid.	-

Parameter	Description	Value
trunk	Sets the link type of an interface to trunk.	-
negotiation-desirable	Sets LNP negotiation mode for a Layer 2 Ethernet interface to negotiation-desirable. **NOTE** This parameter is not supported in the VE interface view.	-
negotiation-auto	Sets the LNP negotiation mode for a Layer 2 Ethernet interface to negotiation-auto. **NOTE** This parameter is not supported in the VE interface view.	-

Views

Ethernet interface view, GE interface view, XGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, MultiGE interface view, VE interface view, Eth-Trunk interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Access, hybrid, trunk, and dot1q-tunnel link types are statically configured, and the LNP negotiation mode of **negotiation-desirable** or **negotiation-auto** is dynamically negotiated. The interface where **negotiation-desirable** or **negotiation-auto** is configured is negotiated as the access or trunk interface.

Characteristics of different interfaces are:

- An access interface connects to a user device. It can connect only to an access link, and Ethernet frames transmitted on the access link are untagged. If the default VLAN is configured for an access interface, the interface adds a VLAN tag to packets and sets the VID field in the VLAN tag to the default VLAN ID. The access link transmits only the packets with the default VLAN ID.
- A trunk interface connects to a switch and can connect only to a trunk link. A trunk interface allows frames from multiple VLANs to pass.

- A hybrid interface can connect to either a user device or a switch, and it can connect to an access link or a trunk link. A hybrid interface allows frames from multiple VLANs to pass and can remove VLAN tags of outgoing frames.
- A QinQ interface connects to a switch and can process double-tagged frames.
- The interface configured with **negotiation-desirable** can actively send negotiation packets, while the interface configured with **negotiation-auto** cannot actively send negotiation packets. The interface where **negotiation-desirable** or **negotiation-auto** is configured is negotiated as the access or trunk interface through LNP and added to a VLAN. **Table 5-46** describes the negotiation result when the local and remote ends use different negotiation modes.

Table 5-46 LNP negotiation

Local LNP Negotiation Mode	Remote Link Type or LNP Negotiation Mode	Locally Negotiated Link Type	Remotely Negotiated Link Type	Link Type When Negotiation Fails
negotiation-desirable/ negotiation-auto	Access (negotiate on)	Access	Access	Access
	Hybrid (negotiate on)	Trunk	Hybrid	Access
	Dot1q-tunnel (negotiate on)	Access	Dot1q-tunnel	Access
	Trunk (negotiate on)	Trunk	Trunk	Access
	LNP negotiation not supported or negotiate off	Access	N/A	Access
negotiation-desirable	negotiation-desirable	Trunk	Trunk	Access
negotiation-desirable	negotiation-desirable	Trunk	Trunk	Access
negotiation-auto	negotiation-desirable	Access	Access	Access

negotiate on: LNP negotiation is enabled. negotiate off: LNP negotiation is disabled. N/A: The link type is uncertain.

Prerequisites

LNP has been enabled.

Follow-up Procedure

Add the interface to VLANs.

Precautions

This command is invalid on a member interface of an Eth-Trunk.

Starting from V200R005C00, the default link type of an interface is not hybrid. Before upgrading the device of an earlier version of V200R005C00 to V200R005C00 or later, the **port link-type hybrid** command configuration is generated.

If you run the **port link-type** command multiple times in the same interface view, only the latest configuration takes effect.

After VLAN-related configurations are configured on an interface, the **[undo] port link-type** command is an interactive command. You need to enter confirmation information.

When using LNP negotiation, pay attention to the following points:

- If a Layer 2 Ethernet interface is Down, it does not participate in LNP negotiation.
- If the two ends of an Eth-Trunk link have different numbers of member interfaces, LNP negotiation may fail.
- If the link type of the Layer 2 Ethernet interface is configured as access, hybrid, trunk, or dot1q-tunnel using the **port link-type** command, LNP does not take effect on the interface.
- The interface configured with **negotiation-desirable** or **negotiation-auto** is negotiated as an access or trunk interface. By default, the negotiated access interface joins VLAN 1, and the negotiated trunk interface allows all VLANs and uses default VLAN 1. **port default vlan** and **port trunk allow-pass only-vlan** can be simultaneously used on the interface configured with **negotiation-desirable** or **negotiation-auto**. If the interface is negotiated as an access interface, **port default vlan** takes effect. If the interface is negotiated as a trunk interface, **port trunk allow-pass only-vlan** takes effect.

Before changing the link type of an interface, you do not need to restore the default VLAN configuration. However, if the link type of the interface is changed, the VLAN configuration of the interface is deleted. Exercise caution when you perform this configuration.

There are limitations on the interface where **negotiation-desirable** or **negotiation-auto** is configured:

- The sub-interface cannot be created.
- No MUX VLAN can be enabled.
- No voice VLAN in auto mode can be configured.

Dot1q-tunnel interfaces do not support the voice VLAN function.

On the S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735-S-I, and S5735S-S, after the **port link-type dot1q-tunnel** command is run on an interface, IP packets cannot be forwarded on the interface.

If the device works in VBST mode, changing the link type of an interface may cause a loop on the network, resulting in a traffic storm. If the link type of an interface must be changed, disable the interfaces on both ends and then change the link type of these interfaces.

Example

# Set the link type of GE0/0/1 to trunk.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] port link-type trunk
```

5.3.35 port negotiation disable

Function

The **port negotiation disable** command disables LNP negotiation on a Layer 2 Ethernet interface.

The **undo port negotiation disable** command enables LNP negotiation on a Layer 2 Ethernet interface.

By default, LNP negotiation is enabled on a Layer 2 Ethernet interface.

Format

port negotiation disable

undo port negotiation disable

Parameters

None

Views

Ethernet interface view, GE interface view, XGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, MultiGE interface view, VE interface view, Eth-Trunk interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

By default, LNP negotiation is enabled for all interfaces on a Layer 2 device. If an LNP-capable Layer 2 device is connected to an LNP-incapable Layer 2 device, the LNP-capable device keeps sending LNP packets, wasting bandwidth resources. In this situation, you can run the **port negotiation disable** command to disable LNP negotiation on the Layer 2 Ethernet interface connected to the LNP-incapable Layer 2 device.

To disable LNP negotiation on all interfaces of a Layer 2 device, run the **lnp disable** command in the system view.

Prerequisites

The interface must be a layer 2 interface before using the **port negotiation disable** command. Use the **portswitch** command to switch a layer 3 interface to a Layer 2 interface.

Precautions

By default, LNP negotiation is enabled for all interfaces on a Layer 2 device. If you run the **lnp disable** command in the system view to disable LNP negotiation on all interfaces of a Layer 2 device. LNP negotiation cannot be enabled on a Layer 2 Ethernet interface by running the **undo port negotiation disable** command in the interface view.

For LNP negotiation to take effect, LNP negotiation must be enabled on both the device and Layer 2 Ethernet interfaces.

Example

# Disable LNP negotiation on a Layer 2 Ethernet interface.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] port negotiation disable
```

5.3.36 port trunk allow-pass vlan

Function

The **port trunk allow-pass vlan** command adds a trunk interface to the specified VLANs.

The **undo port trunk allow-pass vlan** command deletes a trunk interface from the specified VLANs.

By default, a trunk interface is in VLAN 1.

Format

port trunk allow-pass vlan { { *vlan-id1* [**to** *vlan-id2*] }&<1-10> | **all** }

undo port trunk allow-pass vlan { { *vlan-id1* [**to** *vlan-id2*] }&<1-10> | **all** }

(Port group view) **port trunk allow-pass vlan** *vlan-id3* [**step** *step-number* [**increased** | **decreased**]]

(Port group view) **undo port trunk allow-pass vlan** *vlan-id3* [**step** *step-number* [**increased** | **decreased**]]

Parameters

Parameter	Description	Value
vlan-id1 [**to** *vlan-id2*]	Adds a trunk interface to specified VLANs. ● *vlan-id1* specifies the start VLAN ID. ● **to** *vlan-id2* specifies the end VLAN ID. The value of *vlan-id2* must be greater than or equal to the value of *vlan-id1*.	The value of *vlan-id1* is an integer that ranges from 1 to 4094. The value of *vlan-id2* is an integer that ranges from 1 to 4094.
all	Adds a trunk interface to all VLANs.	-
vlan-id3	Specifies the ID of the start VLAN to be bound to the member port of a port group.	The value is an integer that ranges from 1 to 4094.
step *step-number*	Specifies the step for the increase or decrease in the value of the VLAN ID. With this parameter specified, the member ports in a port group can be bound to VLANs starting from the one identified by *vlan-id3* in an ascending or descending order at a step specified by *step-number*. This facilitates the subsequent user configuration. For example: A port group has 10 member ports. You can configure **increased**, and set *vlan-id3* to 1 and *step-number* to 1 in the **port trunk allow-pass vlan** command. After this configuration, member port 1 joins VLAN 1; member port 2 joins VLAN 2... By analogy, member port 10 joins VLAN 10.	The value is an integer that ranges from 1 to 4093.

Parameter	Description	Value
increased	Specifies an increase in the values of VLAN IDs starting from the one identified by *vlan-id3* at a step specified by *step-number* to bind the VLANs to the member ports of a port group.	By default, Layer 2 ports are bound to the VLANs in an ascending order.
decreased	Specifies a decrease in the values of VLAN IDs starting from the one identified by *vlan-id3* at a step specified by *step-number* to bind the VLANs to the member ports of a port group. When setting **decreased**, ensure that the value of *vlan-id3* is greater than or equal to the number of the member ports of the port group.	-

Views

Ethernet interface view, GE interface view, XGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, MultiGE interface view, VE interface view, Eth-Trunk interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A trunk interface can join multiple VLANs and connects to a network device. To allow all packets from one or more VLANs to pass through a trunk interface, the trunk interface must be added to the VLANs using the **port trunk allow-pass vlan** command.

Prerequisites

The link type of the interface has been set to trunk or negotiation.

Precautions

If a specified VLAN does not exist, the configuration does not take effect.

The command cannot be used on a member interface of an Eth-Trunk.

If you run the **port trunk allow-pass vlan** command multiple times in the same interface view, the interface is added to all the specified VLANs.

If a port is configured with a PVID VLAN, run the **port trunk allow-pass vlan** *pvid-vlan* command to add the PVID VLAN to the port.

Example

# Add GE0/0/1 to VLANs 10 to 30.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] port link-type trunk
[HUAWEI-GigabitEthernet0/0/1] port trunk allow-pass vlan 10 to 30
```

5.3.37 port trunk allow-pass only-vlan

Function

The **port trunk allow-pass only-vlan** command configures VLANs allowed by the interface that is configured as a trunk interface through LNP negotiation.

The **undo port trunk allow-pass only-vlan** command restores the default VLANs allowed by the interface that is configured as a trunk interface through LNP negotiation.

By default, if the Layer 2 Ethernet interface is negotiated as a trunk interface, the interface allows all VLANs.

Format

port trunk allow-pass only-vlan { { *vlan-id1* [**to** *vlan-id2*] } &<1-10> | **none** }

undo port trunk allow-pass only-vlan

Parameters

Parameter	Description	Value
vlan-id1 [**to** *vlan-id2*]	Specifies VLANs on a Layer 2 Ethernet interface so that the interface forwards only packets for these VLANs after LNP negotiation. ● *vlan-id1* specifies the first VLAN. ● **to** *vlan-id2* specifies the last VLAN. *vlan-id2* must be greater than or equal to *vlan-id1*. *vlan-id2* and *vlan-id1* specify a VLAN range. ● If **to** *vlan-id2* is not specified, only the VLAN specified by *vlan-id1* can be configured for the Layer 2 Ethernet interface. In one **port trunk allow-pass only-vlan** command, a maximum of 10 VLAN ranges can be specified using **to**.	The value is an integer ranging from 1 to 4094.

Parameter	Description	Value
none	Specifies that the Layer 2 Ethernet interface cannot forward packets for any VLAN after the LNP negotiation.	-

Views

Ethernet interface view, GE interface view, XGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, MultiGE interface view, VE interface view, Eth-Trunk interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Link-type Negotiation Protocol (LNP) dynamically negotiates the link type of an Ethernet interface. The negotiated link type can be access or trunk.

In routine maintenance, if the network administrator wants to update the VLANs on a Layer 2 Ethernet interface so that the interface forwards only packets for these VLANs after LNP negotiation, perform the following operations in the corresponding interface view.

1. Run the **port trunk allow-pass vlan all** command to delete all VLANs from the Layer 2 Ethernet interface.
2. Run the **port trunk allow-pass only-vlan** { { *vlan-id1* [**to** *vlan-id2*] } &<1-10> | **none** } to update VLANs on the Layer 2 Ethernet interface so that the interface forwards only packets for these VLANs after LNP negotiation.

Alternatively, to simplify configurations and reduce the network administrator's maintenance workload, run the **port trunk allow-pass only-vlan** to update VLANs on the Layer 2 Ethernet interface so that the interface forwards only packets for these VLANs after LNP negotiation.

Prerequisites

The LNP function is supported on the Layer 2 Ethernet interface, and the Layer 2 Ethernet interface is configured to work in auto-negotiation mode using the **port link-type negotiation** command.

Example

# Configure VLANs 10 to 20 on the interface so that the interface forwards only packets for these VLANs.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet0/0/1
[HUAWEI-GigabitEthernet0/0/1] port trunk allow-pass only-vlan 10 to 20
```

5.3.38 port trunk pvid vlan

Function

The **port trunk pvid vlan** command specifies the default VLAN for a trunk interface.

The **undo port trunk pvid vlan** command restores the default VLAN of a trunk interface to the default setting.

By default, VLAN 1 is the default VLAN of trunk interfaces.

Format

port trunk pvid vlan *vlan-id*

undo port trunk pvid vlan

Parameters

Parameter	Description	Value
vlan-id	Specifies the default VLAN ID of a trunk interface.	The value is an integer that ranges from 1 to 4094.

Views

Ethernet interface view, GE interface view, XGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, MultiGE interface view, VE interface view, Eth-Trunk interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

An interface may receive untagged and tagged frames, but the device processes only tagged frames. Therefore, the device adds a tag to each untagged frame received by an interface. The default VLAN ID of the interface can be added to untagged frames so that these frames are forwarded in the default VLAN.

Follow-up Procedure

Add the trunk interface to the default VLAN.

Precautions

- If the ID of a nonexistent VLAN is configured as the PVID, VLAN 1 is added to the untagged packets. After the PVID is configured globally, the PVID of the interface is changed to the configured one.

- The **port trunk pvid vlan** command only specifies the default VLAN of a trunk interface but does not add the trunk interface to the default VLAN. A trunk interface forwards frames with the default VLAN ID only after it is added to the default VLAN using the **port trunk allow-pass vlan** command.
- If you run the **port trunk pvid vlan** command multiple times in the same interface view, only the latest configuration takes effect.

Example

# Specify VLAN 5 as the default VLAN of GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] port link-type trunk
[HUAWEI-GigabitEthernet0/0/1] port trunk pvid vlan 5
```

5.3.39 protocol-transparent

Function

Using the **protocol-transparent** command, you can enable transparent transmission of protocol packets in a VLAN.

Using the **undo protocol-transparent** command, you can disable transparent transmission of protocol packets in a VLAN.

By default, transparent transmission of protocol packets is disabled in a VLAN.

NOTE

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

Format

protocol-transparent

undo protocol-transparent

Parameters

None

Views

VLAN view, VLAN-Range view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the device used as the gateway or Layer 2 switches is enabled with snooping functions such as DHCP/IGMP/MLD snooping, the device needs to parse and process protocol packets such as ARP, DHCP, and IGMP packets. The interface sends protocol packets without differentiating VLANs. That is, if any of the preceding snooping functions are deployed, protocol packets from all VLANs are sent to the CPU for processing.

If the device is a gateway of some VLANs or snooping functions is deployed in some VLANs, the device does not need to process protocol packets in other VLANs. After the protocol packets in other VLANs are sent to the CPU, the CPU needs to forward them to other devices. This mechanism is called software forwarding. Software forwarding affects the forwarding speed and efficiency of protocol packets because protocol packets need to be processed.

To address this issue, deploy transparent transmission of protocol packets in VLANs where protocol packets do not need to be processed. This function enables the device to transparently transmit the protocol packets in the VLANs to other devices, which improves the forwarding speed and efficiency.

The switch can transparently transmit the following protocol packets: CFM/ARP/BFD/DHCP/DHCPV6/HTTP/IGMP/MLD/ND/PIM/PIMv6/PPPoE/TACACS.

Precautions

- Before running the **protocol-transparent** command, ensure that IGMP snooping or MLD snooping has been disabled in the VLAN. Otherwise, the configuration fails.
- After the **protocol-transparent** command is executed in a VLAN view, the switch does not participate in protocol calculation in this VLAN.

Example

# Enable transparent transmission of protocol packets in VLAN 100.

```
<HUAWEI> system-view
[HUAWEI] vlan 100
[HUAWEI-vlan100] protocol-transparent
```

# Enable transparent transmission of protocol packets in VLAN 10 to 20.

```
<HUAWEI> system-view
[HUAWEI] vlan batch 10 to 20
[HUAWEI] vlan range 10 to 20
[HUAWEI-vlan-range] protocol-transparent
```

5.3.40 protocol-vlan

Function

The **protocol-vlan** command associates a protocol with a VLAN.

The **undo protocol-vlan** command disassociates a protocol from a VLAN.

Format

protocol-vlan [*protocol-index*] { **at** | **ipv4** | **ipv6** | **ipx** { **ethernetii** | **llc** | **raw** | **snap** } | **mode** { **ethernetii-etype** *etype-id1* | **llc dsap** *dsap-id* **ssap** *ssap-id* | **snap-etype** *etype-id2* } }

undo protocol-vlan { **all** | *protocol-index1* [**to** *protocol-index2*] }

Parameters

Parameter	Description	Value
protocol-index	Specifies the index of a protocol. If no protocol index is set, the switch generates an index based on the order in which protocols were associated with a VLAN.	The value is an integer that ranges from 0 to 15. The value range varies according to the device type. ● S1720GW-E,S1720GWR-E,S5720I-SI, S5720-LI, S5720S-LI, S5735S-H, S5736-S, and S6720S-S: 0 to 11 ● S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735-S-I, and S5735S-S: 0 to 7 ● other models: 0 to 15
at	Associates the AppleTalk protocol with a VLAN.	-
ipv4	Associates the IPv4 protocol with a VLAN.	-
ipv6	Associates the IPv6 protocol with a VLAN.	-
ipx	Associates the Internetwork Packet Exchange (IPX) protocol with a VLAN. The encapsulation type of IPX packets can be Ethernet II, Logical Link Control (LLC), raw, or Subnetwork Access Protocol (SNAP).	-
ethernetii	Indicates that the encapsulation format of Ethernet frames is Ethernet II.	-

Parameter	Description	Value
llc	Indicates that the encapsulation format of Ethernet frames is LLC.	-
raw	Indicates that the encapsulation format of Ethernet packets is raw.	-
snap	Indicates that the encapsulation format of Ethernet packets is SNAP.	-
mode	Indicates a user-defined protocol.	-
ethernetii-etype *etype-id1*	Specifies the protocol type ID that matches the Ethernet II encapsulation format.	The value ranges from 0x600 to ffff, excluding 800, 809b, 8137, and 86dd.
dsap *dsap-id*	Specifies the destination service access point.	The value ranges from 0x0 to ff.
ssap *ssap-id*	Specifies the source service access point.	The value ranges from 0x0 to ff.
snap-etype *etype-id2*	Specifies the protocol type ID that matches the SNAP encapsulation format.	The value ranges from 0x600 to ffff, excluding 800, 809b, 8137, and 86dd.
all	Disassociates all protocols from a VLAN.	-

Parameter	Description	Value
protocol-index1	Specifies the start protocol index.	The value is an integer that ranges from 0 to 15. The value range varies according to the device type. ● S1720GW-E,S1720GWR-E,S5720I-SI, S5720-LI, S5720S-LI, S5735S-H, S5736-S, and S6720S-S: 0 to 11 ● S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735-S-I, and S5735S-S: 0 to 7 ● other models: 0 to 15
protocol-index2	Specifies the end protocol index.	The value of *protocol-index2* must be greater than or equal to the value of *protocol-index1*.

Views

VLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Protocol-based VLAN assignment is a method to associate protocols with VLANs. After a protocol is associated with a VLAN, packets of this protocol are transmitted in the associated VLAN. This function allows different protocol packets to be transmitted on different paths.

Follow-up Procedure

Add interfaces to the VLAN associated with protocols, and then associate the interfaces with the VLAN.

Precautions

The control VLAN of an RRPPor ERPS ring cannot be associated with protocols.

The AppleTalk, IPv4, and IPv6 protocols can be associated with VLANs directly. When associating other protocols with a VLAN, set the encapsulation format.

When specifying the source and destination service access points, pay attention to the following points:

- The *dsap-id* and *ssap-id* parameters cannot be set to 0xaa (indicating the SNAP encapsulation format) simultaneously.
- The *dsap-id* and *ssap-id* parameters cannot be set to 0xe0 (indicating the LLC encapsulation format) simultaneously.
- The *dsap-id* and *ssap-id* parameters cannot be set to 0xff (indicating the raw encapsulation format) simultaneously.

If you run the **protocol-vlan** command multiple times in the same VLAN view, all the specified protocols are associated with the VLAN.

Example

# Associate IPv4 with VLAN 3.

```
<HUAWEI> system-view
[HUAWEI] vlan 3
[HUAWEI-vlan3] protocol-vlan ipv4
```

5.3.41 protocol-vlan vlan

Function

The **protocol-vlan vlan** command associates an interface with a protocol-based VLAN.

The **undo protocol-vlan vlan** command disassociates an interface from a VLAN.

By default, an interface is not associated with any protocol-based VLAN.

Format

protocol-vlan vlan *vlan-id* { **all** | *protocol-index1* [**to** *protocol-index2*] } [**priority** *priority*]

undo protocol-vlan { **all** | **vlan** *vlan-id* { **all** | *protocol-index1* [**to** *protocol-index2*] } }

Parameters

Parameter	Description	Value
all	The **all** keywords in the command have different meanings: ● The one followed by *protocol-index1* indicates all protocols. ● The one followed by **vlan** indicates all protocol-based VLANs.	-
vlan *vlan-id*	Specifies the ID of a protocol-based VLAN.	The value is an integer that ranges from 1 to 4094.
protocol-index1 [**to** *protocol-index2*]	Specifies the start protocol index. If no protocol index is set, the switch generates an index based on the order in which protocols were associated with a VLAN.	The value is an integer that ranges from 0 to 15. The value range varies according to the device type. ● S1720GW-E,S1720GWR-E,S5720I-SI, S5720-LI, S5720S-LI, S5735S-H, S5736-S, and S6720S-S: 0 to 11 ● S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735-S-I, and S5735S-S: 0 to 7 ● other models: 0 to 15
priority *priority*	Specifies the 802.1p priority of a VLAN.	The value is an integer that ranges from 0 to 7. A larger value indicates a higher priority. The default value is 0.

Views

Ethernet interface view, GE interface view, XGE interface view, 40GE interface view, 100GE interface view, MultiGE interface view, Eth-Trunk interface view, port group view, 25GE interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Protocol-based VLAN assignment is a method to associate protocols with VLANs. After a protocol is associated with a VLAN, packets of this protocol are transmitted in the associated VLAN. This function allows different protocol packets to be transmitted on different paths.

After an interface is associated with a protocol-based VLAN:

- When receiving an untagged packet, the interface searches for the VLAN entry matching the protocol type of the packet. If a matching entry is found, the interface forwards the packet based on the matching VLAN ID and priority. If no matching entry is found, the interface uses other matching rules to forward the packet.
- When receiving a tagged packet, the interface forwards the packet based on the port-based VLAN configuration.

Prerequisites

The VLAN has been associated with a protocol using the **protocol-vlan** command.

Precautions

On access and trunk interfaces, protocol-based VLAN assignment can be used only when the protocol-based VLAN is the same as the PVID. It is recommended that protocol-based VLAN assignment be configured on hybrid interfaces.

After an interface is associated with a protocol-based VLAN, the switch checks the protocol type of a received packet and forwards the packet in the VLAN associated with the protocol.

Example

# Associate GE0/0/1 with VLAN 2, which is associated with the protocol with index 0.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] port link-type hybrid
[HUAWEI-GigabitEthernet0/0/1] protocol-vlan vlan 2 0
```

5.3.42 reset lnp statistics

Function

The **reset lnp statistics** command clears statistics on LNP packets.

Format

reset lnp statistics [**interface** *interface-type interface-number*]

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Clears statistics on LNP packets on a specified interface.	-

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To collect statistics about LNP packets for a specified period of time, run the **reset lnp statistics** command to clear existing statistics and allow the system to re-collect them.

Configuration Note

Cleared statistics on LNP packets cannot be restored. Exercise caution when running this command.

Example

# Clear statistics about LNP packets.

```
<HUAWEI> reset lnp statistics interface gigabitethernet 0/0/1
```

5.3.43 reset vlan statistics

Function

Using the **reset vlan statistics** command, you can clear traffic statistics in a specified VLAN.

Format

reset vlan *vlan-id* **statistics**

Parameters

Parameter	Description	Value
vlan-id	Specifies the ID of a VLAN.	The value is an integer that ranges from 1 to 4094.

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

This command is used when you need to collect new packet statistics in a VLAN. After this command is executed, the packet count in the VLAN becomes 0.

Prerequisites

The traffic statistics function has been enabled in the VLAN by using the **statistic enable (VLAN view)** command.

Precautions

⚠ CAUTION

Traffic statistics cannot be restored after they are cleared. Exercise caution when you use the command.

Example

# Clear traffic statistics in VLAN 3.

```
<HUAWEI> reset vlan 3 statistics
```

5.3.44 shutdown (VLANIF interface view)

Function

Using the **shutdown** command, you can shut down a VLANIF interface.

Using the **undo shutdown** command, you can enable a VLANIF interface.

By default, a VLANIF interface is enabled.

Format

shutdown

undo shutdown

Parameters

None

Views

VLANIF interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When a VLANIF interface fails or is not needed, you can run the **shutdown** command on the VLANIF interface.

Precautions

A VLANIF interface is Up as long as an interface in the corresponding VLAN is Up.

After the VLANIF interface is shut down, the interface status changes to Down even if physical interfaces in the corresponding VLAN are Up.

After a VLANIF interface is shut down, none of the users who use the VLANIF interface address as the gateway address can communicate at Layer 3. In addition, the VLANIF interface address cannot be used in route calculation.

After a VLANIF interface is shut down, the dynamic ARP entry corresponding to the VLANIF interface starts aging in the ARP table. If the VLANIF interface address is in a static ARP entry, the ARP entry is not deleted.

Example

# Enable VLANIF 2.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 2
[HUAWEI-Vlanif2] undo shutdown
```

5.3.45 statistic enable (VLAN view)

Function

The **statistic enable** command enables the traffic statistics function in a VLAN.

The **undo statistic enable** command disables the traffic statistics function in a VLAN.

By default, the traffic statistics function is disabled in a VLAN.

Format

statistic enable

undo statistic enable

Parameters

None

Views

VLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To check the network status or locate network faults, you can use the **statistic enable** command to enable the traffic statistics function in a VLAN.

After the traffic statistics function is enabled in a VLAN, the device collects statistics on unicast packets, broadcast packets, and broadcast packets transmitted in the VLAN.

Precautions

- On different models, the number of VLANs where the traffic statistics function can be configured is different:
  - S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S: 256
  - S5720I-SI, S5735-S, S5735S-S, S5735-S-I, S5735S-H, S5736-S, and S6720S-S: 64
  - Other models: 16
- Traffic statistics are accumulative and cannot be cleared by the system. To clear traffic statistics in a VLAN, run the **reset vlan statistics** command in the VLAN.
- The traffic statistics function occupies system resources. If system resources are insufficient, the configuration may fail. Disable this function when traffic statistics do not need to be collected.
- After enabling the traffic statistics function in a VLAN, you can use the **display vlan** *vlan-id* **statistics** command to view traffic statistics in the VLAN.
- On the SS1720GW-E, S1720GWR-E, S5720I-SI, S5720-LI, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5720S-LI, S5735-S, S500, S5735S-S, S5735-S-I, S5735S-H, S5736-S, and S6720S-S if the traffic policy is bound to the traffic behavior containing traffic statistics and is applied to an interface in the inbound direction, and the **statistic enable** command is enabled in the VLAN that the interface joins, the **statistic enable** command cannot collect statistics on packets in the inbound direction of the interface.
- For the S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S, configuring traffic statistics collection on VLANs and VLANIF interfaces may affect forwarding performance. For example, some packets may be discarded during line-rate forwarding on all ports. Configure this function if necessary.

Example

# Enable the traffic statistics function in VLAN 100.

```
<HUAWEI> system-view
[HUAWEI] vlan 100
[HUAWEI-vlan100] statistic enable
```

5.3.46 statistic enable (VLANIF interface view)

Function

The **statistic enable** command enables the traffic statistics function on a VLANIF interface.

The **undo statistic enable** command disables the traffic statistics function on a VLANIF interface.

By default, the traffic statistics function is disabled on a VLANIF interface.

NOTE

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

Format

[**ipv4** | **ipv6**] * **statistic enable** { **both** | **inbound** | **outbound** }

undo [**ipv4** | **ipv6**] * **statistic enable** { **both** | **inbound** | **outbound** }

Parameters

Parameter	Description	Value
ipv4	Indicates IPv4 packet statistics collection.	-
ipv6	Indicates IPv6 packet statistics collection.	-
both	Enables the traffic statistics function for incoming and outgoing traffic.	-
inbound	Enables the traffic statistics function for incoming traffic.	-
outbound	Enables the traffic statistics function for outgoing traffic.	-

Views

VLANIF interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To check the network status or locate network faults, you can use the **statistic enable** command to enable the traffic statistics function on VLANIF interfaces. The switch then collects traffic statistics on the VLANIF interfaces.

Precautions

- On the S6735-S, S6720S-EI and S6720-EI, if the traffic statistics function is enabled in the VLAN corresponding to the VLANIF interface, the traffic statistics function is invalid on the VLANIF interface in the **outbound** direction.
- After you run the **undo statistic enable** command on a VLANIF interface, the switch stops collecting traffic statistics on the VLANIF interface, and the collected traffic statistics are deleted.
- The switch uses ACL resources when collecting traffic statistics. If the traffic statistics function is enabled on too many VLANIF interfaces, other services may fail to obtain ACL resources. The device supports traffic statistics on a maximum of 100 VLANIF interface.
- Traffic statistics on VLANIF interfaces is unavailable for error packets.
- On the VLANIF interface enabled with the traffic statistics function, the packets such as ping packets sent from the device cannot be counted.
- After enabling the traffic statistics function in a VLANIF, you can use the **display interface vlanif** command to view traffic statistics in the VLANIF.
- The traffic statistics function on VLANIF interfaces is unavailable for MPLS packets.
- A higher number of VLANIF interfaces configured with the traffic statistics function leads to higher CPU usage.
- For the S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S, configuring traffic statistics collection on VLANs and VLANIF interfaces may affect forwarding performance. For example, some packets may be discarded during line-rate forwarding on all ports. Configure this function if necessary.

Example

# Enable the traffic statistics function for incoming and outgoing traffic on the VLANIF interface.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] statistic enable both
```

5.3.47 trace mac

Function

The **trace mac** command locates a link connectivity fault between the local device and the destination device. The operation is called GMAC trace.

Format

trace mac *mac-address* **vlan** *vlan-id* [**interface** *interface-type interface-number* | **-t** *timeout* | **-h**]*

Parameters

Parameter	Description	Value
mac-address	Specifies the MAC address of the destination node. The destination node can be a MEP or a MIP. An MP's MAC address can be a bridge MAC address or the MAC address of the interface where the MP is configured. The MAC address depends on the configured MP address model: ● If the shared MP address model is configured, an MP uses a bridge MAC address as its own MAC address. ● If the independent MP address model is configured, an MP uses the MAC address of the interface where the MP is configured.	The value is in H-H-H format. An H is a hexadecimal number of 1 to 4 digits. The value cannot be a broadcast or multicast MAC address.
vlan *vlan-id*	Specifies the ID of a VLAN.	The value is an integer that ranges from 1 to 4094.

Parameter	Description	Value
interface *interface-type interface-number*	Specifies the outbound interface on the local device for sending trace packets. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number. ● If this parameter is specified, the device sends trace packets directly through the interface. ● If this parameter is not specified, the device searches the MAC address table based on the specified destination MAC address and VLAN ID. If the forwarding entry is found, the device sends trace packets according to the entry. If the forwarding entry is not found but there is one interface in the VLAN, the device sends trace packets from this interface. If there is more than one interface in the VLAN, the device discards trace packets directly.	-
-t *timeout*	Specifies the timeout interval for waiting for an LTR.	The value is an integer that ranges from 1 to 65535, in milliseconds. The default value is 2000 ms.
-h	Specifies the host name and IP address of a device that an LTM passes through.	-

Views

All views

Default Level

0: Visit level

Usage Guidelines

Usage Scenario

To perform GMAC trace, run this command.

Prerequisites

GMAC trace has been enabled using the **trace mac enable** command.

Precautions

A MEP is not required to initiate GMAC trace. The destination node can be not a MEP or MIP. That is, GMAC trace can be implemented without configuring the MD, MA, or MEP on the source device, intermediate device, and the destination device. All the intermediate devices can respond with an LTR.

NOTE

The two devices must be configured with IEEE 802.1ag of the same version. If the local device is configured with IEEE 802.1ag Draft 7 and the peer device is configured with IEEE Standard 802.1ag-2007, the **trace mac** command does not take effect. That is, the connectivity fault cannot be located.

-h is only supported by the device running IEEE Standard 802.1ag-2007.

Example

# Trace the destination device with the MAC address as 00e0-fc12-3456. The device belongs to VLAN 2.

```
<HUAWEI> system-view
[HUAWEI] trace mac enable
[HUAWEI] trace mac 00e0-fc12-3456 vlan 2
Tracing the route to 00e0-fc12-3456 over a maximum of 255 hops:
 Hops  Ingress MAC     Ingress Port              Ingress Action    Relay Action
       Egress MAC      Egress Port               Egress Action
 1     00e0-fc12-3456 GigabitEthernet0/0/1       IngOK             RlyHit
       --              --                        --
Info: Succeed in tracing the destination address 00e0-fc12-3456.
```

# Trace the destination device with the MAC address as 00e0-fc12-3455. The device belongs to VLAN 2.

```
<HUAWEI> system-view
[HUAWEI] trace mac enable
[HUAWEI] trace mac 00e0-fc12-3455 vlan 2 -h
Tracing the route to 00e0-fc12-3455 over a maximum of 255 hops:
 Hops  Host Name (IP Address)
       Ingress MAC     Ingress Port              Ingress Action    Relay Action
       Egress MAC      Egress Port               Egress Action
 1     173 (10.10.10.173)
       00e0-fc12-3455 GigabitEthernet0/0/1       IngOK             RlyHit
       --              --                        --
Info: Succeed in tracing the destination address 00e0-fc12-3455.
```

Table 5-47 Description of the trace mac command output

Item	Description
Hops	Number of hops.
Ingress Action	Action taken by the inbound interface to process LTMs: ● IngOK: The inbound interface forwards LTMs successfully. ● If this field is empty, the inbound interface fails to forward LTMs.

Item	Description
Relay Action	Action taken by the device to process LTMs: ● RlyFDB: The device forwards LTMs to the next hop device. ● RlyHit: The device forwards LTMs to the destination device.
Egress Action	Action taken by the outbound interface to process trace packets: ● EgrOK: The outbound interface forwards LTMs successfully. ● If this field is empty, the outbound interface does not or fails to forward LTMs.

5.3.48 trace mac enable

Function

The **trace mac enable** command enables GMAC trace.

The **undo trace mac enable** command disables GMAC trace.

By default, GMAC trace is disabled (except the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S).

Format

trace mac enable

undo trace mac enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To implement the following functions, use the **trace mac enable** command:

- Implement GMAC trace.
- Enable the device to respond to LTMs of MAC trace.

Example

# Enable GMAC trace.

```
<HUAWEI> system-view
[HUAWEI] trace mac enable
```

5.3.49 unknown-flow drop

Function

The **unknown-flow drop** command configures unknown packet isolation in a VLAN.

The **undo unknown-flow drop** command cancels unknown packet isolation in a VLAN.

By default, unknown packet isolation is not configured in a VLAN.

NOTE

This function is supported only on the following models: S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S.

Format

unknown-flow drop

undo unknown-flow drop

Parameters

None

Views

VLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To isolate unknown packets in a VLAN, run the **unknown-flow drop** command. This function applies to large- and medium-sized campus networks where aggregation and access switches go online through Option 148.

Example

# Configure unknown packet isolation in VLAN 100.

```
<HUAWEI> system-view
[HUAWEI] vlan 100
[HUAWEI-vlan100] unknown-flow drop
```

5.3.50 vlan

Function

The **vlan** command creates a VLAN and displays the VLAN view. If the VLAN exists, the VLAN view is displayed.

The **undo vlan** command deletes a VLAN.

By default, all interfaces belong to the default VLAN, named VLAN 1.

Format

vlan *vlan-id*

vlan batch { *vlan-id1* [**to** *vlan-id2*] } &<1-10>

undo vlan *vlan-id*

undo vlan batch { *vlan-id1* [**to** *vlan-id2*] } &<1-10>

Parameters

Parameter	Description	Value
vlan-id	Specifies the VLAN ID.	The value is an integer ranging from 1 to 4094.
batch	Configures VLANs in batches.	-
vlan-id1 **to** *vlan-id2*	Specifies range of VLANs to be configured in batches: ● *vlan-id1* specifies the start VLAN ID. ● *vlan-id2* specifies the end VLAN ID. *vlan-id2* must be greater than or equal to *vlan-id1*. *vlan-id1* and *vlan-id2* define a range together. ● If the parameter **to** *vlan-id2* is not specified, only the VLAN specified by *vlan-id1* is created.	The *vlan-id1* and *vlan-id2* are integers ranging from 1 to 4094.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To reduce broadcast domains and enhance security on a complex network, VLANs can be created on the network to isolate the hosts that do not need to communicate with each other. The **vlan batch** command creates multiple VLANs at one time, simplifying VLAN configuration.

Follow-up Procedure

Assign VLANs according to network requirements.

Precautions

- VLAN 1 is the default VLAN, which cannot be deleted and does not need to be created.
- The **vlan** command can be used to create a VLAN and enter the VLAN view. If a VLAN has been created, the VLAN view is displayed after this command is used. You can repeat the **vlan** command for multiple times. If a VLAN has been created, this command cannot be used to create the same VLAN or modify the configurations of the VLAN.
- The **vlan batch** command can be used to create multiple VLANs in batches. If a VLAN has been created, this command cannot be used to create the same VLAN or modify the configurations of the VLAN. If you run the **vlan batch** command multiple times, all the specified VLANs are created.
- The allowed VLANs on a sub-interface cannot be created in the system view or be displayed by the display command.

Example

# Create VLAN 100 and enter the VLAN 100 view. If VLAN 100 exists, the VLAN 100 view is displayed directly.

```
<HUAWEI> system-view
[HUAWEI] vlan 100
[HUAWEI-vlan100]
```

5.3.51 vlan configuration

Function

The **vlan configuration** command creates and enters the configuration view of a VLAN. When the VLAN is not created, this command does not create the VLAN.

The **undo vlan** *vlan-id* **configuration** command deletes the configuration view of a VLAN.

By default, no VLAN configuration view is created.

Format

vlan *vlan-id* **configuration**

undo vlan *vlan-id* **configuration**

Parameters

Parameter	Description	Value
vlan-id	Specifies the VLAN ID.	The value is an integer ranging from 1 to 4094.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

This command applies to the following scenarios:

- If you need to perform configurations in a VLAN without creating the VLAN on VCMP clients, create the VLAN on the VCMP server and run the **vlan configuration** command on VCMP clients to enter the VLAN configuration view.
- After a VLAN is deleted on the VCMP server, VCMP clients delete the local VLAN but do not delete configurations in the VLAN. To delete or modify configurations in a VLAN without creating the VLAN, run the **vlan configuration** command to enter the VLAN configuration view to delete or modify configurations.

The **vlan** *vlan-id* **configuration** command completes the VLAN configuration when the VLAN is not created.

Precautions

The **vlan configuration** command only enters the VLAN configuration view. Neither the corresponding VLAN or configurations in the VLAN take effect. To make configurations in the VLAN take effect, create the VLAN using the **vlan** command.

The **vlan** *vlan-id* **configuration** command configuration is displayed in the following situations:

- The **vlan** *vlan-id* **configuration** command displays the VLAN view and services are configured in the VLAN.
- The VLAN is deleted using VCMP.

Example

# Enter the configuration view of VLAN 10.

```
<HUAWEI> system-view
[HUAWEI] vlan 10 configuration
[HUAWEI-vlan10]
```

5.3.52 vlan precedence

Function

The **vlan precedence** command configures the device to preferentially use a VLAN assignment mode when both MAC address-based and IP subnet-based VLAN assignment modes are matched.

The **undo vlan precedence** command restores the default VLAN assignment mode on an interface when both MAC address-based and IP subnet-based VLAN assignment modes are matched.

By default, MAC address-based VLAN assignment takes precedence over IP subnet-based VLAN assignment.

NOTE

Only the S5720I-SI, S5735-S, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S6735-S, S6720-EI, S6720S-EI, and S6720S-S support this command.

Format

vlan precedence { **ip-subnet-vlan** | **mac-vlan** }

undo vlan precedence

Parameters

Parameter	Description	Value
ip-subnet-vlan	Indicates that IP subnet-based VLAN assignment takes precedence over MAC address-based VLAN assignment.	-
mac-vlan	Indicates that MAC address-based VLAN assignment takes precedence over IP subnet-based VLAN assignment.	-

Views

system view, Ethernet interface view, GE interface view, XGE interface view, 40GE interface view, Eth-Trunk interface view, MultiGE interface view, port group view

NOTE

S5720I-SI, S5735-S, S5735S-S, S5735-S-I, S5735S-H, S5736-S, and S6720S-S support the **vlan precedence** command only in the system view. Other switches support the **vlan precedence** command only in the interface view.

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can configure all the VLAN assignment methods simultaneously on the switch. By default, the priority order of VLAN assignment methods is: policy-based VLAN > MAC address-based > IP subnet-based > protocol-based > port-based.

The **vlan precedence** command changes the priority order of MAC address-based VLAN assignment and IP subnet-based VLAN assignment. For example, the **vlan precedence ip-subnet-vlan** command makes IP subnet-based VLAN assignment take precedence over MAC address-based VLAN assignment.

Currently, port-based VLAN assignment is used most widely.

Precautions

This command does not change the priority order of the other VLAN assignment methods.

Packets may be transmitted in a different VLAN after the priority order of MAC address-based VLAN assignment and IP subnet-based VLAN assignment changes. This may cause a traffic forwarding failure in the VLAN.

When the command is used on the S5720I-SI, S5735-S, S5735S-S, S5735-S-I, S5735S-H, S5736-S, and S6720S-S to adjust the priority, the command is valid for MAC-VLAN entries with the mask and without the mask. The command is valid for only MAC-VLAN entries without the mask on other models.

If you run the **vlan precedence** command multiple times in the same interface view, only the latest configuration takes effect.

Example

# Specify that IP subnet-based VLAN assignment takes precedence over MAC address-based VLAN assignment.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] vlan precedence ip-subnet-vlan
```

5.3.53 vlan range

Function

The **vlan range** command creates a temporary VLAN range and displays the VLAN-Range view.

By default, no temporary VLAN ranges are created.

NOTE

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

Format

vlan range { *vlan-id1* [**to** *vlan-id2*] } &<1-10>

Parameters

Parameter	Description	Value
vlan-id1 [**to** *vlan-id2*]	Specifies VLAN IDs to be created in batches: ● *vlan-id1* specifies the start VLAN ID. ● *vlan-id2* specifies the end VLAN ID. *vlan-id2* must be greater than or equal to *vlan-id1*. *vlan-id1* and **to** *vlan-id2* specify a VLAN range. ● If **to** *vlan-id2* is not specified, only the VLAN specified by *vlan-id1* is configured.	The value is an integer ranging from 1 to 4094.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Manually configuring and maintaining VLANs is challenging on a large Layer 2 network. Configuration inconsistency may also occur. To improve maintenance efficiency and simplify configurations, run the **vlan range** command to create a temporary VLAN range. You can then configure services in the VLAN-Range view. Configured services will be delivered in batches to all the VLANs in the VLAN range.

Precautions

The **vlan range** command configuration is not saved in the configuration file. If services are configured in the VLAN-Range view, the service configurations of all the VLANs in the VLAN range will be saved in the configuration file.

A temporary VLAN range fails to be created if the specified VLAN is a dynamic VLAN or is not created. VLANs that have been added to a temporary VLAN range will automatically leave the VLAN range after being deleted.

Configuration Impact

If the **vlan range** command is run more than once, all configurations take effect.

Example

# Create a VLAN range 10 to 20 and enter the VLAN-Range view.

```
<HUAWEI> system-view
[HUAWEI] vlan batch 10 to 20
[HUAWEI] vlan range 10 to 20
[HUAWEI-vlan-range]
```

5.3.54 vlan statistics

Function

The **vlan statistics** command configures the way to collect VLAN traffic statistics.

The **undo vlan statistics** command restores the default way to collect VLAN traffic statistics.

By default, VLAN traffic statistics are collected by packets.

Format

vlan statistics { **by-bytes** | **by-packets** }

undo vlan statistics { **by-bytes** | **by-packets** }

NOTE

Only the SS1720GW-E, S1720GWR-E, S5720I-SI, S5720-LI, S5720S-LI, S5735S-H, S5736-S, and S6720S-S support this command.

Parameters

Parameter	Description	Value
by-bytes	Collects VLAN traffic statistics by bytes.	-
by-packets	Collects VLAN traffic statistics by packets.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To check the network status or locate network faults, you can use the **statistic enable (VLAN view)** command to enable traffic statistics collection in VLANs.

After traffic statistics collection is enabled in a VLAN, the switch collects statistics on unicast packets, broadcast packets, and broadcast packets transmitted in the VLAN.

The **vlan statistics** { **by-bytes** | **by-packets** } command configures whether traffic statistics are collected by packet s or bytes.

Example

# Configure the system to collect VLAN traffic statistics by bytes.

```
<HUAWEI> system-view
[HUAWEI] vlan statistics by-bytes
```

5.3.55 vlan statistics interval

Function

The **vlan statistics interval** command sets the interval for collecting VLAN traffic statistics.

The **undo vlan statistics interval** command restores the default interval for collecting VLAN traffic statistics.

By default, VLAN traffic statistics are collected at an interval of 300 seconds.

Format

vlan statistics interval *interval-time*

undo vlan statistics interval

Parameters

Parameter	Description	Value
interval-time	Specifies the interval for collecting VLAN traffic statistics.	The value is an integer that ranges from 60 to 600, in seconds.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To check the network status or locate network faults, you can use the **statistic enable (VLAN view)** command to enable traffic statistics collection in VLANs.

After traffic statistics collection is enabled in a VLAN, the switch collects statistics on unicast packets, broadcast packets, and broadcast packets transmitted in the VLAN.

You can use the **vlan statistics interval** command to specify the interval at which traffic statistics are collected.

Example

# Set the interval for collecting VLAN traffic statistics to 500 seconds.

```
<HUAWEI> system-view
[HUAWEI] vlan statistics interval 500
```

5.3.56 vlan vlan-name

Function

The **vlan vlan-name** command displays the view of a VLAN with the specified VLAN name.

The **undo vlan vlan-name** command deletes a VLAN with the specified VLAN name. After the command is used, the VLAN name is also deleted.

Format

vlan vlan-name *vlan-name*

undo vlan vlan-name *vlan-name*

Parameters

Parameter	Description	Value
vlan-name	Specifies the VLAN name.	The name is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the **name** command is run to set a VLAN name, you can run the **vlan vlan-name** command in the system view to enter the corresponding VLAN view.

Assume that a device has multiple VLANs and each VLAN has a name. If you need to delete the VLAN that is used to transmit voice services but cannot remember the ID of the VLAN, you can run the **undo vlan vlan-name** command to delete the VLAN by inputting the VLAN name.

Prerequisites

Before running the **vlan vlan-name** command, ensure that the **name** command is run to set the VLAN name.

Precautions

When you run the **undo vlan vlan-name** command to delete a VLAN, services configured for the VLAN are deleted at the same time. The deleted services cannot be restored even if you recreate the VLAN. Therefore, exercise caution when running the **undo vlan vlan-name** command.

Example

# Enter the view of the VLAN named **user1**.

```
<HUAWEI> system-view
[HUAWEI] vlan vlan-name user1
[HUAWEI-vlan2]
```

5.4 VLAN Aggregation Configuration Commands

5.4.1 Command Support

Only the following switch models support VLAN aggregation:

S5720I-SI, S5735S-H, S5736-S, S5731-H, S5731-S, S5731S-S, S5731S-H, S5732-H, S5735-S, S5735S-S, S5735-S-I, S6720S-S, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S

5.4.2 access-vlan

Function

The **access-vlan** command adds one or more sub-VLANs to a super-VLAN.

The **undo access-vlan** command removes one or more sub-VLANs from a super-VLAN.

By default, no sub-VLAN is added to the super-VLAN.

Format

access-vlan { *vlan-id1* [**to** *vlan-id2*] } &<1-10>

undo access-vlan { *vlan-id1* [**to** *vlan-id2*] } &<1-10>

Parameters

Parameter	Description	Value
vlan-id1 [**to** *vlan-id2*]	Specifies a range of sub-VLAN IDs. ● *vlan-id1* specifies the start VLAN ID. ● **to** *vlan-id2* specifies the end VLAN ID. The value of *vlan-id2* must be greater than or equal to the value of *vlan-id1*. If **to** *vlan-id2* is not specified, only one VLAN is added to the super-VLAN. You can specify a maximum of 10 VLAN ID ranges at a time. The ranges cannot overlap.	● The value of *vlan-id1* is an integer that ranges from 1 to 4094. ● The value of *vlan-id2* is an integer that ranges from 1 to 4094.

Views

VLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The VLAN technology is widely applied to packet switching networks because it controls broadcast domains flexibly and is easy to deploy. Generally, a Layer 3 switch usually uses a Layer 3 logical interface in each VLAN to allow user hosts in different broadcast domains to communicate. This wastes IP addresses. The VLAN aggregation function is introduced to save IP addresses while implementing communication between VLANs.

The VLAN aggregation function associates a super-VLAN with multiple sub-VLANs. A VLANIF interface can be created in the super-VLAN and be configured with an IP address. Interfaces in all the sub-VLANs use this IP address as the gateway address to communicate with interfaces in other VLANs. This reduces subnet IDs, subnet default gateway addresses, and subnet broadcast IP addresses. In a word, the VLAN aggregation function allows different broadcast domains to use the same subnet address, implements flexible addressing, and saves IP addresses.

Prerequisites

The super-VLAN has been configured using the **aggregate vlan** command.

Before running the **access-vlan** command, delete VLANIF interfaces from all the sub-VLANs.

Follow-up Procedure

Configure the sub-VLANs to implement Layer 2 communication between them.

Precautions

The super-VLAN must be different from all its sub-VLANs.

A VLAN can be added to only one super-VLAN.

If you run the **access-vlan** command multiple times in the same VLAN view, all the specified VLANs are added to the super-VLAN.

Example

# Add sub-VLAN20 and sub-VLAN30 to super-VLAN2.

```
<HUAWEI> system-view
[HUAWEI] vlan 2
[HUAWEI-vlan2] aggregate-vlan
[HUAWEI-vlan2] access-vlan 20 30
```

5.4.3 aggregate-vlan

Function

The **aggregate-vlan** command configures a VLAN as a super-VLAN.

The **undo aggregate-vlan** command cancels the configuration.

By default, no VLAN is configured as a super-VLAN.

Format

aggregate-vlan

undo aggregate-vlan

Parameters

None

Views

VLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The VLAN technology is widely applied to packet switching networks because it controls broadcast domains flexibly and is easy to deploy. Generally, a Layer 3 switch usually uses a Layer 3 logical interface in each VLAN to allow user hosts in different broadcast domains to communicate. This wastes IP addresses. The VLAN aggregation function is introduced to save IP addresses while implementing communication between VLANs.

The VLAN aggregation function associates a super-VLAN with multiple sub-VLANs. A VLANIF interface can be created in the super-VLAN and be configured with an IP address. Interfaces in all the sub-VLANs use this IP address as the gateway address to communicate with interfaces in other VLANs. This reduces subnet IDs, subnet default gateway addresses, and subnet broadcast IP addresses. In a word, the VLAN aggregation function allows different broadcast domains to use the same subnet address, implements flexible addressing, and saves IP addresses.

Prerequisites

Before configuring a VLAN as a super-VLAN, delete all physical interfaces from the VLAN.

Precautions

VLAN 1 cannot be configured as a super-VLAN.

If a VLAN has been configured as a guest VLAN, it cannot be configured as a super-VLAN.

If a VLAN or the VLAN pool to which a VLAN belongs has been configured as a service VLAN for the WLAN network, the VLAN cannot be configured as a super-VLAN. Similarly, if a VLAN has been configured as a super-VLAN, the VLAN or the VLAN pool to which the VLAN belongs cannot be configured as a service VLAN for the WLAN network. In addition, if a VLAN pool has been configured as a service VLAN for a WLAN network, a super-VLAN cannot be added to the VLAN pool.

The super-VLAN must be different from all its sub-VLANs.

After a VLAN is configured as a super-VLAN, no physical interface can be added to the VLAN.

If too many sub-VLANs are added to the super-VLAN, the ARP broadcast storm degrades the system performance and affects the ARP learning.For S6730-H, S6730-S, S6730S-H, S6730S-S, S5731-H, S5731-S, S5731S-H, S5731S-S, and S5732-H, the number of sub-VLANs that are added to a super-VLAN cannot exceed 24. For other models, the number cannot exceed 16.

Example

# Configure VLAN 2 as a Super-VLAN.

```
<HUAWEI> system-view
[HUAWEI] vlan 2
[HUAWEI-vlan2] aggregate-vlan
```

5.4.4 display sub-vlan

Function

The **display sub-vlan** command displays information about sub-VLAN entries.

Format

display sub-vlan [*vlan-id*]

Parameters

Parameter	Description	Value
vlan-id	Specifies the VLAN ID of a sub-VLAN. When multiple VLANs are configured on a device, you are recommended to specify the VLAN ID so that you can view information about a specific sub-VLAN.	The value is an integer ranging from 1 to 4094.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After VLAN aggregation is configured on a device, you can determine whether VLAN aggregation has been correctly configured by running the **display sub-vlan** command to check information about sub-VLANs and check which sub-VLANs are contained in a super-VLAN.

When using the **display sub-vlan** command, note the following issues:

- If *vlan-id* is not specified, information about all sub-VLANs on the device is displayed.
- If *vlan-id* is specified, information about a specific sub-VLAN is displayed.

Before running the **display sub-vlan** command, ensure that the device is configured with sub-VLANs. Otherwise, no command output is displayed.

Example

# Display information about all sub-VLANs.

```
<HUAWEI> display sub-vlan
```

```
VLAN ID   Super-VLAN
------------------------
10        40
20        40
30        40
```

Table 5-48 Description of the **display sub-vlan** command output

Item	Description
VLAN ID	Existing sub-VLAN on the device. To specify the parameter, run the **access-vlan** command.
Super-VLAN	Super-VLAN that the sub-VLAN belongs to. To specify the parameter, run the **aggregate-vlan** command.

5.4.5 display super-vlan

Function

The **display super-vlan** command displays information about super-VLAN entries.

Format

display super-vlan [*vlan-id*]

Parameters

Parameter	Description	Value
vlan-id	Specifies the VLAN ID of a super-VLAN. When multiple VLANs are configured on a device, you are recommended to specify the VLAN ID so that you can view information about a specific super-VLAN.	The value is an integer ranging from 1 to 4094.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After VLAN aggregation is configured on a device, you can determine whether VLAN aggregation has been correctly configured by running the **display super-vlan** command to check information about super-VLANs and check which sub-VLANs are contained in a super-VLAN.

When using the **display super-vlan** command, note the following issues:

- If *vlan-id* is not specified, information about all super-VLANs on the device is displayed.
- If *vlan-id* is specified, information about a specific super-VLAN is displayed.

Before running the **display super-vlan** command, ensure that the device is configured with super-VLANs. Otherwise, no command output is displayed.

Example

# Display information about all super-VLANs.

```
<HUAWEI> display super-vlan
VLAN ID   Sub-VLAN
------------------------
40        10 20 30
```

Table 5-49 Description of the **display super-vlan** command output

Item	Description
VLAN ID	Existing super-VLAN on the device. To specify the parameter, run the **aggregate-vlan** command.
Sub-VLAN	Sub-VLAN in the super-VLAN. To specify the parameter, run the **access-vlan** command.

5.5 MUX VLAN Configuration Commands

5.5.1 Command Support

Commands provided in this section and all the parameters in the commands are supported by all switch models (except the S5731-L and S5731S-L), unless otherwise specified. For details, see specific commands.

5.5.2 display mux-vlan

Function

Using the **display mux-vlan** command, you can view the MUX VLAN configuration.

Format

display mux-vlan

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

After configuring the MUX VLAN function, you can use the **display mux-vlan** command to verify the configuration. This command displays the principal VLAN ID, subordinate VLAN ID, VLAN type, and interfaces in each VLAN.

Precautions

If no MUX VLAN is configured by using the **mux-vlan** command, the **display mux-vlan** command does not display any information.

Example

# Display the MUX VLAN configuration.

```
<HUAWEI> display mux-vlan
Principal Subordinate Type      Interface
------------------------------------------------------------------------------
100       -          principal
100       120        separate    GigabitEthernet0/0/1
100       130        group       GigabitEthernet0/0/2
100       140        group       GigabitEthernet0/0/3
------------------------------------------------------------------------------
```

Table 5-50 Description of the display mux-vlan command output

Item	Description
Principal	ID of a principal VLAN. To specify the parameter, run the **mux-vlan** command.
Subordinate	ID of a subordinate VLAN To specify the parameter, run the **subordinate group**, or **subordinate separate** command.
Type	Type of a VLAN. ● principal: indicates a principal VLAN, configured by the **mux-vlan** command. ● group: indicates a subordinate group VLAN, configured by the **subordinate group** command. ● separate: indicates a subordinate separate VLAN, configured by the **subordinate separate** command.
Interface	Interfaces in a VLAN.

5.5.3 mux-vlan

Function

The **mux-vlan** command configures a VLAN as a principal VLAN.

The **undo mux-vlan** command cancels the configuration.

By default, no VLAN is configured as a principal VLAN.

Format

mux-vlan

undo mux-vlan

Parameters

None

Views

VLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

All employees and customers of an enterprise can access servers on the enterprise network. The enterprise allows employees to communicate but expects to isolate customers from one another. To meet this requirement, the enterprise can add the servers to a VLAN, add employees to another VLAN, and add each customer to a different VLAN. This wastes VLAN IDs and increases workload on VLAN configuration.

The MUX VLAN function is introduced to solve this problem. The MUX VLAN function isolates Layer 2 traffic between interfaces in a VLAN. This function involves the following VLANs:

- Principal VLAN: allows member interfaces to communicate with each other and with interfaces in subordinate VLANs.
- Subordinate VLAN
  - Subordinate separate VLAN: allows member interfaces to communicate with only interfaces in the principal VLAN. An interface in a subordinate separate VLAN cannot communicate with interfaces in the same VLAN or other subordinate VLANs.
  - Subordinate group VLAN: allows member interfaces to communicate with interfaces in the same VLAN and interfaces in the principal VLAN. An interface in a subordinate group VLAN cannot communicate with interfaces in other subordinate VLANs.

According to features of the preceding VLANs, the enterprise can add the servers to the principal VLAN, add employees to a subordinate group VLAN, and add customers to a subordinate separate VLAN. Customers are then allowed to access the servers but isolated from one another. This saves VLAN IDs on the enterprise network and facilitates network management.

Prerequisites

The VLAN to be configured as a principal VLAN is not a super-VLAN, a sub-VLAN, or a subordinate VLAN.

Follow-up Procedure

Configure subordinate VLANs for the principal VLAN and enable the MUX VLAN function on interfaces.

Precautions

The VLAN ID assigned to a principal VLAN cannot be used to configure the super-VLAN or sub-VLAN. Additionally, it is not recommended that this VLAN ID be used to configure VLAN mapping and VLAN stacking.

If a VLAN has been configured as a principal VLAN, it cannot be configured as a subordinate VLAN of another principal VLAN.

Example

# Configure VLAN 5 as a principal VLAN.

```
<HUAWEI> system-view
[HUAWEI] vlan 5
[HUAWEI-vlan5] mux-vlan
```

5.5.4 port mux-vlan enable

Function

The **port mux-vlan enable** command enables the MUX VLAN function on an interface.

The **undo port mux-vlan enable** command disables the MUX VLAN function on an interface.

By default, the MUX VLAN function is disabled on an interface.

Format

port mux-vlan enable vlan { *vlan-id1* [**to** *vlan-id2*] } &<1-10>

undo port mux-vlan enable vlan { *vlan-id1* [**to** *vlan-id2*] } &<1-10>

undo port mux-vlan enable

Parameters

Parameter	Description	Value
vlan { *vlan-id1* [**to** *vlan-id2*] }	Enables MUX VLAN for specified VLANs. For principal VLANs, a VLAN ID range can be specified. For subordinate group VLANs or separate VLANs, only one VLAN ID can be specified.	The value is an integer ranging from 1 to 4094.

Views

Ethernet interface view, GE interface view, XGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, MultiGE interface view, VE interface view, Eth-Trunk interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The MUX VLAN function isolates Layer 2 traffic between interfaces in a VLAN. This function involves a MUX VLAN and several subordinate VLANs. Subordinate VLANs are classified into subordinate group VLANs and subordinate separate VLANs. Subordinate VLANs can communicate with the principal VLAN but cannot communicate with each other. Interfaces in a subordinate group VLAN can communicate with each other, and interfaces in a subordinate separate VLAN are isolated from each other.

The MUX VLAN function takes effect only after it is enabled on an interface.

Prerequisites

Before enabling the MUX VLAN function, ensure that the interface has been added to a principal or subordinate VLAN as an access, hybrid, or trunk interface.

Precautions

- Disabling MAC address learning or limiting the number of learned MAC addresses on an interface affects the MUX VLAN function on the interface.
- The MUX VLAN and port security functions conflict on an interface; therefore, the **port mux-vlan enable** and **port-security enable** commands are not advised to be used on the same interface.
- The MUX VLAN and MAC address authentication conflict on an interface; therefore, the **port mux-vlan enable** and **mac-authen** commands are not advised to be used on the same interface.
- The MUX VLAN and 802.1x authentication conflict on an interface; therefore, the **port mux-vlan enable** and **dot1x enable** commands are not advised to be used on the same interface.

- You can create a VLANIF interface for a principal VLAN, but cannot create a VLANIF interface for a subordinate group VLAN or separate VLAN.
- The **port mux-vlan enable** command is not supported on a **negotiation-auto** or **negotiation-desirable** port.
- When the interface is enabled with MUX VLAN and configured with the PVID using the **port trunk pvid vlan** command, do not configure the PVID as the ID of the principal VLAN or subordinate VLAN of the MUX VLAN. For example, VLAN 10 is the principal VLAN, VLAN 11 is a subordinate group VLAN, and VLAN 12 is a subordinate separate VLAN. After the **port mux-vlan enable vlan 10** command is used on the interface to enable MUX VLAN, do not run the **port trunk pvid vlan** command to set the PVID to VLAN 11 or VLAN 12.

Example

# Enable the MUX VLAN function in VLAN 2 on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] port link-type hybrid
[HUAWEI-GigabitEthernet0/0/1] port mux-vlan enable vlan 2
```

5.5.5 subordinate group

Function

The **subordinate group** command configures subordinate group VLANs for a principal VLAN.

The **undo subordinate group** command removes subordinate group VLANs from a principal VLAN.

By default, a principal VLAN does not have any subordinate group VLAN.

Format

subordinate group { *vlan-id1* [**to** *vlan-id2*] } &<1-10>

undo subordinate group { *vlan-id1* [**to** *vlan-id2*] } &<1-10>

Parameters

Parameter	Description	Value
vlan-id1 [**to** *vlan-id2*]	Specifies a range of VLAN IDs. ● *vlan-id1* specifies the start VLAN ID. ● **to** *vlan-id2* specifies the end VLAN ID. If **to** *vlan-id2* is not specified, only one subordinate group VLAN is configured.	● The value of *vlan-id1* is an integer that ranges from 1 to 4094. ● The value of *vlan-id2* is an integer that ranges from 1 to 4094 and must be greater than or equal to the value of *vlan-id1*.

Views

VLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

All employees and customers of an enterprise can access servers on the enterprise network. The enterprise allows employees to communicate but expects to isolate customers from one another. To meet this requirement, the enterprise can add the servers to a VLAN, add employees to another VLAN, and add each customer to a different VLAN. This wastes VLAN IDs and increases workload on VLAN configuration.

The MUX VLAN function is introduced to solve this problem. The MUX VLAN function isolates Layer 2 traffic between interfaces in a VLAN. This function involves the following VLANs:

- Principal VLAN: allows member interfaces to communicate with each other and with interfaces in subordinate VLANs.
- Subordinate VLAN
  - Subordinate separate VLAN: allows member interfaces to communicate with only interfaces in the principal VLAN. An interface in a subordinate separate VLAN cannot communicate with interfaces in the same VLAN or other subordinate VLANs.
  - Subordinate group VLAN: allows member interfaces to communicate with interfaces in the same VLAN and interfaces in the principal VLAN. An interface in a subordinate group VLAN cannot communicate with interfaces in other subordinate VLANs.

According to features of the preceding VLANs, the enterprise can add the servers to the principal VLAN, add employees to a subordinate group VLAN, and add customers to a subordinate separate VLAN. Customers are then allowed to access the servers but isolated from one another. This saves VLAN IDs on the enterprise network and facilitates network management.

After interfaces using by employees are added to the subordinate group VLAN, employees can access servers of the enterprise and communicate with one another.

Prerequisites

The specified subordinate group VLANs are not super-VLANs and do not have any VLANIF interface.

Before configuring a VLAN as a subordinate group VLAN, run the **undo subordinate group** command to delete all its member interfaces.

Follow-up Procedure

Add interfaces to subordinate group VLANs and enable the MUX VLAN function on the interfaces.

Precautions

Before configuring a VLAN as a subordinate separate VLAN, ensure that the VLAN and its principal VLAN have been created. Otherwise, this command does not take effect even if it is executed successfully.

Subordinate VLANs must be different from the principal VLAN.

A VLAN cannot be configured as a subordinate group VLAN and a subordinate separate VLAN simultaneously.

If you run the **subordinate group** command multiple times in the same VLAN view, all the specified VLANs are configured as subordinate group VLANs. A maximum of 128 subordinate group VLANs can be configured in a primary VLAN.

The VLAN ID assigned to a group VLAN cannot be used to configure a VLANIF interface, super-VLAN, or sub-VLAN. Additionally, it is not recommended that this VLAN ID be used to configure VLAN mapping and VLAN stacking.

When you configure a subordinate VLAN using the **subordinate group** or **subordinate separate** command or create a VLAN with an ID same as an existing subordinate VLAN, the device deletes existing dynamic MAC address entries and duplicated MUX MAC address entries of the principal VLAN of this subordinate VLAN.

Example

# Configure VLAN 7 as the subordinate group VLAN of VLAN 5.

```
<HUAWEI> system-view
[HUAWEI] vlan 5
[HUAWEI-vlan5] subordinate group 7
```

5.5.6 subordinate separate

Function

The **subordinate separate** command configures a subordinate separate VLAN for a principal VLAN.

The **undo subordinate separate** command removes the subordinate separate VLAN from a principal VLAN.

By default, a principal VLAN does not have any subordinate separate VLAN.

Format

subordinate separate *vlan-id*

undo subordinate separate

Parameters

Parameter	Description	Value
vlan-id	Specifies the ID of an existing VLAN.	The value is an integer that ranges from 1 to 4094.

Views

VLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

All employees and customers of an enterprise can access servers on the enterprise network. The enterprise allows employees to communicate but expects to isolate customers from one another. To meet this requirement, the enterprise can add the servers to a VLAN, add employees to another VLAN, and add each customer to a different VLAN. This wastes VLAN IDs and increases workload on VLAN configuration.

The MUX VLAN function is introduced to solve this problem. The MUX VLAN function isolates Layer 2 traffic between interfaces in a VLAN. This function involves the following VLANs:

- Principal VLAN: allows member interfaces to communicate with each other and with interfaces in subordinate VLANs.
- Subordinate VLAN
  - Subordinate separate VLAN: allows member interfaces to communicate with only interfaces in the principal VLAN. An interface in a subordinate

separate VLAN cannot communicate with interfaces in the same VLAN or other subordinate VLANs.

- Subordinate group VLAN: allows member interfaces to communicate with interfaces in the same VLAN and interfaces in the principal VLAN. An interface in a subordinate group VLAN cannot communicate with interfaces in other subordinate VLANs.

According to features of the preceding VLANs, the enterprise can add the servers to the principal VLAN, add employees to a subordinate group VLAN, and add customers to a subordinate separate VLAN. Customers are then allowed to access the servers but isolated from one another. This saves VLAN IDs on the enterprise network and facilitates network management.

After interfaces using by customers are added to the subordinate separate VLAN, customers can neither communicate with each other nor access servers of the enterprise.

Prerequisites

The specified subordinate separate VLANs are not super-VLANs and do not have any VLANIF interface.

Before configuring a VLAN as a subordinate separate VLAN, run the **undo subordinate separate** command to delete all its member interfaces.

Follow-up Procedure

Add interfaces to the subordinate separate VLAN and enable the MUX VLAN function on the interfaces.

Precautions

Before configuring a VLAN as a subordinate separate VLAN, ensure that the VLAN and its principal VLAN have been created. Otherwise, this command does not take effect even if it is executed successfully.

Subordinate VLANs must be different from the principal VLAN.

A VLAN cannot be configured as a subordinate group VLAN and a subordinate separate VLAN simultaneously.

A principal VLAN can be configured with only one subordinate separate VLAN. Before configuring another VLAN as the subordinate separate VLAN, run the **undo subordinate separate** command to delete the previous one.

The VLAN ID assigned to a separate VLAN cannot be used to configure a VLANIF interface, super-VLAN, or sub-VLAN. Additionally, it is not recommended that this VLAN ID be used to configure VLAN mapping and VLAN stacking.

When you configure a subordinate VLAN using the **subordinate group** or **subordinate separate** command or create a VLAN with an ID same as an existing subordinate VLAN, the device deletes existing dynamic MAC address entries and duplicated MUX MAC address entries of the principal VLAN of this subordinate VLAN.

Example

# Configure VLAN 6 as the subordinate separate VLAN of VLAN 5.

```
<HUAWEI> system-view
[HUAWEI] vlan 5
[HUAWEI-vlan5] subordinate separate 6
```

5.6 VLAN Termination Configuration Commands

5.6.1 Command Support

Only the following switch models support VLAN termination:

S5731-H, S5731-S, S5731S-S, S5731S-H, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S

5.6.2 arp broadcast enable

Function

The **arp broadcast enable** command enables ARP broadcast on a VLAN tag termination sub-interface.

The **undo arp broadcast enable** command disables ARP broadcast on a VLAN tag termination sub-interface.

By default, ARP broadcast is disabled on a VLAN tag termination sub-interface.

Format

arp broadcast enable

undo arp broadcast enable

NOTE

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

Parameters

None

Views

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

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

VLAN tag termination sub-interfaces discard broadcast packets after receiving the packets. To permit a VLAN tag termination sub-interface to forward broadcast packets, run the **arp broadcast enable** command on the sub-interface to enable ARP broadcast.

Configuration Impact

When IP packets need to be sent out from the termination sub-interface and there is no corresponding ARP entry on the device, the following situations may occur:

- If ARP broadcast is not enabled on the termination sub-interface, the system does not send or forward broadcast ARP packets to learn ARP entries (gratuitous ARP packets will still be sent normally). In this case, the IP packets are discarded directly.
- The system tags an ARP broadcast packet and forwards it through the VLAN tag termination sub-interface when ARP broadcast is enabled run on the VLAN tag termination sub-interface.

Precautions

When you enable or disable ARP broadcast on a VLAN tag termination sub-interface, the routing status of the sub-interface becomes Down and then Up. This may result in route flapping on the entire network, affecting services.

After the ARP broadcast function is enabled using the **arp broadcast enable** command, if a service packet is sent from a termination sub-interface but does not have an ARP entry, an ARP request is copied and sent in all VLANs of the sub-interface. If a large number of VLANs are configured, the number of ARP requests to be copied and sent is large, which may bring a heavy burden on the peer devices that receive the ARP requests. Consequently, the peer devices may encounter exceptions, such as high CPU usage and broadcast suppression. The local device may also fail to immediately send ARP requests as it is busy in processing packet copying, leading to ARP learning failures. To prevent this issue, you are advised to reduce the number of VLANs configured on sub-interfaces.

Example

# Enable ARP broadcast on XGigabitEthernet0/0/1.1.

```
<HUAWEI> system-view
[HUAWEI] vcmp role silent
[HUAWEI] interface xgigabitethernet 0/0/1
[HUAWEI-XGigabitEthernet0/0/1] port link-type hybrid
[HUAWEI-XGigabitEthernet0/0/1] quit
[HUAWEI] interface xgigabitethernet 0/0/1.1
[HUAWEI-XGigabitEthernet0/0/1.1] dot1q termination vid 10
[HUAWEI-XGigabitEthernet0/0/1.1] arp broadcast enable
```

5.6.3 display dot1q information

Function

The **display dot1q information termination** command displays the configuration of a dot1q sub-interface.

Format

display dot1q information termination [**interface** *interface-type interface-number* [.*subinterface-number*]]

NOTE

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

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Specifies the type and number of an interface.	-
subinterface-number	Specifies the number of a sub-interface.	The value is an integer that ranges from 1 to 4096.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After configuring dot1q termination on sub-interfaces, run the **display dot1q information termination** command to view the sub-interfaces where dot1q termination is configured and configuration of the dot1q sub-interfaces.

Example

# Display the configuration of all dot1q sub-interfaces.

```
<HUAWEI> display dot1q information termination
 XGigabitEthernet0/0/1.3
   Total QinQ Num: 1
   dot1q  termination vid 3
   Total vlan-group Num: 0
```

Table 5-51 Description of the display dot1q information command output

Item	Description
XGigabitEthernet0/0/1.3	Sub-interface name.
Total QinQ Num	Number of QinQ entries configured for user packets on a sub-interface.

Item	Description
dot1q termination vid 3	VLAN allowed by a sub-interface. To specify the parameter, run the **dot1q termination vid** command.
Total vlan-group Num	Number of VLAN groups configured on a sub-interface.

5.6.4 display qinq information

Function

The **display qinq information** command displays the configuration of all the sub-interfaces configured with QinQ termination, QinQ stacking, or QinQ mapping.

Format

display qinq information { **termination** | **stacking** | **mapping** } [**interface** *interface-type interface-number* [.*subinterface-number*]]

NOTE

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

Parameters

Parameter	Description	Value
termination	Displays all the sub-interfaces configured with QinQ termination.	-
stacking	Displays all the sub-interfaces configured with QinQ stacking.	-
mapping	Displays all the sub-interfaces configured with QinQ mapping.	-
interface *interface-type interface-number*	Displays whether all the sub-interfaces of the specified main interface are configured with QinQ termination, QinQ stacking, or QinQ mapping. *interface-type* specifies the interface type. *interface-number* specifies the number of the main interface.	-

Parameter	Description	Value
subinterface-number	Specifies the number of a sub-interface.	The value is an integer that ranges from 1 to 4096.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After configuring QinQ termination, QinQ stacking, and QinQ mapping, run the **display qinq information** command to view the configuration and the sub-interfaces configured with these functions.

When a large number of QinQ termination, QinQ stacking, and QinQ mapping entries are configured, it is recommended that you specify a QinQ function, a main interface, a sub-interface, or a pipe operator (|) to filter the output. Otherwise, too much information is displayed, which has the following negative effects:

- The displayed information is updated continuously on the display terminal and the required information cannot be obtained.
- The system traverses and retrieves information for a long time. As a result, the system does not respond to any request.

When using this command, note the following points:

- If you specify only **termination** in the command, all sub-interfaces configured with QinQ termination are displayed.
- If you specify **termination** and **interface** *interface-type interface-number*, the sub-interface configured with QinQ termination on the specified main interface is displayed.
- If you specify **termination** and **interface** *interface-type interface-number.subinterface-number*, the specified sub-interface configured with QinQ termination is displayed.
- If you specify only **stacking** in the command, all sub-interfaces configured with QinQ stacking are displayed.
- If you specify **stacking** and **interface** *interface-type interface-number*, the sub-interface configured with QinQ stacking on the specified main interface is displayed.
- If you specify **stacking** and **interface** *interface-type interface-number.subinterface-number*, the specified sub-interface configured with QinQ stacking is displayed.
- If you specify only **mapping** in the command, all sub-interfaces configured with QinQ mapping are displayed.

- If you specify **mapping** and **interface** *interface-type interface-number*, the sub-interface configured with QinQ mapping on the specified main interface is displayed.
- If you specify **mapping** and **interface** *interface-type interface-number.subinterface-number*, the specified sub-interface configured with QinQ mapping is displayed.

Example

# Display all the sub-interfaces configured with QinQ termination.

```
<HUAWEI> display dot1q information termination
 XGigabitEthernet0/0/1.30
  Total QinQ Num: 1
  qinq termination pe-vid 300 ce-vid 200
  Total vlan-group Num: 0
```

# Display all the sub-interfaces configured with QinQ stacking.

```
<HUAWEI> display qinq information stacking
 XGigabitEthernet0/0/1.4
  Total QinQ Num: 1
   qinq stacking vid 25 pe-vid 35
  Total vlan-group Num: 0
```

# Display all the sub-interfaces configured with QinQ mapping.

```
<HUAWEI>display qinq information mapping
 XGigabitEthernet0/0/1.5
  Total QinQ Num: 1
   qinq mapping vid 55 map-vlan vid 65
  Total vlan-group Num: 0
```

Table 5-52 Description of the display qinq information command output

Item	Description
XGigabitEthernet0/0/1.30	Sub-interface name.
Total QinQ Num	Number of QinQ entries configured for user packets on a sub-interface.
Total vlan-group Num	Number of VLAN groups configured on a sub-interface.

5.6.5 dot1q termination vid

Function

The **dot1q termination vid** command sets the single VLAN ID for Dot1q termination on a sub-interface.

The **undo dot1q termination vid** command deletes the single VLAN ID for Dot1q termination on a sub-interface.

By default, the single VLAN ID for Dot1q termination is not set on a sub-interface.

Format

dot1q termination vid *low-pe-vid* [**to** *high-pe-vid*]

undo dot1q termination vid *low-pe-vid* [**to** *high-pe-vid*]

NOTE

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

Parameters

Parameter	Description	Value
low-pe-vid	Specifies the minimum value of the VLAN tag in user packets.	The value is an integer that ranges from 2 to 4094.
high-pe-vid	Specifies the maximum value of the VLAN tag in user packets. The value of *high-pe-vid* must be greater than or equal to the value of *low-pe-vid*.	The value is an integer that ranges from 2 to 4094.

Views

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

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

- Communication between VLANs

  VLANs are widely used because they can separate Layer 2 packets. A physical LAN is divided into multiple logical broadcast domains. Hosts in the same VLAN can communicate with each other but the hosts of different VLANs cannot. The Layer 3 routing technology is used for communication between hosts of different VLANs in the following two methods:

  - Through the VLANIF interface on the Layer 3 switch.
  - Through the Layer 3 Ethernet interface on the Layer 3 switch.

    However, when a traditional Layer 3 Ethernet interface receives VLAN packets, the VLAN packets are discarded. To enable communication between hosts of different VLANs, you can create an Ethernet sub-interface on the Layer 3 Ethernet interface and enable QinQ termination on the sub-interface to remove the tag from the VLAN packet.

- Communication between a LAN and a WAN

  Most packets on a LAN have VLAN tags, but some WAN protocols such as ATM, FR, and PPP, cannot identify VLAN packets. To send a VLAN packet from LAN to WAN, the device records VLAN information in the packet, removes the VLAN tag, and forwards the packet.

Based on the number of tags, VLAN packets can be classified into Dot1q packets and QinQ packets. A Dot1q packet carries a single-layer VLAN tag and a QinQ packet carries a double-layer VLAN tag. Accordingly, there are two VLAN tag termination modes:

- Dot1q termination, which terminates tags carried in Dot1q packets

  To configure Dot1q termination, run the **dot1q termination vid** command.

- QinQ termination, which terminates tags carried in QinQ packets.

  To configure QinQ termination, run the **qinq termination pe-vid ce-vid** command in the sub-interface view.

After the **dot1q termination vid** command is run, the sub-interface for VLAN tag termination processes the packet in the following procedures:

- The sub-interface removes the tag in the VLAN packet when receiving the packet and forwards the packet on Layer 3. The outbound interface determines whether the forwarded VLAN packet carries tags.
- The sub-interface adds VLAN information to the packet and then sends the packet.

Precautions

- The tag values of the user packet received by the sub-interface must be in the range of *low-pe-vid* to *high-pe-vid* specified in the command; otherwise, the packet is discarded.
- The VLANs allowed by a sub-interface cannot be created globally or on main interfaces, and their information cannot be displayed either.The VLANs allowed by a sub-interface cannot be the same as the default VLAN of its main interface.
- When the sub-interface is used for Layer 3 forwarding, it is recommended that there should be a maximum of 128 VLANs in the VLAN range. When there are more than 128 VLANs, IPv4 addresses can be configured but IPv6 addresses cannot be configured.
- If the **dot1q termination vid** command is run more than once, all configurations take effect.
- VLAN termination sub-interfaces cannot be created on a VCMP client.

Example

# Set the encapsulation mode on XGigabitEthernet0/0/1.1 to Dot1q and allow the packets with the VLAN tag 100 to pass through.

```
<HUAWEI> system-view
[HUAWEI] vcmp role silent
[HUAWEI] interface xgigabitethernet 0/0/1
```

```
[HUAWEI-XGigabitEthernet0/0/1] port link-type hybrid
[HUAWEI-XGigabitEthernet0/0/1] quit
[HUAWEI] interface xgigabitethernet 0/0/1.1
[HUAWEI-XGigabitEthernet0/0/1.1] dot1q termination vid 100
```

5.6.6 qinq termination l2

Function

The **qinq termination l2** command configures the mode in which a sub-interface for QinQ VLAN tag termination connects to a Pseudo-Wire Emulation Edge to Edge (PWE3)/Virtual Leased Line (VLL)/Virtual Private LAN Service (VPLS) network.

The **undo qinq termination l2** command deletes the mode configured for a sub-interface for QinQ VLAN tag termination in which the sub-interface connects to a PWE3/VLL/VPLS network.

By default, access attributes are not configured on a sub-interface for QinQ VLAN tag termination.

Format

qinq termination l2 { **symmetry** | **asymmetry** }

undo qinq termination l2

NOTE

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

Parameters

Parameter	Description	Value
symmetry	Configures the sub-interface for QinQ VLAN tag termination to connect to a PWE3/VLL/VPLS network in symmetry mode.	-
asymmetry	Configures the sub-interface for QinQ VLAN tag termination to connect to a PWE3/VLL/VPLS network in asymmetry mode.	-

Views

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

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

More QinQ encapsulation and termination modes are provided to differentiate users and services and save VLAN resources. These modes are widely used for refined operation.

If users communicate over an L2VPN (a PWE3, VLL, or VPLS network), you can run the **qinq termination l2** command on the sub-interfaces for QinQ VLAN tag termination of L2VPN edge devices to configure the mode in which the sub-interfaces connect to the L2VPN.

Prerequisites

A VLL, PWE3, or VPLS network-side has been deployed.

For VLL, PWE3, or VPLS configurations, see VLL Configuration, PWE3 Configuration, and VPLS Configuration in the *S300, S500, S2700, S5700, and S6700 V200R023C00 Configuration Guide - VPN*.

When a sub-interface for QinQ VLAN tag termination is connected to the L2VPN, the PE processes packets based on the QinQ termination configuration, attributes of the sub-interface for QinQ VLAN tag termination when the sub-interface connects to the PWE3, VLL, or VPLS network, and encapsulation mode.

NOTE

Select the encapsulation mode according to **encapsulation (VSI view)** or **mpls l2vc**.

Table 5-53 Packet processing on the inbound interface in the VPLS scenario

Inbound Interface Type	Ethernet Encapsulation	VLAN Encapsulation
Symmetrical mode	Removes the outer tag.	Reserves double tags. No action is required.
Asymmetrical mode	Removes double tags.	Removes the outer tag.
Default	Removes double tags.	Reserves double tags. No action is required.

Table 5-54 Packet processing on the outbound interface in the VPLS scenario

Inbound Interface Type	Ethernet Encapsulation	VLAN Encapsulation
Symmetrical mode	Removes the MPLS label and adds the outer tag specified by **pe-vid** that is configured on the sub-interface for QinQ VLAN tag termination.	If packets carry the inner tag: removes the MPLS label and replaces the outer tag with the tag specified by **pe-vid** that is configured on the sub-interface for QinQ VLAN tag termination. If packets do not carry the inner tag: removes the MPLS label and adds the outer tag specified by **pe-vid** that is configured on the sub-interface for QinQ VLAN tag termination.

Inbound Interface Type	Ethernet Encapsulation	VLAN Encapsulation
Asymmetrical mode	S5731-H, S5731S-H, S5732-H, S5731-S, S5731S-S, S6730-S, S6730S-S, S6730S-H, and S6730-H: removes the MPLS label and adds double tags according to **ce-vid** and **pe-vid** configured on the sub-interface for QinQ VLAN tag termination. Other models: If packets do not carry the inner tag: removes the MPLS label and adds double tags according to **ce-vid** and **pe-vid** configured on the sub-interface for QinQ VLAN tag termination. If packets carry the inner tag: removes the MPLS label, removes the inner tag, and adds double tags according to **ce-vid** and **pe-vid** configured on the sub-interface for QinQ VLAN tag termination.	S5731-H, S5731S-H, S5732-H, S5731-S, S5731S-S, S6730-S, S6730S-S, S6730S-H, and S6730-H: If packets do not carry the inner tag: removes the MPLS label and adds double tags according to **ce-vid** and **pe-vid** configured on the sub-interface for QinQ VLAN tag termination. If packets carry the inner tag: removes the MPLS label, removes the inner tag, and adds double tags according to **ce-vid** and **pe-vid** configured on the sub-interface for QinQ VLAN tag termination. Other models: If packets do not carry the inner tag: removes the MPLS label and adds double tags according to **ce-vid** and **pe-vid** configured on the sub-interface for QinQ VLAN tag termination. If packets carry one inner tag: removes the MPLS label, removes one inner tag, and adds double tags according to **ce-vid** and **pe-vid** configured on the sub-interface for QinQ VLAN tag termination. If packets carry double inner tags: removes the MPLS label, removes double inner tags, and adds double tags according to **ce-vid** and **pe-vid** configured on the sub-interface for QinQ VLAN tag termination.

Inbound Interface Type	Ethernet Encapsulation	VLAN Encapsulation
Default	S5731-H, S5731S-H, S5732-H, S5731-S, S5731S-S, S6730-S, S6730S-S, S6730S-H and S6730-H: removes the MPLS label and adds double tags according to **ce-vid** and **pe-vid** configured on the sub-interface for QinQ VLAN tag termination. Other models: If packets do not carry the inner tag: removes the MPLS label and adds double tags according to **ce-vid** and **pe-vid** configured on the sub-interface for QinQ VLAN tag termination. If packets carry the inner tag: removes the MPLS label, removes the inner tag, and adds double tags according to **ce-vid** and **pe-vid** configured on the sub-interface for QinQ VLAN tag termination.	Removes the MPLS label and transparently transmits packets.

Table 5-55 Packet processing on the inbound interface in the VLL or PWE3 scenario

Inbound Interface Type	Raw Encapsulation	Tagged Encapsulation
Symmetrical mode	Removes the outer tag.	Reserves double tags. No action is required.
Asymmetrical mode	Removes double tags.	Removes the outer tag.
Default	Removes the outer tag.	Reserves double tags. No action is required.

Table 5-56 Packet processing on the outbound interface in the VLL or PWE3 scenario

Inbound Interface Type	Raw Encapsulation	Tagged Encapsulation
Symmetrical mode	Removes the MPLS label and adds the outer tag specified by **pe-vid** that is configured on the sub-interface for QinQ VLAN tag termination.	If packets carry the inner tag: removes the MPLS label and replaces the outer tag with the tag specified by **pe-vid** that is configured on the sub-interface for QinQ VLAN tag termination. If packets do not carry the inner tag: removes the MPLS label and adds the outer tag specified by **pe-vid** that is configured on the sub-interface for QinQ VLAN tag termination.

Inbound Interface Type	Raw Encapsulation	Tagged Encapsulation
Asymmetrical mode	S5731-H, S5731S-H, S5732-H, S5731-S, S5731S-S, S6730-S, S6730S-S, S6730S-H, and S6730-H: removes the MPLS label and adds double tags according to **ce-vid** and **pe-vid** configured on the sub-interface for QinQ VLAN tag termination. Other models: If packets do not carry the inner tag: removes the MPLS label and adds double tags according to **ce-vid** and **pe-vid** configured on the sub-interface for QinQ VLAN tag termination. If packets carry the inner tag: removes the MPLS label, removes the inner tag, and adds double tags according to **ce-vid** and **pe-vid** configured on the sub-interface for QinQ VLAN tag termination.	S5731-H, S5731S-H, S5732-H, S5731-S, S5731S-S, S6730-S, S6730S-S, S6730S-H, and S6730-H: If packets do not carry the inner tag: removes the MPLS label and adds double tags according to **ce-vid** and **pe-vid** configured on the sub-interface for QinQ VLAN tag termination. If packets carry the inner tag: removes the MPLS label, removes the inner tag, and adds double tags according to **ce-vid** and **pe-vid** configured on the sub-interface for QinQ VLAN tag termination. Other models: If packets do not carry the inner tag: removes the MPLS label and adds double tags according to **ce-vid** and **pe-vid** configured on the sub-interface for QinQ VLAN tag termination. If packets carry one inner tag: removes the MPLS label, removes one inner tag, and adds double tags according to **ce-vid** and **pe-vid** configured on the sub-interface for QinQ VLAN tag termination. If packets carry double inner tags: removes the MPLS label, removes double inner tags, and adds double tags according to **ce-vid** and **pe-vid** configured on the sub-interface for QinQ VLAN tag termination.

Inbound Interface Type	Raw Encapsulation	Tagged Encapsulation
Default	Removes the MPLS label and adds the outer tag specified by **pe-vid** that is configured on the sub-interface for QinQ VLAN tag termination.	If packets carry the inner tag: removes the MPLS label and replaces the outer tag with the tag specified by **pe-vid** on the sub-interface for QinQ VLAN tag termination. If packets do not carry the inner tag: removes the MPLS label and adds the outer tag specified by **pe-vid** on the sub-interface for QinQ VLAN tag termination.

Example

# Configure the sub-interface for QinQ VLAN tag termination XGigabitEthernet0/0/1.1 to connect to an L2VPN in asymmetry mode.

```
<HUAWEI> system-view
[HUAWEI] vcmp role silent
[HUAWEI] interface xgigabitethernet 0/0/1
[HUAWEI-XGigabitEthernet0/0/1] port link-type hybrid
[HUAWEI-XGigabitEthernet0/0/1] quit
[HUAWEI] interface xgigabitethernet 0/0/1.1
[HUAWEI-XGigabitEthernet0/0/1.1] qinq termination l2 asymmetry
[HUAWEI-XGigabitEthernet0/0/1.1] qinq termination pe-vid 100 ce-vid 200
[HUAWEI-XGigabitEthernet0/0/1.1] quit
```

5.6.7 qinq termination pe-vid ce-vid

Function

The **qinq termination pe-vid ce-vid** command configures QinQ termination on a sub-interface.

The **undo qinq termination pe-vid ce-vid** command cancels QinQ termination on a sub-interface.

By default, QinQ termination is disabled on a sub-interface.

Format

qinq termination pe-vid *pe-vid* **ce-vid** *ce-vid1* [**to** *ce-vid2*]

undo qinq termination pe-vid *pe-vid* **ce-vid** *ce-vid1* [**to** *ce-vid2*]

NOTE

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

Parameters

Parameter	Description	Value
pe-vid *pe-vid*	Specifies the outer VLAN ID.	The value is an integer that ranges from 2 to 4094.
ce-vid *ce-vid1* [**to** *ce-vid2*]	Specifies the inner VLAN ID. ● *ce-vid1*: specifies the lower threshold of the inner VLAN tag in the user packet. ● *ce-vid2*: specifies the upper threshold of the outer VLAN tag in the user packet. ● The value of *ce-vid2* must be greater than or equal to the value of *ce-vid1*.	The value of *ce-vid1* is an integer that ranges from 1 to 4094. The value of *ce-vid2* is an integer that ranges from 1 to 4094.

Views

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

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

- Communication between VLANs

  VLANs are widely used because they can separate Layer 2 packets. A physical LAN is divided into multiple logical broadcast domains. Hosts in the same VLAN can communicate with each other but the hosts of different VLANs cannot. The Layer 3 routing technology is used for communication between hosts of different VLANs in the following two methods:

  - Through the VLANIF interface on the Layer 3 router.
  - Through the Layer 3 Ethernet interface on the router.

    However, when a traditional Layer 3 Ethernet interface receives VLAN packets, the VLAN packets are discarded. To enable communication between hosts of different VLANs, you can create an Ethernet sub-interface on the Layer 3 Ethernet interface and enable QinQ termination on the sub-interface to remove the tag from the VLAN packet.

- Communication between a LAN and a WAN

  Most packets on a LAN have VLAN tags, but some WAN protocols such as ATM, FR, and PPP, cannot identify VLAN packets. To send a VLAN packet from LAN to WAN, the device records VLAN information in the packet, removes the VLAN tag, and forwards the packet.

Based on the number of tags, VLAN packets can be classified into Dot1q packets and QinQ packets. A Dot1q packet carries a single-layer VLAN tag and a QinQ packet carries a double-layer VLAN tag. Accordingly, there are two VLAN tag termination modes:

- Dot1q termination, which terminates tags carried in Dot1q packets

  To configure Dot1q termination, run the **dot1q termination vid** command in the sub-interface view.

- QinQ termination, which terminates tags carried in QinQ packets.

  To configure Dot1q termination, run the **qinq termination pe-vid ce-vid** command.

After the **qinq termination pe-vid ce-vid** command is run, the sub-interface for VLAN tag termination processes the packet in the following procedures:

- The sub-interface removes the tag in the VLAN packet when receiving the packet and forwards the packet on Layer 3. Whether the forwarded VLAN packet carries tags is determined by the outbound interface.
- The sub-interface adds VLAN information to the packet and then sends the packet.

Precautions

- The tag values of the user packet received by the sub-interface must be in the range specified in the command; otherwise, the packet is discarded.
- The allowed VLANs on a sub-interface cannot be created in the system view or be displayed by the display command.
- When the sub-interface is used for Layer 3 forwarding, it is recommended that there should be a maximum of 128 VLANs in the VLAN range. When there are more than 128 VLANs, IPv4 addresses can be configured but IPv6 addresses cannot be configured.

Example

# Set the encapsulation mode on XGigabitEthernet0/0/1.1 to QinQ and allow the packets with the outer VLAN tag 100 and inner VLAN tag 200 to pass through.

```
<HUAWEI> system-view
[HUAWEI] vcmp role silent
[HUAWEI] interface xgigabitethernet 0/0/1
[HUAWEI-XGigabitEthernet0/0/1] port link-type hybrid
[HUAWEI-XGigabitEthernet0/0/1] quit
[HUAWEI] interface xgigabitethernet 0/0/1.1
[HUAWEI-XGigabitEthernet0/0/1.1] qinq termination pe-vid 100 ce-vid 200
```

5.7 Voice VLAN Configuration Commands

5.7.1 Command Support

Commands provided in this section and all the parameters in the commands are supported by all switch models (except the S5731-L and S5731S-L), unless otherwise specified. For details, see specific commands.

5.7.2 display voice-vlan oui

Function

The **display voice-vlan oui** command displays the OUI address and OUI attributes of a voice VLAN.

Format

display voice-vlan oui

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

This command displays the OUI address, OUI mask, and OUI description of the voice VLAN.

Example

# Display the OUI address of the voice VLAN.

```
<HUAWEI> display voice-vlan oui
----------------------------------------------------
OuiAddress       Mask             Description
----------------------------------------------------
00e0-fc00-0000   ffff-ff00-0000   PhoneA
00e0-fc00-0000   ffff-ff00-0000   PhoneB
```

Table 5-57 Description of the display voice-vlan oui command output

Item	Description
OuiAddress	OUI address of the packets that can pass through the device. You can run the **voice-vlan mac-address** command to configure the OUI address.

Item	Description
Mask	OUI mask of the packets that can pass through the device. To specify the parameter, run the **voice-vlan mac-address** command.
Description	Description of the OUI address. To specify the parameter, run the **voice-vlan mac-address** command.

5.7.3 display voice-vlan status

Function

The **display voice-vlan status** command displays information about the current voice VLAN.

Format

display voice-vlan [*vlan-id*] **status**

Parameters

Parameter	Description	Value
vlan-id	Displays information about a specified voice VLAN. If *vlan-id* is not specified, information about all voice VLANs is displayed.	The value is an integer that ranges from 2 to 4094.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After the voice VLAN function is enabled, you can run the **display voice-vlan status** command to check the voice VLAN configuration.

Example

# Display information about the current voice VLAN, such as the working status, secure mode, the 802.1p priority, DSCP value, and information about an interface that is enabled with voice VLAN.

```
<HUAWEI> display voice-vlan status
Voice VLAN Configurations:
----------------------------------------------------------
Voice VLAN ID              : 2
Voice VLAN status          : Enable
Voice VLAN 8021p remark  : 6
Voice VLAN dscp remark   : 46
----------------------------------------------------------
Port Information:
------------------------------------------------------------------------------
Port           Add-Mode  Security-Mode  Legacy  PribyVLAN  Untag
Tag0
------------------------------------------------------------------------------
GE0/0/4         Manual    Normal         Disable Enable     Disable Disable
```

Table 5-58 Description of the display voice-vlan status command output

Item	Description
Voice VLAN ID	ID of the voice VLAN.
Voice VLAN status	Status of the voice VLAN function. The value can be: ● Enable ● Disable You can run the **voice-vlan enable** command to configure the voice VLAN status.
Voice VLAN 8021p remark	802.1p priority of the voice VLAN. You can run the **voice-vlan remark** command to configure the 802.1p priority of the voice VLAN.
Voice VLAN dscp remark	DSCP value of the voice VLAN. You can run the **voice-vlan remark** command to configure the DSCP value of the voice VLAN.
Port	Number of the interface on which the voice VLAN function is enabled.
Add-Mode	Working mode of the voice VLAN. The value can be: ● Manual: indicates the manual mode. ● Auto: indicates the automatic mode. You can run the **voice-vlan mode** command to configure the working mode of the voice VLAN.

Item	Description
Security-Mode	Security mode of the voice VLAN on the interface. The value can be: ● Security: indicates the secure mode. ● Normal: indicates the normal mode. You can run the **voice-vlan security enable** command to configure the secure mode of the voice VLAN.
Legacy	Whether the interface can communicate with voice devices of other vendors. The value can be: ● Enable: indicates that the interface can communicate with voice devices of other vendors. ● Disable: indicates that the interface cannot communicate with voice devices of other vendors. You can run the **voice-vlan legacy enable** command to enable an interface to communicate with voice devices of other vendors.
PribyVLAN	Whether the interface increases the priority of voice packets based on VLAN IDs ● Enable: The priority of voice packets is increased based on VLAN IDs. ● Disable: The priority of voice packets is increased based on MAC addresses. To specify the parameter, run the **voice-vlan remark-mode** command.
Untag	Whether the interface adds voice VLAN IDs to untagged packets ● Enable: The interface adds voice VLAN IDs to untagged packets. ● Disable: The interface adds PVID to untagged packets. To specify the parameter, run the **voice-vlan enable** command.
Tag0	Whether the interface changes VLAN 0 in packets to the voice VLAN ID: ● Enable: The interface changes VLAN 0 in packets to the voice VLAN ID. ● Disable: The interface changes VLAN 0 in packets to the PVID of the interface. To specify the parameter, run the **voice-vlan enable** command. **NOTE** Only the S6735-S, S6720-EI and S6720S-EI support this parameter.

5.7.4 voice-vlan enable

Function

The **voice-vlan enable** command configures the specified VLAN as a voice VLAN and enables the voice VLAN function on an interface.

The **undo voice-vlan enable** command disables the voice VLAN function on an interface.

By default, the voice VLAN function is disabled on an interface.

Format

voice-vlan *vlan-id* **enable** [**include-untagged** | **include-tag0**]*

undo voice-vlan enable (port group view)

undo voice-vlan [*vlan-id*] **enable** (other interface views except the port group view)

NOTE

Only the S6735-S, S6720-EI and S6720S-EI support **include-tag0**.

Parameters

Parameter	Description	Value
vlan-id	Configures a specified VLAN as a voice VLAN.	The value is an integer that ranges from 2 to 4094.
include-untagged	Adds voice VLAN IDs to untagged packets. When an interface receives untagged packets, the interface determines whether to add voice VLAN tags to the packets according to the OUI address configured by the **voice-vlan mac-address** command. When IP phones send untagged voice packets, this parameter is mandatory.	-

Parameter	Description	Value
include-tag0	Changes the VLAN ID in packets from VLAN 0 to the voice VLAN ID. When an interface receives packets tagged with VLAN 0, the interface checks whether the packets match the OUI address configured by the **voice-vlan mac-address** command and determines whether to change the VLAN ID in packets. When IP phones send packets tagged with VLAN 0, this parameter is mandatory.	-

Views

Ethernet interface view, GE interface view, XGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, MultiGE interface view, Eth-Trunk interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After voice VLAN is enabled on a device, based on the mode in which the priority of voice packets is increased by the **voice-vlan remark-mode** command, the device increases the priority of voice packets according to the VLAN or MAC address to ensure that voice packets are sent first.

Precautions

- If the voice VLAN configured on an interface works in automatic mode, you need to run the **port link-type** command to set the interface type to trunk or hybrid.
- To ensure normal transmission of different services, assign different VLAN IDs to the voice VLAN and default VLAN on the interface.
- Only one VLAN on an interface can be configured as a voice VLAN at a time.

- The guest VLAN, restrict VLAN, or critical VLAN on an interface cannot be configured as a voice VLAN.
- A user group VLAN configured using the **user-vlan** command cannot be specified as a voice VLAN.
- Dot1q-tunnel interfaces do not support the voice VLAN function.
- When you run the **voice-vlan enable** command multiple times, only the latest configuration takes effect.
- On the S1720GW-E, S1720GWR-E, S5720I-SI, S5720-LI, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5720S-LI, S5735-S, S500, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6720S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S **include-untagged** is valid for both untagged packets and packets tagged with VLAN 0. On other models, **include-untagged** is valid only for untagged packets. If the voice VLAN is valid for packets tagged with VLAN 0, **include-untagged** and **include-tag0** must be configured.
- On the S6735-S, S6720-EI and S6720S-EI, after a VLAN is associated with a BD or VSI and is specified as a voice VLAN, the VXLAN or MPLS function will not take effect.
- On the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, or S6730S-S, after a VLAN is associated with a BD or VSI, if this VLAN needs to be specified as a voice VLAN, you need to run the **lldp tlv-enable med-tlv network-policy voice-vlan vlan** *vlan-id* [**cos** *cvalue* | **dscp** *dvalue*]* command to configure the voice VLAN capability of LLDP on an interface.
- When a voice VLAN is configured together with VLAN Mapping, VLAN Stacking, or a Traffic Policy on the same interface, the configurations may not take effect.

Example

# Configure VLAN 2 as a voice VLAN and enable the voice VLAN function on GigabitEthernet0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] voice-vlan 2 enable
```

5.7.5 voice-vlan legacy enable

Function

The **voice-vlan legacy enable** command enables CDP-compatible Voice VLAN function so that the switch encapsulates voice VLAN information in CDP packets and sends them to connected IP phones.

The **undo voice-vlan legacy enable** command disables CDP-compatible Voice VLAN function.

By default, CDP-compatible function is disabled.

Format

voice-vlan legacy enable

undo voice-vlan legacy enable

Parameters

None

Views

Ethernet interface view, GE interface view, XGE interface view, 40GE interface view, 100GE interface view, MultiGE interface view, Eth-Trunk interface view, port group view, 25GE interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The switch can encapsulate voice VLAN information into LLDPDUs and send them to connected IP phones. However, IP phones of some vendors send Cisco Discovery Protocol (CDP) packets. You can run the **voice-vlan legacy enable** command to enable CDP-compatible function so that the switch encapsulates voice VLAN information in CDP packets and sends them to connected IP phones.

Prerequisites

The voice VLAN function has been enabled using the **voice-vlan enable** command.

Example

# Enable CDP-compatible Voice VLAN function on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface GigabitEthernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] voice-vlan 10 enable
[HUAWEI-GigabitEthernet0/0/1] voice-vlan legacy enable
```

5.7.6 voice-vlan mac-address

Function

The **voice-vlan mac-address** command sets the OUI address of the voice VLAN.

The **undo voice-vlan mac-address** command cancels the setting of the OUI address.

By default, no OUI address is set.

Format

voice-vlan mac-address *mac-address* **mask** *oui-mask* [**description** *text*]

undo voice-vlan mac-address { *mac-address* | **all** }

Parameters

Parameter	Description	Value
mac-address	Specifies the OUI address of voice packets that can be transmitted in the voice VLAN.	The value is in the format of H-H-H. H is a hexadecimal number that contains 1 to 4 digits, such as 00e0 and fc01. The address cannot be all 0s, multicast address, or broadcast address.
mask *oui-mask*	Specifies the mask of the OUI address.	The value is in the format of H-H-H. H is a 4-digit hexadecimal number that can be f or 0. The value in binary notation must start with consecutive 1s and end with consecutive 0s.
description *text*	Indicates the description of the OUI address.	The value is a string of 1 to 80 case-sensitive characters, spaces supported.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

An OUI is the first 24 bits of a 48-bit MAC address assigned to each vendor by the Institute of Electrical and Electronics Engineers (IEEE). Voice packets sent by IP phones can be identified by the MAC address ranges requested by IP phone vendors.

In voice VLAN, the OUI is user-defined and not necessarily 24 bits long. The OUI is the result of the AND operation between the MAC address and mask in the **voice-vlan mac-address** command.

Precautions

- The *mac-address* value cannot be all 0s or a multicast or broadcast address.
- The S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support a maximum

of 100 OUIs. When the switch is configured with 100 OUIs, subsequent configurations will not take effect. Other models support a maximum of 32 OUIs. When the switch is configured with 32 OUIs, subsequent configurations will not take effect.

When you run the **undo voice-vlan mac-address** command to delete an OUI MAC address, set *mac-address* to the result of the logical AND operation between the OUI and the OUI mask that you set.

Example

# Allow the voice packets coming from Phone A, an IP phone, to be identified by the voice VLAN. The MAC address of Phone A is 00e0-fc04-0004 and the OUI mask address is ffff-ff00-0000.

```
<HUAWEI> system-view
[HUAWEI] voice-vlan mac-address 00e0-fc04-0004 mask ffff-ff00-0000 description PhoneA
```

5.7.7 voice-vlan mode

Function

The **voice-vlan mode** command sets the working mode of the voice VLAN on an interface.

The **undo voice-vlan mode** command restores the mode in which an interface is added to a voice VLAN to the default.

By default, the voice VLAN of an interface works in manual mode.

NOTE

The S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S do not support this configuration.

Format

voice-vlan mode { **auto** | **manual** }

undo voice-vlan mode { **auto** | **manual** }

Parameters

Parameter	Description	Value
auto	Indicates the automatic mode of the voice VLAN. The automatic mode of the voice VLAN is not supported on the negotiation-auto or negotiation-desirable port.	-

Parameter	Description	Value
manual	Indicates the manual mode of the voice VLAN.	-

Views

Ethernet interface view, GE interface view, XGE interface view, 40GE interface view, MultiGE interface view, Eth-Trunk interface view, port group view

NOTE

The **undo voice-vlan mode manual** command is not supported in the port group view.

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Ports can be added to a voice VLAN in either of the following modes:

- Automatic mode

  A voice VLAN-enabled port learns source MAC addresses of frames from voice devices, adds ports connecting the device to voice devices to a voice VLAN.

  In auto mode, you cannot manually add ports to a voice VLAN.

  NOTE

  The automatic mode takes effect only when the **voice-vlan remark-mode mac-address** command is configured to increase the priority of voice packets based on MAC addresses and the **voice-vlan enable** command without **include-untagged** specified is configured to enable voice VLAN on the interface and add voice VLAN IDs to only tagged packets.

- Manual mode

  After the voice VLAN function is enabled, ports connected to voice devices must be manually added to a voice VLAN. Otherwise, the voice VLAN function does not take effect.

Pre-configuration Tasks

Before configuring a port to work in automatic mode, run the **voice-vlan enable** command to enable the voice VLAN function and run the **voice-vlan remark-mode mac-address** command to increase the priority of voice packets based on MAC addresses.

In auto mode, access, negotiation-auto, or negotiation-desirable interfaces cannot be added to a voice VLAN. To add the interface to the voice VLAN, run the **port link-type** command to change the link type of the interface to trunk or hybrid.

Precautions

The working mode of the voice VLAN on an interface does not affect the working mode of the voice VLAN on another interface. That is, voice VLANs on different interfaces can adopt different working modes.

Example

# On GE0/0/1, configure the voice VLAN to work in manual mode.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] port link-type hybrid
[HUAWEI-GigabitEthernet0/0/1] voice-vlan 10 enable
[HUAWEI-GigabitEthernet0/0/1] voice-vlan remark-mode mac-address
[HUAWEI-GigabitEthernet0/0/1] voice-vlan mode manual
[HUAWEI-GigabitEthernet0/0/1] port hybrid tagged vlan 10
```

5.7.8 voice-vlan remark

Function

The **voice-vlan remark** command changes the 802.1p priority and DSCP value for a voice VLAN.

The **undo voice-vlan remark** command restores the 802.1p priority and DSCP value to their default values for a voice VLAN.

By default, the 802.1p priority and DSCP value for a voice VLAN are 6 and 46 respectively.

Format

voice-vlan remark { **8021p** *8021p-value* | **dscp** *dscp-value* } *

undo voice-vlan remark { **8021p** | **dscp** } *

Parameters

Parameter	Description	Value
8021p *8021p-value*	Specifies the 802.1p priority. The 802.1p priority is indicated by the value in the 3-bit PRI field in each 802.1Q VLAN frame. This field determines the transmission priority for data packets when a switching device is congested.	The value is an integer that ranges from 0 to 7. The default value 6. The larger the value, the higher the priority.

Parameter	Description	Value
dscp *dscp-value*	Specify the DSCP value. The DSCP value is indicated by the 6 bits in the ToS field in the IPv4 packet header. DSCP, as the signaling for DiffServ, is used for QoS guarantee on IP networks. The traffic controller on the network gateway takes actions merely based on the information carried by the 6 bits.	The value is an integer that ranges from 0 to 63. The default value is 46.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When voice VLAN is deployed on a network, voice service must be transmitted with a shorter delay than data service. Therefore, voice data packets need to be transmitted with a higher priority than other service data packets to reduce the transmission delay. You can run the **voice-vlan remark** command to change the 802.1p and DSCP priorities of a voice VLAN to allow voice data packets to be transmitted with a high priority.

Precautions

The **voice-vlan** *vlan-id* **enable** command has been run on an interface to specify a VLAN as a voice VLAN, and the voice VLAN function has been enabled on the interface.

If the **voice-vlan remark** command has been run multiple times, the last configuration overrides the previous configurations.

When the **remark** and **voice-vlan remark** commands are used together to modify the user packet priority, if the services conflict:

- For S5731-H, S5731S-H, S5731-S, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S, the priority configured using the **remark** command takes effect.
- For S6720-EI, S6720S-EI, the priority configured using the **voice-vlan remark** command takes effect.

Example

# Set the DSCP value for a voice VLAN to 20.

```
<HUAWEI> system-view
[HUAWEI] voice-vlan remark dscp 20
```

5.7.9 voice-vlan remark-mode

Function

The **voice-vlan remark-mode** command configures a mode to increase the priority of voice packets.

The **undo voice-vlan remark-mode** command restores the default configuration.

By default, the priority of voice packets is increased based on VLAN IDs.

Format

voice-vlan remark-mode { **vlan** | **mac-address** }

undo voice-vlan remark-mode

Parameters

Parameter	Description	Value
vlan	Specifies that the priority of voice packets is increased based on VLAN IDs.	-
mac-address	Specifies that the priority of voice packets is increased based on MAC addresses.	-

Views

Ethernet interface view, GE interface view, XGE interface view, 40GE interface view, 100GE interface view, MultiGE interface view, Eth-Trunk interface view, port group view, 25GE interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After voice VLAN is enabled on an interface, the device determines whether a data flow consists of voice packets based on the VLAN ID by default. In this situation, even if you do not run the **voice-vlan mac-address** command to configure the OUI of the voice VLAN, you can use the voice VLAN function. Therefore, the voice VLAN configuration is more flexible and simple. Specifically, you can configure voice VLAN in the following methods:

- If you want to increase the priority of voice packets based on MAC addresses, run the **voice-vlan remark-mode mac-address** and **voice-vlan mac-address** commands.
- If you want to increase the priority of voice packets based on VLAN IDs, run the **voice-vlan remark-mode vlan** command.

Prerequisites

Voice VLAN has been enabled on the interface using the **voice-vlan enable** command.

Example

# Configure GE0/0/1 to increase the priority of voice packets based on MAC addresses.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] voice-vlan remark-mode mac-address
```

5.7.10 voice-vlan security enable

Function

The **voice-vlan security enable** command enables the secure mode of the voice VLAN.

The **undo voice-vlan security enable** command disables the secure mode of the voice VLAN.

By default, the secure mode of the voice VLAN is disabled.

Format

voice-vlan security enable

undo voice-vlan security enable

Parameters

None

Views

Ethernet interface view, GE interface view, XGE interface view, 40GE interface view, 100GE interface view, MultiGE interface view, Eth-Trunk interface view, port group view, 25GE interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Based on the data filtering mechanism, a voice VLAN works in either secure or normal mode:

- Secure mode

  A voice VLAN-enabled inbound port transmits only frames of which the source MAC addresses match OUIs configured on the device, discards the voice data not belong to the current voice VLAN and the other data can be forwarded normally.

The secure mode prevents a voice VLAN from being attacked by malicious data flows, but consumes system resources to check frames.

NOTE

The secure mode takes effect only when the **voice-vlan remark-mode mac-address** command is configured to increase the priority of voice packets based on MAC addresses.

- Normal mode

  A voice VLAN-enabled inbound port transmits both voice and non-voice data. The port does not compare source MAC addresses in received frames with configured OUIs, exposing a voice VLAN to malicious attacks.

Pre-configuration Tasks

Voice VLAN has been enabled using the **voice-vlan enable** command.

Run the **voice-vlan remark-mode mac-address** command to increase the priority of voice packets based on MAC addresses.

Precautions

When a voice VLAN works in secure mode, only voice packets in the VLAN can be transmitted in the voice VLAN.

To allow both voice packets and data packets to be transmitted in the voice VLAN, configure the voice VLAN to work in normal mode.

Example

# Disable the secure mode of the voice VLAN on GigabitEthernet 0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] voice-vlan remark-mode mac-address
[HUAWEI-GigabitEthernet0/0/1] undo voice-vlan security enable
```

5.8 QinQ Configuration Commands

5.8.1 Command Support

Commands provided in this section and all the parameters in the commands are supported by all switch models (except the S5731-L and S5731S-L), unless otherwise specified. For details, see specific commands.

5.8.2 add-tag vlan-id

Function

The **add-tag vlan-id** command configures an action of adding an outer VLAN tag in a traffic behavior.

The **undo add-tag** command deletes the action.

By default, no action of adding an outer VLAN tag is configured in a traffic behavior.

NOTE

Only the S5735S-H, S5736-S, and S6720S-S support this command.

Format

add-tag vlan-id *vlan-id*

undo add-tag

Parameters

Parameter	Description	Value
vlan-id	Specifies the VLAN ID in the outer VLAN tag.	The value is an integer that ranges from 1 to 4094.

Views

Traffic behavior view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the downstream device needs to provide services based on the outer VLAN tag, run the **add-tag vlan-id** command to configure the device to add an outer VLAN tag to packets matching the traffic classifier.

Follow-up Procedure

Run the **traffic policy** command to create a traffic policy and run the **classifier behavior** command in the traffic policy view to bind the traffic classifier to the traffic behavior containing the action of adding an outer VLAN tag.

Precautions

- After the **add-tag vlan-id**, **remark 8021p**, **remark cvlan-id** or **remark vlan-id** command is used, the system modifies the VLAN tag of packets according to its configuration. The behavior configured through these commands is called VLAN-based action.

  To apply a VLAN-based action and a non-VLAN-based action to the same upstream traffic policy, configure the VLAN-based action and non-VLAN-based action in different traffic behaviors bound to the same traffic policy.
- In the scenario where a traffic policy is bound to multiple pairs of traffic classifiers and traffic behaviors, a traffic behavior contains **add-tag vlan-id**,

and a traffic classifier bound to another traffic behavior that does not define any VLAN-specific actions defines **if-match vlan-id**, the VLAN ID specified by **add-tag vlan-id** is matched. If another traffic behavior defines **if-match cvlan-id**, the VLAN ID in the packets is matched.

- The **add-tag vlan-id** command is invalid for double-tagged VLAN packets.
- When **port vlan-stacking**, **port vlan-stacking untagged**, or **port link-type dot1q-tunnel** is configured on an interface to add a VLAN tag to packets so that packets carry double VLAN tags, the **add-tag vlan-id** command is invalid for the double-tagged VLAN packets.
- If you run the **add-tag vlan-id** command in the same traffic classifier view multiple times, only the latest configuration takes effect.

Example

# Configure an action of adding an outer VLAN tag for traffic behavior **tb** to 100.

```
<HUAWEI> system-view
[HUAWEI] traffic behavior tb
[HUAWEI-behavior-tb] add-tag vlan-id 100
```

5.8.3 display spare-bucket resource

Function

The **display spare-bucket resource** command displays the usage of backup resources when VLAN translation resources conflict.

Format

display spare-bucket resource [**slot** *slot-number*]

NOTE

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

Parameters

Parameter	Description	Value
slot *slot-number*	Specifies the slot ID where the usage of backup resources is displayed.	The value is an integer and must be the ID of an existing slot on the device.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The command displays the usage of backup VLAN translation resources, including the total number of backup VLAN translation resources, and the numbers of used and remaining backup VLAN translation resources. The command output helps you manage backup VLAN translation resources and locate the problem of ineffective VLAN mapping due to insufficient resources.

When no slot ID is specified, the usage of backup VLAN translation resources in all slots is displayed.

Example

# Display the usage of backup VLAN translation resources in slot 0.

```
<HUAWEI> display spare-bucket resource slot 0
----------------------------------------------------------
 Slot            Used         Free         Total
----------------------------------------------------------
 0               0            66           66
```

Table 5-59 Description of the **display spare-bucket resource** command output

Item	Description
Slot	Slot ID
Used	Number of used backup VLAN translation resources.
Free	Number of remaining backup VLAN translation resources.
Total	Total number of backup VLAN translation resources.

5.8.4 display vlan-translation resource

Function

The **display vlan-translation resource** command displays VLAN translation resource usage.

Format

display vlan-translation resource [**slot** *slot-number*]

NOTE

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

Parameters

Parameter	Description	Value
slot *slot-number*	Displays VLAN translation resource usage in a specified slot.	The value is an integer and must be an existing slot on the device.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

The **display vlan-translation resource** command displays VLAN translation resource usage, including the total number of inbound/outbound VLAN translation resources, the number of used VLAN translation resources, and the number of remaining VLAN translation resources. The command output helps you manage VLAN translation resources, and locate faults of insufficient VLAN translation resources caused by VLAN Mapping or Selective QinQ.

Example

# Display VLAN translation resource usage.

```
<HUAWEI> display vlan-translation resource slot 0
 Interface:
   GigabitEthernet0/0/1 to GigabitEthernet0/0/48
-------------------------------------------------
 Type      Total      Configured      Remaining
-------------------------------------------------
 Ingress   65536      0               65536
 Egress    65536      0               65536
```

Table 5-60 Description of the display vlan-translation resource command output

Item	Description
Interface	Interface where VLAN translation is performed.
Type	VLAN translation resource type, which can be **Ingress** or **Egress**.
Total	Total number of VLAN translation resources.
Configured	Number of used VLAN translation resources.
Remaining	Number of remaining VLAN translation resources.

5.8.5 port add-tag acl

Function

The **port add-tag acl** command adds an outer tag to the packet that matches an ACL rule on an interface.

The **undo port add-tag acl** command cancels the configuration.

By default, the device does not add an outer tag to the packet that matches an ACL rule.

NOTE

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

Format

port add-tag acl { *acl-number* | **name** *acl-name* } [**rule** *rule-id*] **vlan** *vlan-id* { **priority-inherit** | **remark-8021p** *8021p-value* }

undo port add-tag acl { *acl-number* | **name** *acl-name* } [**rule** *rule-id*]

If both Layer 2 ACLs and Layer 3 ACLs are configured, use the following command:

port add-tag acl *l2-acl* [**rule** *rule-id*] [**acl** { *basic-acl* | *advance-acl* | **name** *acl-name* } [**rule** *rule-id*]] **vlan** *vlan-id* { **priority-inherit** | **remark-8021p** *8021p-value* }

port add-tag acl { *basic-acl* | *advance-acl* } [**rule** *rule-id*] [**acl** { *l2-acl* | **name** *acl-name* } [**rule** *rule-id*]] **vlan** *vlan-id* { **remark-8021p** *8021p-value* | **priority-inherit** }

port add-tag acl name *acl-name* [**rule** *rule-id*] [**acl** { *basic-acl* | *advance-acl* | *l2-acl* | **name** *acl-name* } [**rule** *rule-id*]] **vlan** *vlan-id* { **remark-8021p** *8021p-value* | **priority-inherit** }

undo port add-tag acl *l2-acl* [**rule** *rule-id*] [**acl** { *basic-acl* | *advance-acl* | **name** *acl-name* } [**rule** *rule-id*]]

undo port add-tag acl { *basic-acl* | *advance-acl* } [**rule** *rule-id*] [**acl** { *l2-acl* | **name** *acl-name* } [**rule** *rule-id*]]

undo port add-tag acl name *acl-name* [**rule** *rule-id*] [**acl** { *basic-acl* | *advance-acl* | *l2-acl* | **name** *acl-name* } [**rule** *rule-id*]]

Parameters

Parameter	Description	Value
acl-number	Specifies the number of an ACL.	The value is an integer that ranges from 2000 to 4999. The value ranges of different types of ACLs are as follows: ● The value of a basic ACL ranges from 2000 to 2999. ● The value of an advanced ACL ranges from 3000 to 3999. ● The value of a Layer 2 ACL ranges from 4000 to 4999.
rule-id	Specifies the ID of an ACL rule.	The value of an IPv4 ACL ranges from 0 to 4294967294. ● When the rule ID is specified and the rule associated with the rule ID exists, the new rule takes effect. ● If the rule associated with the rule ID does not exist, you can create a rule with a specified rule ID and add the rule according to the rule ID. **NOTE** The number of ACL rules assigned automatically by the device starts from the step. The default step is 5. With this step, the device creates ACL rules with the numbers of 5, 10, 15, and so on.
name *acl-name*	Specifies a named ACL.	The value must the name of an existing ACL.
vlan *vlan-id*	Specifies a VLAN ID.	The value is an integer that ranges from 1 to 4094.

Parameter	Description	Value
l2-acl	Specifies the number of a Layer 2 ACL.	The value is an integer that ranges from 4000 to 4999.
basic-acl	Specifies the number of a basic ACL.	The value is an integer that ranges from 2000 to 2999.
advance-acl	Specifies the number of an advance ACL.	The value is an integer that ranges from 3000 to 3999.
priority-inherit	Indicates that the outer VLAN tag inherits the priority in the inner VLAN tag.	-
remark-8021p *8021p-value*	Specifies the re-marked priority of the added outer VLAN tag. *8021p-value* specifies the 802.1p priority.	The value is an integer that ranges from 0 to 7. A larger value indicates a higher priority.

Views

Ethernet interface view, GE interface view, XGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, MultiGEinterface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A device interface adds the specified outer tag to a packet based on the VLAN tag, MAC address, IP protocol, source address, destination address, priority, or port number of an application of a user.

Precautions

- After you run the **port add-tag acl** command, the following situations may occur:
  - The device does not take the original forwarding action to forward the packet that matches an ACL rule. Instead, the device adds an outer tag to the packet and forwards the packet in the VLAN specified by the added outer tag.
  - The device adds an outer tag to the packet that does not match an ACL rule based on the default VLAN of an interface.

- A Layer 2 ACL and a Layer 3 ACL can be set in the **port add-tag acl** command simultaneously. The Layer 3 ACL and its rules can be configured only after the Layer 2 ACL and its rules are configured. The Layer 2 ACL number ranges from 4000 to 4999 and the Layer 3 ACL number ranges from 2000 to 2999 and 3000 to 3999.
- This command is invalid for packets tagged with VLAN 0. If packets tagged with VLAN 0 need to be processed, configure a traffic policy on the switch.
- For the S6735-S, The **port add-tag acl** command is invalid for double-tagged VLAN packets.

Example

# Add the outer tag of VLAN 1001 to the packet that matches the source IP address of 192.168.0.0/16 on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] acl name test 2000
[HUAWEI-acl-basic-test] rule 1 permit source 192.168.0.0 0.0.255.255
[HUAWEI-acl-basic-test] quit
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] port link-type trunk
[HUAWEI-GigabitEthernet0/0/1] port trunk allow-pass vlan all
[HUAWEI-GigabitEthernet0/0/1] port add-tag acl 2000 rule 1 vlan 1001 priority-inherit
```

5.8.6 port vlan-stacking

Function

The **port vlan-stacking** command configures VLAN stacking.

The **undo port vlan-stacking** command cancels the configuration.

By default, VLAN stacking is not configured.

Format

port vlan-stacking vlan *vlan-id1* [**to** *vlan-id2*] **stack-vlan** *vlan-id3* [**remark-8021p** *8021p-value1*]

port vlan-stacking vlan *vlan-id1* **stack-vlan** *vlan-id3* [**remark-8021p** *8021p-value1*] **map-vlan** *vlan-id4* [**remark-inner-8021p** *8021p-value2*]

undo port vlan-stacking vlan *vlan-id1* [**to** *vlan-id2*] [**stack-vlan** *vlan-id3*]

undo port vlan-stacking all

Parameters

Parameter	Description	Value
vlan *vlan-id1* [**to** *vlan-id2*]	Specifies the VLAN ID in a received tagged frame. ● *vlan-id1* specifies the start VLAN ID. ● **to** *vlan-id2* specifies the end VLAN ID. The value of *vlan-id2* must be larger than the value of *vlan-id1*. *vlan-id1* and *vlan-id2* identify a VLAN range.	The value of *vlan-id1* is an integer that ranges from 1 to 4094. The value of *vlan-id2* is an integer that ranges from 1 to 4094.
stack-vlan *vlan-id3*	Specifies the outer VLAN ID added to a frame.	The value is an integer that ranges from 1 to 4094.
remark-8021p *8021p-value1*	Specifies the re-marked 802.1p priority in the outer tag added to a frame.	The value is an integer that ranges from 0 to 7. A larger value indicates a higher priority.
map-vlan *vlan-id4*	Specifies the mapped VLAN ID in the stacked inner tag.	The value is an integer that ranges from 1 to 4094.
remark-inner-8021p *8021p-value2*	Specifies the re-marked 802.1p priority in the mapped inner tag.	The value is an integer that ranges from 0 to 7. A larger value indicates a higher priority.
all	Deletes all VLAN stacking configurations on the interface.	-

Views

Ethernet interface view, GE interface view, XGE interface view, 40GE interface view, 100GE interface view, MultiGE interface view, Eth-Trunk interface view, port group view, 25GE interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

VLAN stacking, also called selective QinQ, is a Layer 2 technology that enables a device to add outer VLAN tags based on VLAN IDs.

When frames are transmitted on the ISP network, the frames are differentiated based on user applications, access sites, or access devices. A device enabled with VLAN stacking adds outer tags to user frames based on the inner tags or priorities in the user frames so that traffic from different users are differentiated. A VLAN stacking interface has the following features:

- A VLAN stacking port can be configured with multiple outer VLAN tags so that the port can add different outer VLAN tags to different VLAN frames.
- A VLAN stacking interface can add the outer tag to received frames. After an interface joins the stacked VLAN in untagged mode, the interface removes the outer tag from outgoing frames.

When a network edge device needs to act as a user-side device and the received single-tagged packets are from one type of service, the same service from different users needs to be sent in different VLANs. That is, 1:1 VLAN mapping is implemented. After mapped VLAN tags enter the carrier network, VLAN stacking needs to be enabled on the network edge device to distinguish different users and services, because the number of VLANs that can be provided by the carrier network is limited. In addition, specified tags need to be added to packets of different users and services. Outer tags are the same as those provided by the carrier network and can be transmitted over the carrier network, and inner tags are transparently transmitted over the carrier network, enabling communication between different users. You need to run the **port vlan-stackingvlan***vlan-id1***stack-vlan***vlan-id2* [**remark-8021p***8021p-value1*] **map-vlan***vlan-id4* [**remark-inner-8021p***8021p-value2*] command to enable both VLAN mapping and VLAN stacking functions. **remark-8021p***8021p-value1* and **remark-inner-8021p***8021p-value2* specify 802.1p priorities of inner and outer VLAN tags.

If you want to implement both VLAN mapping and VLAN stacking, you cannot enable them separately by running the corresponding commands. This is because the VLAN ID that is mapped based on VLAN mapping cannot be mapped again based on VLAN stacking. For example, if **port vlan-stacking vlan 210 stack-vlan 2010** and **port vlan-mapping vlan 10 map-vlan 210** are configured on a device, the device maps VLAN 10 to VLAN 210 based on **port vlan-mapping vlan 10 map-vlan 210**. However, VLAN 210 after mapping will not be mapped to VLAN 2010 based on **port vlan-stacking vlan 210 stack-vlan 2010**. To implement both VLAN stacking and VLAN mapping, run the **port vlan-stacking vlan***vlanid1***stack-vlan***vlanid2***map-vlan***vlanid3* command.

When **remark-8021p** *8021p-value* is not specified:

- On the SS1720GW-E, S1720GWR-E, S5720I-SI, S5720-LI, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5720S-LI, S5735-S, S500, S5735S-S, S5735-S-I, S5735S-H, S5736-S, and S6720S-S, the 802.1p priority in the outer VLAN tag is the same as the interface priority. If **trust 8021p** is configured on the interface, the 802.1p priority in the outer VLAN tag is the same as the 802.1p priority in the inner VLAN tag.
- On other models, the 802.1p priority in the outer VLAN tag is the same as the 802.1p priority in the inner VLAN tag.

Precautions

When you configure selective QinQ, note the following points:

- Selective QinQ is recommended to be enabled on a hybrid interface. Selective QinQ can take effect on the interface only in the inbound direction.
- The outer VLAN must be created before VLAN stacking is performed.
- When an interface configured with VLAN stacking needs to remove the outer tag from outgoing frames, the interface must join the VLAN specified by **stack-vlan** in untagged mode. If the outer VLAN does not need to be removed, the interface must join the VLAN specified by **stack-vlan** in tagged mode.
- When **map-vlan** *vlan-id4* is configured to perform VLAN stacking and VLAN mapping concurrently, on switches other than the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S, the same outer VLAN tag cannot be added to packets from different user VLANs. On the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S, the same outer VLAN tag cannot be added to packets from different user VLANs, and different inner VLAN tags in packets from different user VLANs cannot be matched to the same VLAN tag. For example, if packets containing VLAN IDs 10 and 20 respectively are received on an interface, the **port vlan-stacking vlan 10 stack-vlan 100 map-vlan 200** and **port vlan-stacking vlan 20 stack-vlan 100 map-vlan 200** commands cannot be configured together.
- On the S6735-S, the **qinq protocol** and **port vlan-stacking** commands cannot be run simultaneously on an interface.
- On the S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735-S-I, and S5735S-S, after the **port vlan-stacking** command is run on an interface, IP packets cannot be forwarded on the interface.
- On the S6735-S, after the **port vlan-stacking** command is run on an interface, the inner VLAN tag of packets is not removed and the outer VLAN tag is replaced during Layer 3 forwarding.

Example

# On GE0/0/1, configure selective QinQ and outer VLAN tag 100 to the tagged frames with the inner VLAN tags 10 to 13.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] port link-type hybrid
[HUAWEI-GigabitEthernet0/0/1] qinq vlan-translation enable
[HUAWEI-GigabitEthernet0/0/1] port hybrid untagged vlan 100
[HUAWEI-GigabitEthernet0/0/1] port vlan-stacking vlan 10 to 13 stack-vlan 100
```

5.8.7 port vlan-stacking untagged

Function

The **port vlan-stacking untagged** command configures a device to add double VLAN tags to an untagged frame.

The **undo port vlan-stacking untagged** command cancels the configuration.

By default, the device does not add double tags to an untagged frame.

Format

port vlan-stacking untagged stack-vlan *vlan-id1* **stack-inner-vlan** *vlan-id2*

undo port vlan-stacking untagged

Parameters

Parameter	Description	Value
stack-vlan *vlan-id1*	Specifies the outer VLAN tag added to an untagged frame.	The value of *vlan-id1* is an integer that ranges from 1 to 4094.
stack-inner-vlan *vlan-id2*	Specifies the inner VLAN tag added to an untagged frame.	The value of *vlan-id2* is an integer that ranges from 1 to 4094.

Views

Ethernet interface view, GE interface view, XGE interface view, 40GE interface view, 100GE interface view, MultiGE interface view, Eth-Trunk interface view, port group view, 25GE interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If double tags need to be added to packets, two devices are required. The **port vlan-stacking untagged** command adds double tags to packets on one device or untagged packets received on a Layer 2 interface to differentiate services or users.

For outgoing packets:

- S5720I-SI, S5720-LI, S5720S-LI, S5735S-H, S5736-S, and S6720S-S:
  - Double-tagged packets: The switch removes tags, as long as the outer VLAN ID is matched (regardless of whether the inner VLAN ID is matched).
  - Single-tagged packets: If QinQ (doltq or VLAN stacking) is configured on the inbound interface and the outer VLAN ID in QinQ is the same as the outer VLAN ID specified by the **port vlan-stacking untagged stack-vlan** *vlan-id1* **stack-inner-vlan** *vlan-id2* command, the VLAN ID of outgoing packets is the VLAN ID of original packets.
- Other models: When only the outer VLAN ID is matched and the VLAN is configured on the interface in untagged mode, the outer VLAN tag is removed and the inner VLAN tag is reserved.

Precautions

To enable an interface to add double VLAN tags to an untagged packet, you need to set the link type of the interface to hybrid, and add the interface to the VLAN specified by **stack-vlan** on the S6720S-S, S5735S-H, S5736-S, S5720S-LI, S5720-LI, S5720I-SI. On other devices, you need to set the link type of the interface to hybrid or trunk, and add the interface to the VLAN specified by **stack-vlan**.

When the interface PVID is not VLAN 1, restore the PVID to VLAN 1 before the **port vlan-stacking untagged** command is executed.

Adding double VLAN tags to untagged frames is port-based VLAN assignment. Different VLAN assignment modes are in the following order of priority: policy-based VLAN assignment > MAC address-based VLAN assignment > IP subnet-based VLAN assignment > protocol-based VLAN assignment > interface-based VLAN assignment.

On the S5720I-SI, S5720-LI, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5720S-LI, S5735-S, S500, S5735S-S, S5735-S-I, S5735S-H, S5736-S, and S6720S-S if the **port vlan-stacking untagged** *vlan-id1* **stack-inner-vlan** *vlan-id2* command is used on an interface, the VLAN specified by *vlan-id1* cannot be configured as the outer VLAN in the **port vlan-stacking** command.

If the **port vlan-stacking untagged** command is used on an interface, the interface processes the received packets with VLAN tag 0 as untagged packets.

Example

# Add double VLAN tags to untagged frames received on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] port link-type hybrid
 [HUAWEI-GigabitEthernet0/0/1] qinq vlan-translation enable
 [HUAWEI-GigabitEthernet0/0/1] port hybrid untagged vlan 100
[HUAWEI-GigabitEthernet0/0/1] port vlan-stacking untagged stack-vlan 100 stack-inner-vlan 200
```

5.8.8 qinq mapping pe-vid ce-vid

Function

The **qinq mapping pe-vid ce-vid** command configures a sub-interface to map the outer VLAN tag of a frame.

The **undo qinq mapping pe-vid ce-vid** command cancels the configuration.

By default, VLAN mapping is not configured on a sub-interface.

Format

qinq mapping pe-vid *vlan-id1* **ce-vid** *vlan-id2* [**to** *vlan-id3*] **map-vlan vid** *vlan-id4*

undo qinq mapping pe-vid *vlan-id1* **ce-vid** *vlan-id2* [**to** *vlan-id3*] **map-vlan vid** *vlan-id4*

NOTE

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

Parameters

Parameter	Description	Value
pe-vid *vlan-id1*	Specifies the outer VLAN tag in a received frame.	The value is an integer that ranges from 2 to 4094.
ce-vid *vlan-id2* [**to** *vlan-id3*]	Specifies the inner VLAN tag in a received frame. ● *vlan-id2*: specifies the start inner VLAN tag. ● *vlan-id3*: specifies the end inner VLAN tag. ● The value of *vlan-id3* must be greater than or equal to the value of *vlan-id2*. *vlan-id2* and *vlan-id3* identify a VLAN range.	The value of *vlan-id2* is an integer that ranges from 1 to 4094. The value of *vlan-id3* is an integer that ranges from 1 to 4094.
map-vlan vid *vlan-id4*	Specifies the VLAN ID in the mapped outer tag.	The value is an integer that ranges from 1 to 4094.

Views

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

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

QinQ mapping is generally deployed on edge devices of a metro Ethernet and often used to map the VLAN tag carried in a frame to a specified VLAN tag before the frame is transmitted on the public network. QinQ mapping can be applied to the following scenarios:

- The VLAN IDs deployed in new sites and old sites conflict, but new sites need to communicate with old sites.
- The VLAN ID planning of each site on the public network is different. As a result, the VLAN IDs conflict. However, the sites do not need to communicate.

- The VLAN IDs on both ends of the public network are different.

When a network edge device receives double-tagged frames, the inner tags indicate users and outer tags indicates services. To differentiate services on the ISP network, you can configure 2 to 1 QinQ mapping on network edge devices. The double tags of frames are mapped to a specified S-VLAN tag so that the outer tag can be transparently transmitted on the ISP network.

The **qinq mapping pe-vid ce-vid** command on a sub-interface has similar functions with the **port vlan-mapping vlan inner-vlan** command on the main interface. The differences are as follows:

- QinQ mapping on a sub-interface is mainly used to access the L2VPN.
- QinQ mapping used on the main interface is used for interconnection on the Layer 2 MAN so that users of different VLANs can communicate with each other.
- QinQ mapping saves a large number of physical ports.

Precautions

The **qinq mapping pe-vid ce-vid** command maps the outer VLAN tags of the frames on a sub-interface, but does not change the inner VLAN tags. This command takes effect for only incoming frames.

The original VLAN IDs specified for QinQ mapping on a sub-interface cannot be globally created or displayed by display commands.

VLAN mapping or VLAN stacking cannot be configured for the same VLAN on the main interface and its sub-interfaces.

The mapped VLAN IDs specified in QinQ mapping configuration must be different from the control VLAN IDs for ring protocols such as SEP, RRPP, and ERPS. Otherwise, an error message will be displayed, indicating that the configuration fails.

Example

# On XGigabitEthernet0/0/1.1, set the outer VLAN tag 10 of frames with the inner VLAN tag 20 to outer VLAN tag 30.

```
<HUAWEI> system-view
[HUAWEI] vcmp role silent
[HUAWEI] interface xgigabitethernet 0/0/1
[HUAWEI-XGigabitEthernet0/0/1] port link-type hybrid
[HUAWEI-XGigabitEthernet0/0/1] quit
[HUAWEI] interface xgigabitethernet 0/0/1.1
[HUAWEI-XGigabitEthernet0/0/1.1] qinq mapping pe-vid 10 ce-vid 20 map-vlan vid 30
```

5.8.9 qinq mapping vid map-vlan

Function

The **qinq mapping vid map-vlan** command configures 1 to 1 QinQ mapping on a sub-interface.

The **undo qinq mapping vid map-vlan** command cancels the configuration.

By default, 1 to 1 QinQ mapping is not configured on a sub-interface.

Format

qinq mapping vid *vlan-id1* [**to** *vlan-id2*] **map-vlan vid** *vlan-id3*

undo qinq mapping vid *vlan-id1* [**to** *vlan-id2*] **map-vlan vid** *vlan-id3*

NOTE

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

Parameters

Parameter	Description	Value
vid *vlan-id1* **to** *vlan-id2*	Specifies the VLAN ID of the tag carried in the received packet. ● *vlan-id1*: specifies the start inner VLAN tag. ● *vlan-id2*: specifies the end inner VLAN tag. ● The value of *vlan-id2* must be greater than or equal to the value of *vlan-id1*. *vlan-id1* and *vlan-id2* identify a VLAN range.	*vlan-id1* is an integer that ranges from 2 to 4094. *vlan-id2* is an integer that ranges from 2 to 4094.
map-vlan vid *vlan-id3*	Specifies the VLAN ID in the mapped outer tag.	The value is an integer that ranges from 1 to 4094.

Views

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

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

QinQ mapping is often deployed on edge devices of a metro Ethernet and is used to map the frames sent from the user side. The devices map the VLAN IDs in user packets to specified VLAN IDs before forwarding the packets to the public network. QinQ mapping can be applied to the following scenarios:

- The VLAN IDs deployed in new sites and old sites conflict, but new sites need to communicate with old sites.

- The VLAN ID planning of each site on the public network is different. As a result, the VLAN IDs conflict. However, the sites do not need to communicate.
- The VLAN IDs on both ends of the public network are different.

The **qinq mapping vid map-vlan** command on a sub-interface has similar functions with the **port vlan-mapping vlan inner-vlan** command on the main interface. The differences are as follows:

- QinQ mapping on a sub-interface is mainly used to access the L2VPN.
- QinQ mapping used on the main interface is used for interconnection on the Layer 2 MAN so that users of different VLANs can communicate with each other.
- QinQ mapping saves a large number of physical ports.

Precautions

The **qinq mapping vid map-vlan** command maps the single tags in frames on a sub-interface. This command takes effect only for incoming packets.

The original VLAN IDs specified for QinQ mapping on a sub-interface cannot be globally created or displayed by display commands.

VLAN mapping or VLAN stacking cannot be configured for the same VLAN on the main interface and its sub-interfaces.

The mapped VLAN IDs specified in QinQ mapping configuration must be different from the control VLAN IDs for ring protocols such as SEP, RRPP, and ERPS. Otherwise, an error message will be displayed, indicating that the configuration fails.

Example

# Configure QinQ mapping on XGigabitEthernet0/0/1.1 to map outer VLAN tag 100 to inner VLAN tag 200.

```
<HUAWEI> system-view
[HUAWEI] vcmp role silent
[HUAWEI] interface xgigabitethernet 0/0/1
[HUAWEI-XGigabitEthernet0/0/1] port link-type hybrid
[HUAWEI-XGigabitEthernet0/0/1] quit
[HUAWEI] interface xgigabitethernet 0/0/1.1
[HUAWEI-XGigabitEthernet0/0/1.1] qinq mapping vid 100 map-vlan vid 200
```

5.8.10 qinq protocol

Function

The **qinq protocol** command sets the TPID value in the outer VLAN tag of an interface.

The **undo qinq protocol** command restores the default TPID value in the outer VLAN tag.

By default, the TPID value in the outer VLAN tag is 0x8100.

Format

qinq protocol *protocol-id*

undo qinq protocol

Parameters

Parameter	Description	Value
protocol-id	Specifies the TPID value in the outer VLAN tag.	The value is a 4-digit hexadecimal integer that ranges from 0x0600 to 0xFFFF. The default TPID value is 0x8100.

Views

Ethernet interface view, GE interface view, XGE interface view, 40GE interface view, 100GE interface view, MultiGE interface view, Eth-Trunk interface view, 25GE interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To enable devices from different vendors to interoperate, set the same TPID value in outer VLAN tags on the devices. Devices from different vendors or in different network plans may use different Tag Protocol Identifier (TPID) values in VLAN tags of VLAN packets. The switch supports configuration of the TPID value in outer VLAN tags so that it can interoperate with devices from different vendors or operate seamlessly on an existing network.

Precautions

- In earlier versions of V200R010, this command can be configured on Eth-Trunk member interfaces but not the Eth-Trunk. In V200R010 and later versions, this command can be configured on the Eth-Trunk but not Eth-Trunk member interfaces.
- When the device is upgraded from an earlier version of V200R010 to V200R010 or later and the **qinq protocol** command is configured on Eth-Trunk member interfaces, the following situations may occur:
  - If the same **qinq protocol** command has been configured on all Eth-Trunk member interfaces, the **qinq protocol** command configuration takes effect on the Eth-Trunk after the upgrade.
  - If different **qinq protocol** commands are configured on Eth-Trunk member interfaces, the **qinq protocol** command configuration takes effect on the Eth-Trunk member interfaces after the upgrade and there is the configuration on the Eth-Trunk member interfaces. To configure the **qinq protocol** command in the Eth-Trunk interface view, first manually run the **undo qinq protocol** command on Eth-Trunk member interfaces to delete the configuration. In this situation, automatic completion of the

undo qinq protocol command is not supported. You must manually enter the **undo qinq protocol** command.

- The device directly connected to an interface must be able to identify the TPID value in the outer VLAN tag on the interface.
- On the S6735-S, the **qinq protocol** and **port vlan-stacking** commands cannot be run simultaneously on an interface.
- The **qinq protocol** command identifies incoming frames, and adds or changes the TPID value of outgoing frames.
- The **qinq protocol** command can also change the TPID value in the VLAN tag of a single-tagged packet.
- The TPID value specified by the **qinq protocol** command must be different from TPID values of specific protocols. Otherwise, the interface cannot correctly classify protocol packets. The TPID value cannot be any of the values in the following table.

Table 5-61 Description of protocol types and values

Protocol Type	Value
ARP	0x0806
RARP	0x8035
IP	0x0800
IPv6	0x86DD
PPPoE	0x8863/0x8864
MPLS	0x8847/0x8848
IPX/SPX	0x8137
LACP	0x8809
802.1x	0x888E
HGMP	0x88A7
Reserved	0xFFFD/0xFFFE/0xFFFF

Example

# Set the TPID value in the outer VLAN tag of a QinQ frame to 0x9100 on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet0/0/1
[HUAWEI-GigabitEthernet0/0/1] qinq protocol 9100
```

5.8.11 qinq stacking

Function

The **qinq stacking** command configures VLAN stacking on a sub-interface.

The **undo qinq stacking** command cancels the configuration.

By default, VLAN stacking is not configured on a sub-interface.

Format

qinq stacking vid *vlan-id1* [**to** *vlan-id2*] **pe-vid** *vlan-id3*

undo qinq stacking vid *vlan-id1* [**to** *vlan-id2*] **pe-vid** *vlan-id3*

NOTE

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

Parameters

Parameter	Description	Value
vid *vlan-id1* [**to** *vlan-id2*]	Specifies the outer VLAN ID range. ● *vlan-id1* specifies the start VLAN ID. ● **to***vlan-id2* specifies the end VLAN ID. The *vlan-id1* and *vlan-id2* id value of *vlan-id2* must be greater than or equal to the value of *vlan-id1*entify a VLAN range.	The value of *vlan-id1* is an integer that ranges from 2 to 4094. The value of *vlan-id2* is an integer that ranges from 2 to 4094.
pe-vid *vlan-id3*	Specifies the outer VLAN tags added to a frame.	The value is an integer that ranges from 1 to 4094.

Views

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

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **qinq stacking** command adds an outer VLAN tag to the packets on a sub-interface.

Precautions

- The original VLAN IDs specified for QinQ mapping on a sub-interface cannot be globally created or displayed by display commands.
- VLAN mapping or VLAN stacking cannot be configured for the same VLAN on the main interface and its sub-interfaces.
- When a QinQ stacking sub-interface receives a packet, the interface checks whether the packet carries a VLAN tag. If not, the packet is directly dropped. If the packet carries one or two VLAN tags, the interface processes the packet as follows:
  - If the packet carries one VLAN tag and the VLAN ID in the tag matches the VLAN range specified by **vid** *vlan-id1* [**to** *vlan-id2*] in the **qinq stacking vid** command, the interface adds an outer VLAN tag with a VLAN ID in the specified range to the packet. If the VLAN ID in the tag carried by the packet does not match the specified VLAN range, the packet is dropped.
  - If the packet carries two VLAN tags and the VLAN ID in the outer VLAN tag matches the VLAN range specified by **vid** *vlan-id1* [**to** *vlan-id2*] in the **qinq stacking vid** command, the interface adds another outer VLAN tag with a VLAN ID in the specified range to the packet and forwards the packet. In this case, the inner VLAN tag is transmitted transparently. If the VLAN ID in the outer VLAN tag carried by the packet does not match the specified VLAN range, the packet is dropped.

Example

# Configure VLAN stacking on XGigabitEthernet0/0/1.1 and add an outer VLAN tag 100 to frames with the inner VLAN tags 10 to 13.

```
<HUAWEI> system-view
[HUAWEI] vcmp role silent
[HUAWEI] interface xgigabitethernet 0/0/1
[HUAWEI-XGigabitEthernet0/0/1] port link-type hybrid
[HUAWEI-XGigabitEthernet0/0/1] quit
[HUAWEI] interface xgigabitethernet 0/0/1.1
[HUAWEI-XGigabitEthernet0/0/1.1] qinq stacking vid 10 to 13 pe-vid 100
```

5.8.12 qinq stacking vlan

Function

The **qinq stacking vlan** command configures QinQ stacking on a VLANIF interface.

The **undo qinq stacking vlan** command cancels the configuration.

By default, QinQ stacking is not configured on a VLANIF interface.

Format

qinq stacking vlan *vlan-id*

undo qinq stacking vlan

Parameters

Parameter	Description	Value
vlan-id	Specifies the outer VLAN tag added to a frame.	The value is an integer that ranges from 1 to 4094.

Views

VLANIF interface view

Default Level

2: Configuration level

Usage Guidelines

Assume that the local device A is connected to the remote device B over the ISP network.

The ID of the management VLAN on device B is the same as the ID of VLAN for users connected to device A. However, the S-VLAN ID is different from the management VLAN ID.

To log in to device B to manage it from local device A, you can use the qinq stacking vlan command on device B to configure QinQ stacking on the VLANIF interface corresponding to the management VLAN. In addition, you need to configure QinQ on the user-side interface of device A.

- Packets sent from device A to device B are processed as follows:

  The user-side interface of device A sends double-tagged packets to the ISP network. The outer VLAN tag is assigned by the carrier so that the packets can be transparently transmitted over the ISP network to SwitchB.

  When device B receives double-tagged packets, it compares the VLAN tags of the packets with the VLAN tags configured on the VLANIF interface. If the outer tag of the packets is the same as the outer tag configured on the VLANIF interface, device B removes the outer tag and sends the packets to the IP layer for processing.

- Packets sent from device B to device A are processed as follows:

  When the VLANIF interface of SwitchB receives data packets, device B adds a VLAN tag to the packets according to the QinQ stacking configuration. The new outer VLAN tag is assigned by the carrier so that the double-tagged data packets can be transparently transmitted across the ISP network to device A. Device A removes the outer VLAN tag, and then forwards the packets to users.

NOTE

- When configuring QinQ stacking on a VLANIF interface, ensure that the VLANIF interface corresponds to the management VLAN. VLANIF interfaces corresponding to other VLANs do not support QinQ stacking.
- To change the configured outer VLAN, run the **undo qinq stacking vlan** command to disable QinQ stacking, and then run the **qinq stacking vlan** command to configure a new outer VLAN.
- The **qinq stacking vlan** command conflicts with the **icmp host-unreachable send** command. Therefore, you must run the **undo icmp host-unreachable send** command before using the **qinq stacking vlan** command.
- The outer VLAN added to packets must be an existing VLAN without VLANIF interface configured.

Example

# Configure QinQ stacking on VLANIF 10.

```
<HUAWEI> system-view
[HUAWEI] vlan 10
[HUAWEI-vlan10] management-vlan
[HUAWEI-vlan10] quit
[HUAWEI] interface vlanif 10
[HUAWEI-Vlanif10] undo icmp host-unreachable send
[HUAWEI-Vlanif10] qinq stacking vlan 20
```

5.8.13 qinq vlan-translation enable

Function

The **qinq vlan-translation enable** command enables VLAN translation on an interface.

The **undo qinq vlan-translation enable** command disables VLAN translation on an interface.

By default, VLAN translation is disabled on an interface.

Format

qinq vlan-translation enable

undo qinq vlan-translation enable

Parameters

None

Views

Ethernet interface view, GE interface view, XGE interface view, 40GE interface view, 100GE interface view, MultiGE interface view, Eth-Trunk interface view, port group view, 25GE interface view

Default Level

2: Configuration level

Usage Guidelines

You can configure VLAN mapping and selective QinQ on an interface only after VLAN translation is enabled on it.

Example

# Enable VLAN translation on GigabitEthernet0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] port link-type hybrid
[HUAWEI-GigabitEthernet0/0/1] qinq vlan-translation enable
```

5.8.14 qinq vlan-translation miss-drop

Function

The **qinq vlan-translation miss-drop** command configures an interface to discard the packets that do not match any VLAN Stacking, VLAN mapping, and entry.

The **undo qinq vlan-translation miss-drop** command cancels the configuration.

By default, an interface does not discard the packets that do not match any VLAN Stacking, VLAN mapping, and entry.

NOTE

This command does not take effect for untagged packets.

Format

qinq vlan-translation miss-drop

undo qinq vlan-translation miss-drop

Parameters

None

Views

Ethernet interface view, GE interface view, XGE interface view, 40GE interface view, 100GE interface view, MultiGE interface view, Eth-Trunk interface view, 25GE interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

After VLAN Stacking and VLAN mapping, are configured on an interface, you can run the **qinq vlan-translation miss-drop** command to configure the interface to discard the received packets that do not match any VLAN Stacking, VLAN mapping, and entry.

Example

# Configure GE0/0/1 to discard the packets that do not match any VLAN Stacking, VLAN mapping, and entry.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] port link-type hybrid
[HUAWEI-GigabitEthernet0/0/1] qinq vlan-translation enable
[HUAWEI-GigabitEthernet0/0/1] qinq vlan-translation miss-drop
```

5.9 VLAN Mapping Configuration Commands

5.9.1 Command Support

Table 5-62 Products supporting the function of VLAN mapping

VLAN Mapping Mode	Supported Model
1:1 mode for 1 to 1 VLAN mapping	All models.
N:1 mode for 1 to 1 VLAN mapping	S5720I-SI, S5720-LI, S5720S-LI, S5735S-H, S5736-S, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735-S, S500, S5735-S-I, S5735S-L, S5735S-L1, S5735S-L-M, S5735S-S, S6735-S, S6720-EI, S6720S-S, S6720S-EI, S6730-H, S6730-S, S6730S-S, S6730S-H, S5732-H, S5731-H, S5731S-H, S5731-S, and S5731S-S
1:1 mode for 2 to 1 VLAN mapping	S5735S-H, S5736-S, S5731-H, S5731-S, S5731S-S, S5731S-H, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6720S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S
N:1 mode for 2 to 1 VLAN mapping	S6735-S, S6720-EI, S6720S-S, S5736-S, S5735S-H S6720S-EI, S6730-H, S6730-S, S6730S-S, S6730S-H, S5732-H, S5731-H, S5731S-H, S5731-S, and S5731S-S
2 to 2	S5735S-H, S5736-S, S5731-H, S5731-S, S5731S-S, S5731S-H, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6720S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S

5.9.2 port vlan-mapping ingress

Function

The **port vlan-mapping ingress** command configures VLAN mapping in the inbound direction.

The **undo port vlan-mapping ingress** command cancels the configuration.

By default, VLAN mapping is valid for both inbound and outbound directions.

NOTE

This command is only supported by S1720GW-E, S1720GWR-E, S5720I-SI, S5720-LI, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5720S-LI, S5735-S, S500, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S6720S-S.

Format

port vlan-mapping ingress

undo port vlan-mapping ingress

Parameters

None

Views

Ethernet interface view, GE interface view, 40GE interface view, 100GE interface view, MultiGE interface view, Eth-Trunk interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the **port vlan-mapping vlan** *vlan-id1* [**to** *vlan-id2*] **map-vlan** *vlan-id3* [**remark-8021p** *8021p-value*] command is used on an interface, *vlan-id1* [**to** *vlan-id2*] is mapped to *vlan-id3* in the inbound direction, and *vlan-id3* is mapped to *vlan-id1* [**to** *vlan-id2*] in the outbound direction.

On the S1720GW-E, S1720GWR-E, S5720I-SI, S5720-LI, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5720S-LI, S5735-S, S500, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S6720S-S, outbound VLAN mapping cannot be used with a traffic policy containing CAR. You can run the **port vlan-mapping ingress** command to configure VLAN mapping in the inbound direction. The interface configured with VLAN mapping maps *vlan-id1* [**to** *vlan-id2*] to *vlan-id3* in the inbound direction, and does not map *vlan-id3* to *vlan-id1* [**to** *vlan-id2*] in the outbound direction.

Prerequisites

The **qinq vlan-translation enable** command has been executed.

Precautions

To make VLAN mapping take effect in the inbound direction only, configure the **port vlan-mapping ingress** and **port vlan-mapping vlan map-vlan** commands in sequence. To delete the VLAN mapping configuration, delete the **port vlan-mapping vlan map-vlan** and **port vlan-mapping ingress** commands in sequence.

Example

# Configure VLAN mapping in the inbound direction on GE0/0/1 to map VLAN 100 in received frames to VLAN 10.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet0/0/1
[HUAWEI-GigabitEthernet0/0/1] port link-type trunk
[HUAWEI-GigabitEthernet0/0/1] port trunk allow-pass vlan 10
[HUAWEI-GigabitEthernet0/0/1] qinq vlan-translation enable
[HUAWEI-GigabitEthernet0/0/1] port vlan-mapping ingress
[HUAWEI-GigabitEthernet0/0/1] port vlan-mapping vlan 100 map-vlan 10
```

5.9.3 port vlan-mapping vlan inner-vlan

Function

The **port vlan-mapping vlan inner-vlan** command enables the interface to replace the outer VLAN tag or both VLAN tags of a double-tagged packet.

The **undo port vlan-mapping vlan inner-vlan** command disables the interface to replace the outer VLAN tag or both VLAN tags of a double-tagged packet.

By default, the interface does not map tags of packets.

NOTE

Only the S6735-S, S6720-EI, S6720S-EI, S6720S-S, S5736-S, S5735S-H, S6730-H, S6730-S, S6730S-S, S6730S-H, S5732-H, S5731-H, S5731S-H, S5731-S, S5731S-S support this command.

Format

port vlan-mapping vlan *vlan-id1* **inner-vlan** *vlan-id2* [**to** *vlan-id3*] **map-vlan** *vlan-id4* [**remark-8021p** *8021p-value*]

port vlan-mapping vlan *vlan-id1* **inner-vlan** *vlan-id2* **map-vlan** *vlan-id4* [**map-inner-vlan** *vlan-id5*] [**remark-8021p** *8021p-value*]

undo port vlan-mapping { **all** | **vlan** *vlan-id1* **inner-vlan** *vlan-id2* [**to** *vlan-id3*] [**map-vlan** *vlan-id4*] }

undo port vlan-mapping vlan *vlan-id1* **inner-vlan** *vlan-id2* **map-vlan** *vlan-id4* **map-inner-vlan** *vlan-id5*

Parameters

Parameter	Description	Setting
vlan *vlan-id1*	Specifies the VLAN ID of the outer tag in a received packet.	The value is an integer that ranges from 1 to 4094.

Parameter	Description	Setting
inner-vlan *vlan-id2* [**to** *vlan-id3*]	Specifies the VLAN ID of the inner tag in a received packet. ● *vlan-id2*: specifies the start value of the VLAN ID range of the inner tag in the received packet. ● *vlan-id3*: specifies the end value of the VLAN ID range of the inner tag in the received packet. *vlan-id3* is optional. The value of *vlan-id3* must be greater than that of *vlan-id2*.	The value of *vlan-id2* or *vlan-id3* is an integer that ranges from 1 to 4094.
map-vlan *vlan-id4*	Specifies the VLAN ID that replaces the VLAN ID of the outer tag in a packet.	The value is an integer that ranges from 1 to 4094.
map-inner-vlan *vlan-id5*	Specifies the VLAN ID that replaces the VLAN ID of the inner tag in a packet. If the parameter **map-inner-vlan** is configured, the interface maps the VLAN ID of the inner tag in the packet to the value of *vlan-id5* specified by users.	The value is an integer that ranges from 1 to 4094.

Parameter	Description	Setting
remark-8021p *8021p-value*	Specifies the re-marked 802.1p priority of the outer tag. The 802.1p priority is specified by a 3-bit PRI (priority) field in an 802.1Q packet. When congestion occurs on a switch, packets with a higher priority are sent first. If the parameter **remark-8021p** is configured, the interface changes the 802.1p priority in the packet to the value of *8021p-value* specified by users.	The value is an integer that ranges from 0 to 7. A larger value indicates a higher priority.
all	Specifies all VLAN mapping entries configured on the primary interface.	-

Views

Ethernet interface view, GE interface view, XGE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, MultiGE interface view, port group view, 25GE interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When provider edges (PEs) receive double-tagged packets, the inner tag in the packets indicates the user, and the outer tag indicates the service. To differentiate services entering the ISP network, you can configure 2 to 1 VLAN mapping on PEs. To allow users to communicate with each other, the interface maps tags of different services to outer tags, and inner tags are transparently transmitted to the ISP network.

This command allows an interface to map the VLAN ID in a tagged packet to an S-VLAN ID.

Precautions

VLAN mapping can only be configured on trunk or hybrid ports. Hybrid ports on switches except the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, S6730S-S must be added to the mapped VLAN in tagged mode. On the S5720-LI, S5720S-LI, S5720I-SI, S5735S-H, S5736-S, S6720S-S, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735-S-I, and S5735S-S, if a trunk port is added to the mapped VLAN in untagged mode, the port forwards reverse traffic without VLAN tags. As a result, VLAN mapping may not take effect.

Interfaces configured with N:1 VLAN mapping must be added to the original VLAN in tagged mode. On switches except the S5731-S, S5731S-S, S5731-H, S5731S-H, S5732-H, S6730-H, S6730-S, S6730S-S, and S6730S-H, if a trunk port is configured with N:1 VLAN mapping and its PVID is the mapped VLAN ID or it is added to mapped VLANs in untagged mode, the port forwards reverse traffic without VLAN tags. As a result, VLAN mapping may not take effect.

When **inner-vlan** is set to a VLAN ID range, the interface cannot replace the VLAN ID of the inner tag in packets.

If VLAN mapping and DHCP are configured on the same interface, the interface must be added to the original VLANs (VLANs before mapping) in tagged mode.

When the VLAN tags of a packet match both a single-tag VLAN mapping entry and a double-tag VLAN mapping entry, the double-tag VLAN mapping takes effect.

If DHCP snooping is enabled on the device, do not configure 2:2 VLAN mapping. Otherwise, DHCP users cannot go online.

For the S6730-H, S6730-S, S6730S-S, S6730S-H, S5732-H, S5731-H, S5731S-H, S5731-S, and S5731S-S, N:1 VLAN mapping takes effect only when the packets with original VLANs are sent first and MAC address learning is enabled on interfaces and in VLANs. If packets are sent from an S-VLAN first or MAC address learning is disabled on interfaces or in VLANs, the C-VLAN to be mapped cannot be determined because no VLAN mapping information is recorded in MAC address entries. As a result, the packets are discarded. In addition, VLAN mapping cannot be configured together with VPLS or VXLAN tunnels.For the others, N:1 VLAN mapping takes effect only when the packets with original VLANs are sent first. In this case, if packets are sent from an S-VLAN first, the C-VLAN to be mapped cannot be determined because no ACL entry is generated. As a result, the packets are discarded.

Example

# Configure 2 to 1 VLAN mapping, map VLAN 10 in the outer tag of a packet (with VLAN 10 in the outer tag and VLAN 20 in the inner tag) to VLAN 100.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet0/0/1
[HUAWEI-GigabitEthernet0/0/1] port link-type trunk
[HUAWEI-GigabitEthernet0/0/1] port trunk allow-pass vlan 100
[HUAWEI-GigabitEthernet0/0/1] qinq vlan-translation enable
[HUAWEI-GigabitEthernet0/0/1] port vlan-mapping vlan 10 inner-vlan 20 map-vlan 100
```

5.9.4 port vlan-mapping vlan map-vlan

Function

The **port vlan-mapping vlan map-vlan** command enables the interface to map single tags of packets.

The **undo port vlan-mapping** command cancels the interface to map single tags of packets.

By default, the interface does not map tags of packets.

Format

port vlan-mapping vlan *vlan-id1* [**to** *vlan-id2*] **map-vlan** *vlan-id3* [**remark-8021p** *8021p-value*]

undo port vlan-mapping { **all** | **vlan** *vlan-id1* [**to** *vlan-id2*] [**map-vlan** *vlan-id3*]}

NOTE

N:1 VLAN mapping is supported on :

S5720I-SI, S5720-LI, S5720S-LI, S5735S-H, S5736-S, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735-S, S500, S5735-S-I, S5735S-L, S5735S-L1, S5735S-L-M, S5735S-S, S6735-S, S6720-EI, S6720S-S, S6720S-EI, S6730-H, S6730-S, S6730S-S, S6730S-H, S5732-H, S5731-H, S5731S-H, S5731-S, and S5731S-S

Parameters

Parameter	Description	Setting
vlan *vlan-id1* [**to** *vlan-id2*]	Specifies the VLAN ID in a received packet. ● *vlan-id1*: specifies the start value of the VLAN ID range of the tag. ● **to** *vlan-id2*: specifies the end value of the VLAN ID range of the tag. The value of *vlan-id2* must be greater than that of *vlan-id1*.	The value of *vlan-id1* or *vlan-id2* is an integer that ranges from 1 to 4094.
map-vlan *vlan-id3*	Specifies the VLAN ID in the mapped tag.	The value is an integer that ranges from 1 to 4094.

Parameter	Description	Setting
remark-8021p *8021p-value*	Specifies the re-marked 802.1p priority of the mapped tag. The 802.1p priority is specified by a 3-bit PRI (priority) field in an 802.1Q packet. When congestion occurs on a switch, packets with a higher priority are sent first. If the parameter **remark-8021p** is configured, the interface changes the 802.1p priority in the packet to the value of *8021p-value* specified by users.	The value is an integer that ranges from 0 to 7. A larger value indicates a higher priority.
all	Specifies all VLAN mapping entries configured on the interface.	-

Views

Ethernet interface view, GE interface view, XGE interface view, 40GE interface view, 100GE interface view, MultiGE interface view, Eth-Trunk interface view, port group view, 25GE interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

VLAN mapping, also called VLAN translation, implements communication between different VLANs. VLAN mapping takes effect after outbound interfaces on a switch forward the packets received by inbound interfaces. This command allows an interface to map the VLAN ID in a tagged packet to an S-VLAN ID.

After the **port vlan-mapping vlan** *vlan-id1* [**to** *vlan-id2*] **map-vlan** *vlan-id3* [**remark-8021p** *8021p-value*] command is used on an interface, *vlan-id1* [**to** *vlan-id2*] is mapped to *vlan-id3* in the inbound direction, and *vlan-id3* is mapped to *vlan-id1* [**to** *vlan-id2*] in the outbound direction.

Precautions

VLAN mapping can only be configured on trunk or hybrid ports. Hybrid ports on switches except the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, S6730S-S must be added to the mapped VLAN in tagged mode. On the S5720-LI, S5720S-LI, S5720I-SI, S5735S-H, S5736-S, S6720S-S, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735-S-I, and S5735S-S, if a trunk port is added to the mapped VLAN in untagged mode, the port forwards reverse traffic without VLAN tags. As a result, VLAN mapping may not take effect.

Interfaces configured with N:1 VLAN mapping must be added to the original VLAN in tagged mode. On switches except the S5731-S, S5731S-S, S5731-H, S5731S-H, S5732-H, S6730-H, S6730-S, S6730S-S, and S6730S-H, if a trunk port is configured with N:1 VLAN mapping and its PVID is the mapped VLAN ID or it is added to mapped VLANs in untagged mode, the port forwards reverse traffic without VLAN tags. As a result, VLAN mapping may not take effect.

When N:1 VLAN mapping is configured (VLAN IDs can be incontiguous before mapping), the interface needs to be added to these VLANs in tagged mode, and the VLAN specified by **map-vlan** cannot be a VLAN corresponding to a VLANIF interface.

If VLAN mapping and DHCP are configured on the same interface, it is recommended to add the interface to the original VLANs (VLANs before mapping) in tagged mode.

For the S6730-H, S6730-S, S6730S-S, S6730S-H, S5732-H, S5731-H, S5731S-H, S5731-S, and S5731S-S, N:1 VLAN mapping takes effect only when the packets with original VLANs are sent first and MAC address learning is enabled on interfaces and in VLANs. If packets are sent from an S-VLAN first or MAC address learning is disabled on interfaces or in VLANs, the C-VLAN to be mapped cannot be determined because no VLAN mapping information is recorded in MAC address entries. As a result, the packets are discarded. In addition, VLAN mapping cannot be configured together with VPLS or VXLAN tunnels.For the others, N:1 VLAN mapping takes effect only when the packets with original VLANs are sent first. In this case, if packets are sent from an S-VLAN first, the C-VLAN to be mapped cannot be determined because no ACL entry is generated. As a result, the packets are discarded.

N:1 VLAN mapping is not supported in a stack scenario.

A maximum of 16 original VLAN IDs can be specified on an interface.

If the VLANs before and after mapping are the same, return packets may fail to be forwarded. To solve the problem, map the VLAN to itself. For example, packets with VLAN 10 and VLAN 20 (before mapping) need to be sent to the network side and S-VLAN 20 (after mapping) is assigned to users, run the **port vlan-mapping vlan 10 map-vlan 20** command. To ensure that return packets are correctly forwarded, run the **port vlan-mapping vlan 20 map-vlan 20** command.

The S6730-H, S6730-S, S6730S-S, S6730S-H, S5732-H, S5731-H, S5731S-H, S5731-S, and S5731S-S do not support N:1 VLAN mapping on Eth-Trunk interfaces.

Example

# Configure VLAN mapping on the GE0/0/1 and map VLAN 100 of a received packet to VLAN 10 before the packet is forwarded.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet0/0/1
[HUAWEI-GigabitEthernet0/0/1] port link-type trunk
[HUAWEI-GigabitEthernet0/0/1] port trunk allow-pass vlan 10
[HUAWEI-GigabitEthernet0/0/1] qinq vlan-translation enable
[HUAWEI-GigabitEthernet0/0/1] port vlan-mapping vlan 100 map-vlan 10
```

5.9.5 remark cvlan-id

Function

The **remark cvlan-id** command configures an action of re-marking the inner VLAN tag in QinQ packets in a traffic behavior.

The **undo remark cvlan-id** command deletes the configuration.

By default, an action of re-marking the inner VLAN tag in QinQ packets is not configured in a traffic behavior.

NOTE

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

Format

remark cvlan-id *cvlan-id*

undo remark cvlan-id

Parameters

Parameter	Description	Value
cvlan-id	Specifies the inner VLAN tag of QinQ packets to be re-marked.	The value is an integer that ranges from 1 to 4094.

Views

Traffic behavior view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can use the **remark cvlan-id** command to re-mark the inner VLAN tag in QinQ packets in a traffic behavior so that the downstream device can identify packets and provide differentiated services.

Follow-up Procedure

Run the **traffic policy** command to create a traffic policy and run the **classifier behavior** command in the traffic policy view to bind the traffic classifier to the traffic behavior containing the action of re-marking the inner VLAN tag in QinQ packets.

Precautions

The **remark cvlan-id** command is valid for only QinQ packets that carry two or more layers of tags.

After the **remark cvlan-id**, **remark 8021p**, **add-tag vlan-id**, and **remark vlan-id** commands are used, the system modifies VLAN tags of packets according to the configuration. These actions are called VLAN-based actions.

You must configure the VLAN-based action and non-VLAN-based action in different traffic behaviors bound to the same traffic policy.

If you run the **remark cvlan-id** command in the same traffic classifier view multiple times, only the latest configuration takes effect.

Example

# Re-mark the inner VLAN tag in packets with 5 in the traffic behavior **b1**.

```
<HUAWEI> system-view
[HUAWEI] traffic behavior b1
[HUAWEI-behavior-b1] remark cvlan-id 5
```

5.9.6 remark vlan-id

Function

The **remark vlan-id** command configures an action of re-marking the VLAN tag in VLAN packets in a traffic behavior.

The **undo remark vlan-id** command deletes the configuration.

By default, an action of re-marking the VLAN tag in VLAN packets is not configured in a traffic behavior.

Format

remark vlan-id *vlan-id*

undo remark vlan-id

Parameters

Parameter	Description	Value
vlan-id	Specifies the VLAN tag of packets in a VLAN.	The value is an integer that ranges from 1 to 4094.

Views

Traffic behavior view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can use the **remark vlan-id** command to re-mark the VLAN tag in VLAN packets in a traffic behavior so that the downstream device can identify packets and provide differentiated services.

The **remark vlan-id** command re-marks only the outer VLAN tag of double-tagged packets.

Follow-up Procedure

Run the **traffic policy** command to create a traffic policy and run the **classifier behavior** command in the traffic policy view to bind the traffic classifier to the traffic behavior containing VLAN tag re-marking.

Precautions

If the **remark vlan-id** command is used on an inbound interface, on the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S, add the outbound interfaces to the replaced VLAN and the original VLAN. Otherwise, packets cannot be forwarded correctly. On other models, add the inbound and outbound interfaces to the replaced VLAN and the original VLAN. Otherwise, packets cannot be forwarded correctly.

If a traffic policy containing **remark vlan-id** is applied to the outbound direction on an interface, the VLAN that the interface belongs to must work in tag mode.

After the **remark vlan-id**, **remark 8021p**, **remark cvlan-id** command is used, the system modifies the VLAN tag of packets based on the device configuration. The behavior configured through these commands is called VLAN-based action.

To perform VLAN-based actions and non-VLAN-based actions in an upstream traffic policy, you need to configure VLAN-based actions and non-VLAN-based actions in different traffic behaviors.

If you run the **remark vlan-id** command in the same traffic behavior view multiple times, only the latest configuration takes effect.

Example

# Re-mark the VLAN tag of packets in a VLAN to 200.

```
<HUAWEI> system-view
[HUAWEI] traffic behavior tb
[HUAWEI-behavior-tb] remark vlan-id 200
```

5.9.7 set inner-vlan tag0-remove

Function

The **set inner-vlan tag0-remove** command configures whether interfaces retain the inner VLAN tag 0 when forwarding double-tagged frames.

The **undo set inner-vlan tag0-remove disable** command restores the default configuration.

By default, interfaces remove the inner VLAN tag 0 when forwarding double-tagged frames.

NOTE

This command is supported only on the S1720GW-E, S1720GWR-E, S5720-LI, S5720S-LI, S5720I-SI, S6720S-S, S5735S-H, S5736-S.

Format

set inner-vlan tag0-remove { **disable** | **enable** }

undo set inner-vlan tag0-remove disable

Parameters

Parameter	Description	Value
disable	Configures interfaces to retain the inner VLAN tag 0 when forwarding double-tagged frames.	-
enable	Configures interfaces to remove the inner VLAN tag 0 when forwarding double-tagged frames.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

By default, a QinQ interface removes the inner VLAN tag 0 when forwarding double-tagged frames. You can run the **set inner-vlan tag0-remove disable** command to configure interfaces to retain the inner VLAN tag 0 when forwarding double-tagged frames.

Example

# Configure interfaces to retain the inner VLAN tag 0 when forwarding double-tagged frames.

```
<HUAWEI> system-view
[HUAWEI] set inner-vlan tag0-remove disable
```

5.10 GVRP Configuration Commands

5.10.1 Command Support

Commands provided in this section and all the parameters in the commands are supported by all switch models (except the S5731-L and S5731S-L), unless otherwise specified. For details, see specific commands.

5.10.2 display garp statistics

Function

The **display garp statistics** command displays statistics about the Generic Attribute Registration Protocol (GARP) on an interface.

Format

display garp statistics [**interface** { *interface-type interface-number* [**to** *interface-type interface-number*] }&<1-10>]

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Displays the statistics about GARP on the specified interface. ● *interface-type* specifies the type of an interface. ● *interface-number* specifies the number of an interface.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After the GARP VLAN Registration Protocol (GVRP) is enabled on an interface, the system collects statistics about GVRP packets sent, received, and discarded on the interface. You can view the statistics to check whether the GVRP function on the interface is normal.

When using this command, pay attention to the following points:

- If **interface** *interface-type interface-number* is not specified, the system displays statistics about GARP packets on all the interfaces.
- If **interface** *interface-type interface-number* is specified, the system displays statistics about GARP packets on the specified interface.

Example

# Display statistics about GARP packets on a specified interface.

```
<HUAWEI> display garp statistics interface gigabitethernet 0/0/1

 GARP statistics on port GigabitEthernet0/0/1
   Number of GVRP frames received       : 0
   Number of GVRP frames transmitted    : 0
   Number of frames discarded           : 0
```

Table 5-63 Description of the display garp statistics command output

Item	Description
Number of GVRP frames received	Number of GVRP packets received by an interface.
Number of GVRP frames transmitted	Number of GVRP packets sent by an interface.
Number of frames discarded	Number of packets discarded by an interface.

5.10.3 display garp timer

Function

The **display garp timer** command displays the values of GARP timers.

Format

display garp timer [**interface** { *interface-type interface-number* [**to** *interface-type interface-number*] }&<1-10>]

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Displays the GARP timers of the specified interface. ● *interface-type* specifies the type of an interface. ● *interface-number* specifies the number of an interface.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The **display garp timer** command displays the values of GARP timers. When using this command, pay attention to the following points:

- If **interface** *interface-type interface-number* is not specified, the system displays GARP timers of all the interfaces.
- If **interface** *interface-type interface-number* is specified, the system displays GARP timers of the specified interface.

Example

# Display the values of the GARP timers of the specified interface.

```
<HUAWEI> display garp timer interface gigabitethernet 0/0/1

 GARP timers on port GigabitEthernet0/0/1
   GARP JoinTime                : 80 centiseconds
   GARP LeaveTime               : 240 centiseconds
   GARP LeaveAllTime            : 1000 centiseconds
   GARP HoldTime                : 40 centiseconds
```

Table 5-64 Description of the display garp timer command output

Item	Description
GARP JoinTime	Value of the Join timer. You can run the **garp timer** command to set the Join timer.
GARP LeaveTime	Value of the Leave timer. You can run the **garp timer** command to set the Leave timer.

Item	Description
GARP LeaveAllTime	Value of the LeaveAll timer. You can run the **garp timer leaveall** command to set the LeaveAll timer.
GARP HoldTime	Value of the Hold timer. You can run the **garp timer** command to set the Hold timer.

5.10.4 display gvrp state

Function

The **display gvrp state** command displays information about the GVRP state machine.

Format

display gvrp state interface *interface-type interface-number* **vlan** *vlan-id*

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Displays information about the GVRP state machine of the specified interface. ● *interface-type* specifies the type of an interface. ● *interface-number* specifies the number of an interface.	-
vlan *vlan-id*	Displays information about the state machine of the specified VLAN.	The value is an integer that ranges from 2 to 4094.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The GVRP function has two types of state machines: Applicant state machine and Registrar state machine.

An applicant implements declaration of attributes. If no message is lost during transmission, an applicant can ensure that all registrars have registered an attribute after it sends a Join message or receives a JoinIn message. To ensure reliable transmission of messages, the applicant needs to send two Join messages or send a Join message and receive a JoinIn message to confirm that all registrars have registered an attribute. Therefore, a simple counter is used. The counter starts from 0 and increases by 1 every time the applicant sends a Join message or receives a JoinIn message. The maximum value of the counter is 2. If the applicant receives a JoinEmpty, Empty, Leave, or LeaveAll message, the counter is reset to 0. This indicates that the applicant can send PDUs only when the value of the counter is smaller than 2.

The Join timer controls the interval for sending Join messages, but not every attribute has its own Join timer. A GVRP participant uses a Join timer. The value of the Join timer must be long enough to ensure that all the attributes can be packaged in a message and transmitted in a declaration.

- Anxious applicants

  Depending on the value of the applicant counter, an applicant may be in either of the following states:

  - V (very anxious): The value of the counter is 0, indicating that the applicant does not send a Join message or receive a JoinIn message.
  - A (anxious): The value of the counter is 1, indicating that no message is lost and all the registrars have registered the attribute.
  - Q (quiet): The value of the counter is 2, indicating that the applicant does not need to send Join messages.

- Members and observers

  The preceding states are applicable to normal situations. In special cases, for example, when some terminals do not need to send registration messages and only need to retain all the GARP state machines, these terminals must be separated from other entities. Therefore, the concept of member and observer is introduced. A member refers to an entity that tries to declare or retain an attribute value or an entity that has not sent a Leave message yet. An observer refers to an entity that traces the states of attributes but does not declare attributes.

  Multiple entities may actively join or leave the same attribute. To minimize the number of Join or Leave messages in this situation, members are classified into active members and passive members. Therefore, the following states are introduced:

  - A: Active member
  - P: Passive member
  - O: Observer

In addition, when an active member must send a Leave message to cancel a declaration, the active member enters the leaving state. Considering all these states, the state machine of an applicant has multiple state combinations, as shown in the following table.

State Combination	Very Anxious	Anxious	Quiet	Leaving
Active Member	VA	AA	QA	LA
Passive Member	VP	AP	QP	-
Observer	VO	AO	QO	LO

When a passive member needs to cancel a declaration, it can switch to the observer state. Therefore, the leaving passive member state does not exist.

A registrar has a Leave timer and three states: IN (attribute registered), MTR (attribute deregistered), and LV (attribute being deregistered). If a registrar in LV state does not receive the declaration of an attribute within the timeout interval of the Leave timer, the registrar enters the MTR state.

A registrar changes to different states depending on the received message:

- When receiving a Join message, the registrar changes to the IN state.
- When receiving a Leave or LeaveAll message, the registrar changes from the IN state to the LV state and starts the Leave timer. If the registrar is not in IN state, it does not change its state after receiving a Leave or LeaveAll message.
- The registrar does not change its state after receiving an Empty message.

Example

# Display information about the GVRP state machine.

```
<HUAWEI> display gvrp state interface gigabitethernet 0/0/1 vlan 100
   GVRP state of VLAN 100 on port GigabitEthernet0/0/1

       Applicant state machine :    VP
       Registrar state machine :    MTR
```

Table 5-65 Description of the display gvrp state command output

Item	Description
Applicant state machine	State machine of the applicant.
Registrar state machine	State machine of the registrar.

5.10.5 display gvrp statistics

Function

The **display gvrp statistics** command displays statistics about GVRP on an interface.

Format

display gvrp statistics [**interface** { *interface-type interface-number* [**to** *interface-type interface-number*] }&<1-10>]

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Displays the statistics about GVRP on the specified interface. ● *interface-type* specifies the type of an interface. ● *interface-number* specifies the number of an interface. If no interface is specified, the system displays statistics about GVRP on all interfaces.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The **display gvrp statistics** command displays statistics about GVRP on an interface, including the GVRP status, number of GVRP registration failures, source MAC address of the last GVRP PDU, and registration mode of the interface.

Example

# Display the statistics about GVRP on an interface.

```
<HUAWEI> display gvrp statistics interface gigabitethernet 0/0/1
```

```
GVRP statistics on port GigabitEthernet0/0/1
  GVRP status                  : Enabled
  GVRP registrations failed       : 0
  GVRP last PDU origin            : 0000-0000-0000
  GVRP registration type          : Normal
```

Table 5-66 Description of the display gvrp statistics command output

Item	Description
GVRP status	GVRP state. The value can be: ● Enabled ● Disabled To specify the parameter, run the **gvrp** command.
GVRP registrations failed	Number of GVRP registration failures.
GVRP last PDU origin	Source MAC address of the last GVRP PDU.
GVRP registration type	GVRP registration type of an interface, which is configured by the **gvrp registration** command. The registration type can be: ● Fixed ● Forbidden ● Normal

5.10.6 display gvrp status

Function

The **display gvrp status** command displays whether global GVRP is enabled.

Format

display gvrp status

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The device with GVRP enabled can dynamically register VLANs or deregister VLANs from an interface. You can run the **display gvrp status** command to check whether GVRP is enabled.

Example

# Display the enabling status of global GVRP.

```
<HUAWEI> display gvrp status
GVRP status: disabled
```

Table 5-67 Description of the display gvrp status command output

Item	Description
GVRP status	The status of global GVRP. To specify the parameter, run the **gvrp** command.

5.10.7 display gvrp vlan-operation

Function

The **display gvrp vlan-operation** command displays the operation of adding a specified interface to dynamic VLANs.

Format

display gvrp vlan-operation interface *interface-type interface-number*

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Displays operations related to dynamic VLANs performed on the specified interface. ● *interface-type* specifies the type of an interface. ● *interface-number* specifies the number of an interface.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The **display gvrp vlan-operation** command displays the dynamic VLANs to which an interface is added.

Example

# Display the operation of adding an interface to dynamic VLANs.

```
<HUAWEI> display gvrp vlan-operation interface GigabitEthernet 0/0/1
   Dynamic VLAN operations on port GigabitEthernet0/0/1

        Operations of adding VLAN to TRUNK            : none
```

Table 5-68 Description of the display gvrp vlan-operation command output

Item	Description
Operations of adding VLAN to TRUNK	Operation of adding a trunk interface to dynamic VLANs.

5.10.8 garp timer

Function

The **garp timer** command sets GARP timers.

The **undo garp timer** command restores the default values of GARP timers.

By default, the value of the Hold timer is 10 centiseconds, the value of the Join timer is 20 centiseconds, and the value of the Leave timer is 60 centiseconds.

Format

garp timer { **hold** | **join** | **leave** } *timer-value*

undo garp timer { **hold** | **join** | **leave** } [*timer-value*]

Parameters

Parameter	Description	Value
hold *timer-value*	Sets the value of the GARP Hold timer.	- Lower limit: 10 centiseconds - Upper limit: less than or equal to half the value of the Join timer, changing with the value of the Join timer - The value can be exactly divided by 5, in centiseconds.
join *timer-value*	Sets the value of the GARP Join timer.	- Lower limit: greater than or equal to two times the value of the Hold timer, changing with the value of the Hold timer - Upper limit: smaller than half the value of the Leave timer, changing with the value of the Leave timer - The value can be exactly divided by 5, in centiseconds.
leave *timer-value*	Sets the value of the GARP Leave timer.	- Lower limit: greater than two times the value of the Join timer, changing with the value of the Join timer - Upper limit: smaller than the value of the LeaveAll timer, changing with the value of the LeaveAll timer - The value can be exactly divided by 5, in centiseconds.

Views

Ethernet interface view, GE interface view, XGE interface view, MultiGE interface view, 100GE interface view, 40GE interface view, 100GE interface view, port group view, Eth-Trunk interface view, 25GE interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

This command can set the following GARP timers:

- Join timer: controls sending of Join messages including JoinIn messages and JoinEmpty messages.
- Hold timer: controls sending of Join messages (JoinIn messages and JoinEmpty messages) and Leave messages (LeaveIn messages and LeaveEmpty messages).
- Leave timer: controls attribute deregistration.

You can set the GARP timers to control sending of GARP protocol packets.

Prerequisite

The physical port has been added to the port group before running the **garp timer** command in the port group view.

Before setting garp timers on an interface, you must enable GVRP globally and on the interface.

Precautions

When using the **garp timer** command to set the GARP timers, pay attention to the following points:

- The **garp timer** can be used only on trunk interfaces.
- The **undo garp timer** command restores the default values of GARP timers. If the default value of a timer is out of the valid range, the **undo garp timer** command does not take effect.
- The value range of each timer changes with the values of the other timers. If a value you set for a timer is not in the allowed range, you can change the value of the timer that determines the value range of this timer.
- To restore the default values of all the GARP timers, restore the Hold timer to the default value, and then restore the Join timer, Leave timer, and LeaveAll timer to the default values in sequence.

When many dynamic VLANs need to be registered or the network radius is large, using default values of timers may cause VLAN flapping and high CPU usage. In this case, increase values of the timers. The following values are recommended depending on the number of VLANs.

Table 5-69 Relationship between GARP timer values and number of dynamic VLANs that need to be registered

Timer	Number of Dynamic VLANs to Be Registered (N)			
	N <= 500	500 < N <= 1000	1000 < N <= 1500	N > 1500
GARP Hold timer	100 centiseconds (1 second)	200 centiseconds (2 seconds)	800 centiseconds (8 seconds)	1000 centiseconds (10 seconds)
GARP Join timer	600 centiseconds (6 seconds)	1200 centiseconds (12 seconds)	4000 centiseconds (40 seconds)	6000 centiseconds (1 minute)

Timer	Number of Dynamic VLANs to Be Registered (N)			
	N <= 500	500 < N <= 1000	1000 < N <= 1500	N > 1500
GARP Leave timer	3000 centiseconds (30 seconds)	6000 centiseconds (1 minute)	20000 centiseconds (3 minutes and 20 seconds)	30000 centiseconds (5 minutes)
GARP LeaveAll timer	12000 centiseconds (2 minutes)	24000 centiseconds (4 minutes)	30000 centiseconds (5 minutes)	32765 centiseconds (5 minutes and 27.65 seconds)

Example

# Set the Leave timer of GigabitEthernet 0/0/1 to 800 centiseconds.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] port link-type trunk
[HUAWEI-GigabitEthernet0/0/1] garp timer leave 800
```

# Set the Join timer of GigabitEthernet 0/0/1 to 300 centiseconds.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] port link-type trunk
[HUAWEI-GigabitEthernet0/0/1] garp timer join 300
```

# Set the Hold timer of GigabitEthernet 0/0/1 to 100 centiseconds.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] port link-type trunk
[HUAWEI-GigabitEthernet0/0/1] garp timer hold 100
```

5.10.9 garp timer leaveall

Function

The **garp timer leaveall** command sets the GARP LeaveAll timer.

The **undo garp timer leaveall** command restores the default value of the GARP LeaveAll timer.

The default value of the LeaveAll timer is 1000 centiseconds (10 seconds).

Format

garp timer leaveall *timer-value*

undo garp timer leaveall [*timer-value*]

Parameters

Parameter	Description	Value
timer-value	Specifies the value of the GARP LeaveAll timer.	The value is an integer that ranges from 65 to 32765 and that can be exactly divided by 5, in centiseconds. The value of the LeaveAll timer must be greater than the values of Leave timers on all the interfaces.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When a GARP participant is enabled, the LeaveAll timer is started. When the LeaveAll timer expires, the GARP participant sends LeaveAll messages to request other GARP participants to re-register all its attributes. Then the LeaveAll timer restarts.

Devices on a network may have different settings for the LeaveAll timer. In this case, all the devices use the smallest LeaveAll timer value on the network. When the LeaveAll timer of a device expires, the device sends LeaveAll messages to other devices. After other devices receive the LeaveAll messages, they reset their LeaveAll timers. Therefore, only the LeaveAll timer with the smallest value takes effect even if devices have different settings for the LeaveAll timer.

Prerequisites

Before setting LeaveAll timers, you must enable GVRP globally.

Precautions

The Leave timer length on an interface is restricted by the global LeaveAll timer length. When configuring the global LeaveAll timer, ensure that all the interfaces that have a GARP Leave timer configured are working properly.

Example

# Set the LeaveAll timer to 2000 centiseconds.

```
<HUAWEI> system-view
[HUAWEI] garp timer leaveall 2000
```

5.10.10 gvrp

Function

The **gvrp** command enables GVRP globally or on an interface.

The **undo gvrp** command disables GVRP globally or on an interface.

By default, GVRP is disabled globally and on each interface.

Format

gvrp

undo gvrp

Parameters

None

Views

System view, Ethernet interface view, GE interface view, XGE interface view, MultiGE interface view, 40GE interface view, 100GE interface view, port group view, Eth-Trunk interface view, 25GE interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The device with GVRP enabled can dynamically register VLANs or deregister VLANs from an interface. To make GVRP take effect, run the **gvrp** command both in the system view and interface view.

Precautions

When configuring GVRP, pay attention to the following points:

- If you run the **gvrp** command in the system view, GVRP is enabled globally. If you run this command in the interface view, GVRP is enabled on the interface.
- Before enabling GVRP on an interface, you must enable GVRP globally.
- Before enabling GVRP on an interface, you must set the link type of the interface to trunk.
- GVRP and Port security conflict on an interface; therefore, the **port-security enable** and **gvrp** commands cannot be used on the same interface.
- When GVRP is enabled globally, manually change values of timers based on the network scale.

Table 5-70 Relationship between GARP timer values and number of dynamic VLANs that need to be registered

Timer	Number of Dynamic VLANs to Be Registered (N)			
	N <= 500	500 < N <= 1000	1000 < N <= 1500	N > 1500
GARP Hold timer	100 centiseconds (1 second)	200 centiseconds (2 seconds)	800 centiseconds (8 seconds)	1000 centiseconds (10 seconds)
GARP Join timer	600 centiseconds (6 seconds)	1200 centiseconds (12 seconds)	4000 centiseconds (40 seconds)	6000 centiseconds (1 minute)
GARP Leave timer	3000 centiseconds (30 seconds)	6000 centiseconds (1 minute)	20000 centiseconds (3 minutes and 20 seconds)	30000 centiseconds (5 minutes)
GARP LeaveAll timer	12000 centiseconds (2 minutes)	24000 centiseconds (4 minutes)	30000 centiseconds (5 minutes)	32765 centiseconds (5 minutes and 27.65 seconds)

Example

# Enable GVRP globally.

```
<HUAWEI> system-view
[HUAWEI] gvrp
```

# Enable GVRP on GigabitEthernet 0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] port link-type trunk
[HUAWEI-GigabitEthernet0/0/1] gvrp
```

5.10.11 gvrp registration

Function

The **gvrp registration** command sets the registration mode of a GVRP interface.

The **undo gvrp registration** command restores the default registration mode of a GVRP interface.

By default, the registration mode of a GVRP interface is **normal**.

Format

gvrp registration { **fixed** | **forbidden** | **normal** }

undo gvrp registration [**fixed** | **forbidden** | **normal**]

Parameters

Parameter	Description	Value
fixed	Indicates the fixed registration mode.	-
forbidden	Indicates the forbidden registration mode.	-
normal	Indicates the normal registration mode.	-

Views

Ethernet interface view, GE interface view, XGE interface view, MultiGE interface view, 40GE interface view, 100GE interface view, port group view, Eth-Trunk interface view, 25GE interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A GVRP interface supports three registration modes:

- Normal: In this mode, the GVRP interface can dynamically register and deregister VLANs, and transmit dynamic VLAN registration information and static VLAN registration information.
- Fixed: In this mode, the GVRP interface is disabled from dynamically registering and deregistering VLANs and can transmit only the static VLAN registration information. If the registration mode of a trunk interface is set to **fixed**, the interface allows only the manually configured VLANs to pass even if it is configured to allow all the VLANs to pass.
- Forbidden: In this mode, the GVRP interface is disabled from dynamically registering and deregistering VLANs and can transmit only information about VLAN 1. If the registration mode of a trunk interface is set to **forbidden**, the interface allows only VLAN 1 to pass even if it is configured to allow all the VLANs.

Pre-configuration Tasks

Before setting the registration mode of an interface, you must enable GVRP globally and configure the interface as a trunk interface.

Example

# Set the registration mode of GE0/0/1 to **fixed**.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] port link-type trunk
[HUAWEI-GigabitEthernet0/0/1] gvrp
[HUAWEI-GigabitEthernet0/0/1] gvrp registration fixed
```

5.10.12 reset garp statistics

Function

The **reset garp statistics** command clears statistics about GARP packets on an interface.

Format

reset garp statistics [**interface** { *interface-type interface-number* [**to** *interface-type interface-number*] }&<1-10>]

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Clears the statistics about GARP packets on a specified interface. ● *interface-type* specifies the type of an interface. ● *interface-number* specifies the number of an interface.	-

Views

User view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Before collecting GARP traffic statistics on a specific interface within a certain period, you need to clear the existing GARP traffic statistics on this interface.

When using this command, pay attention to the following points:

- If **interface** *interface-type interface-number* is not specified, the system clears statistics about GARP packets on all the interfaces.
- If **interface** *interface-type interface-number* is specified, the system clears statistics about GARP packets on the specified interface.

Precautions

GVRP statistics cannot be restored after being cleared. Confirm your action before using this command.

Example

# Clear statistics about GARP packets on GE0/0/1.

```
<HUAWEI> reset garp statistics interface gigabitethernet 0/0/1
```

5.11 VCMP Configuration Commands

5.11.1 Command Support

Commands provided in this section and all the parameters in the commands are supported by all switch models (except the S5731-L and S5731S-L), unless otherwise specified. For details, see specific commands.

5.11.2 display vcmp counters

Function

The **display vcmp counters** command displays statistics on VCMP packets.

Format

display vcmp counters

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

If VCMP configured on a switch does not take effect, run the **display vcmp counters** command to view statistics on VCMP packets. The statistics helps you determine whether data on the switch is incorrect and locate faults.

Example

# Display statistics on VCMP packets.

```
<HUAWEI> display vcmp counters
VCMP statistics:
```

```
Received summary packets                   : 0
Received request packets                   : 0
Received subset packets                    : 0
Sent summary packets                       : 0
Sent request packets                       : 0
Sent subset packets                        : 0
Received packets with ethheader error      : 0
Received packets with version error        : 0
Received packets with type error           : 0
Received packets with digest error         : 0
Received packets with domain error         : 0
Received packets with deviceid error       : 0
Failed to receive packets for bad vcmp state    : 0
Failed to send packets for bad vcmp state       : 0
Failed to receive packets for bad vlan          : 0
Failed to send packets for bad vlan             : 0
Failed to receive packets for bad link state    : 0
Failed to send packets for bad link state       : 0
Failed to receive packets for bad link type     : 0
Failed to send packets for bad link type        : 0
Failed to receive packets for bad forward state : 0
Failed to send packets for bad forward state    : 0
Failed to receive packets for bad length        : 0
Failed to receive packets for other             : 0
```

Table 5-71 Description of the display vcmp counters command output

Item	Description
VCMP statistics	Statistics on VCMP packets.
Received summary packets	Number of received VCMP Summary-Advert packets.
Received request packets	Number of received VCMP Advert-Request packets.
Received subset packets	Number of received VCMP subset packets.
Sent summary packets	Number of sent VCMP Summary-Advert packets.
Sent request packets	Number of sent VCMP Advert-Request packets.
Sent subset packets	Number of sent VCMP subset packets.
Received packets with ethheader error	Number of received VCMP packets with an incorrect Ethernet header.
Received packets with version error	Number of received VCMP packets with an incorrect protocol version.
Received packets with type error	Number of received VCMP packets of an incorrect type.
Received packets with digest error	Number of received VCMP packets with an incorrect digest.

Item	Description
Received packets with domain error	Number of received VCMP packets with an incorrect VCMP domain name.
Received packets with deviceid error	Number of received VCMP packets with an incorrect device ID.
Failed to receive packets for bad vcmp state	Number of packets that failed to be received due to incorrect VCMP status.
Failed to send packets for bad vcmp state	Number of packets that failed to be sent due to incorrect VCMP status.
Failed to receive packets for bad vlan	Number of packets that failed to be received due to incorrect VLAN information.
Failed to send packets for bad vlan	Number of packets that failed to be sent due to incorrect VLAN information.
Failed to receive packets for bad link state	Number of packets that failed to be received due to incorrect link status.
Failed to send packets for bad link state	Number of packets that failed to be sent due to incorrect link status.
Failed to receive packets for bad link type	Number of packets that failed to be received due to an incorrect link type.
Failed to send packets for bad link type	Number of packets that failed to be sent due to an incorrect link type.
Failed to receive packets for bad forward state	Number of packets that failed to be received due to incorrect forwarding status of the Layer 2 Ethernet interface.
Failed to send packets for bad forward state	Number of packets that failed to be sent due to incorrect forwarding status of the Layer 2 Ethernet interface.
Failed to receive packets for bad length	Number of packets that failed to be received because their lengths are incorrect.
Failed to receive packets for other	Number of packets that failed to be received due to other causes.

5.11.3 display vcmp interface brief

Function

The **display vcmp interface brief** command displays the VCMP status on Layer 2 Ethernet interfaces.

Format

display vcmp interface brief

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

By default, VCMP is enabled on all Layer 2 Ethernet interfaces of a switch. You can run the **display vcmp interface brief** command to view the VCMP status on Layer 2 Ethernet interfaces.

Example

# Display the VCMP status on Layer 2 Ethernet interfaces.

```
<HUAWEI> display vcmp interface brief
Vcmp interface number:2
Interface                Vcmp State
---------------------------------------------
GigabitEthernet0/0/1         disable
GigabitEthernet0/0/2         enable
```

Table 5-72 Description of the display vcmp interface brief command output

Item	Description
Vcmp interface number	Number of Layer 2 Ethernet interfaces supporting VCMP.
Interface	Name and number of a Layer 2 Ethernet interface on which VCMP can run.
Vcmp State	VCMP status on a Layer 2 Ethernet interface. To specify the parameter, run the **vcmp disable** command.

5.11.4 display vcmp status

Function

The **display vcmp status** command displays the VCMP configuration, including the VCMP domain name, VCMP role, device ID, configuration revision number, and VCMP domain authentication password.

Format

display vcmp status

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After VCMP is configured on a switch, you can run the **display vcmp status** command to view the VCMP configuration.

Example

# Display the VCMP configuration.

```
<HUAWEI> display vcmp status
VCMP information:
Domain                  : VLAN
Role                    : Server
Server ID               : VLAN
Configuration Revision  : 0x846a0000
Password                : ******
```

Table 5-73 Description of the display vcmp status command output

Item	Description
VCMP information	VCMP information.
Domain	VCMP domain name. To change the VCMP domain name, run the **vcmp domain** command.
Role	VCMP role of the switch in the VCMP domain. To change the VCMP role, run the **vcmp role** command.
Server ID	ID of the switch functioning as the VCMP server. To change the device ID, run the **vcmp device-id** command.

Item	Description
Configuration Revision	Configuration revision number.
Password	VCMP domain authentication password. To change the authentication password, run the **vcmp authentication** command. If no authentication password is configured, this parameter is left empty.

5.11.5 display vcmp track

Function

The **display vcmp track** command displays VLAN changes on a device functioning as a client.

Format

display vcmp track

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

If VLAN changes, including creating VLANs, deleting VLANs, modifying VLAN names, and modifying VLAN descriptions, are made on a device functioning as a server, the device functioning as a client synchronizes its VLAN information with that on the server by exchanging VCMP packets. To view VLAN changes, run the **display vcmp track** command on the client.

Example

# Display VLAN changes on the client.

```
<HUAWEI> display vcmp track
Operate Flags: A - Add, D - Delete, VN - VLAN Name , VD - VLAN Description
-------------------------------------------------------------------------------
Op System-Time              Operate-VLAN
-------------------------------------------------------------------------------
A  03-19 19:32:27           103
```

```
A  03-19 19:30:57          10
D  03-19 19:15:52          20
VD 03-19 19:12:20           100
VN 03-19 19:12:06           100
A  03-19 19:10:48          101
A  03-19 19:09:45          100
```

Table 5-74 Description of the **display vcmp track** command output

Item	Description
Operate Flags	Operation flag: ● A: Newly created VLANs ● D: Deleted VLANs ● VN: VLANs whose names were modified ● VD: VLANs whose descriptions were modified
Op System-Time	System time
Operate-VLAN	Operated VLAN

5.11.6 reset vcmp

Function

The **reset vcmp** command clears the VCMP domain name and device ID learned on a VCMP client.

Format

reset vcmp

Parameters

None

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

The VCMP domain ID and device ID learned by a VCMP client remain unchanged. The VCMP client needs to learn VCMP information again when the VCMP server in the local VCMP domain is changed. Therefore, clear learned VCMP information before the VCMP client learns VCMP information.

Configuration Impact

After the **reset vcmp** command is executed, the learned VCMP information is cleared and cannot be restored. Therefore, exercise caution when you run the **reset vcmp** command.

Example

# Clear the VCMP domain name and device ID learned on a VCMP client

```
<HUAWEI> reset vcmp
```

5.11.7 reset vcmp counters

Function

The **reset vcmp counters** command clears statistics on VCMP packets.

Format

reset vcmp counters

Parameters

None

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

Before re-collecting statistics on VCMP packets in a specified period, run the **reset vcmp counters** command to clear existing statistics on VCMP packets.

Configuration Impact

After the **reset vcmp counters** command is executed, statistics on VCMP packets are cleared cannot be restored. Therefore, exercise caution when you run the **reset vcmp counters** command.

Example

# Clear statistics on VCMP packets.

```
<HUAWEI> reset vcmp counters
```

5.11.8 reset vcmp track

Function

The **reset vcmp track** command deletes VLAN changes on a device functioning as a client.

Format

reset vcmp track

Parameters

None

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

Before viewing VLAN changes on a client using the **display vcmp track** command, run the **reset vcmp track** command to delete existing VLAN changes.

Configuration Impact

After you run the **reset vcmp track** command, the deleted information cannot be restored. Therefore, exercise caution when running the **reset vcmp track** command.

Example

# Delete existing VLAN changes on the client.

```
<HUAWEI> reset vcmp track
```

5.11.9 vcmp authentication

Function

The **vcmp authentication** command sets a VCMP domain authentication password.

The **undo vcmp authentication** command deletes the VCMP domain authentication password.

By default, no VCMP domain authentication password is set and VCMP packets pass without authentication.

Format

vcmp authentication sha2-256 password *password*

undo vcmp authentication

Parameters

Parameter	Description	Value
sha2-256	Enables SHA2-256 authentication for a VCMP domain.	-
password *password*	Specifies a VCMP domain authentication password.	The value a string of case-sensitive characters, spaces not supported. Passwords are saved in ciphertext in the configuration file. Either of the following passwords can be set: ● A simple text password is a string of 1 to 8 characters. ● A ciphertext password is a string of 48 characters. When double quotation marks are used around the string, spaces are allowed in the string. **NOTE** A 32-character ciphertext password configured in an earlier version is also supported in this version.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To enhance security for a VCMP domain, you can run the **vcmp authentication** command to set a VCMP domain authentication password on each switch for authenticating packets exchanged between the switches in the VCMP domain.

Precautions

All switches in a VCMP domain must use the same VCMP domain authentication password.

Example

# Set the VCMP domain authentication password to **huawei**.

```
<HUAWEI> system-view
[HUAWEI] vcmp authentication sha2-256 password huawei
```

5.11.10 vcmp device-id

Function

The **vcmp device-id** command sets the device ID of the VCMP server.

The **undo vcmp device-id** command deletes the device ID of the VCMP server.

By default, no device ID is set for the VCMP server.

Format

vcmp device-id *device-name*

undo vcmp device-id

Parameters

Parameter	Description	Value
device-name	Specifies a device ID.	The value is a string of 1 to 31 case-sensitive characters without spaces. When double quotation marks are used around the string, spaces are allowed in the string.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A device ID identifies the VCMP server so that other roles in a VCMP domain can identify the VCMP server.

Prerequisites

The **vcmp role server** command has been executed to configure a server role for a switch in a VCMP domain. The device ID can be set only for the VCMP server.

Example

# Set the device ID of the VCMP server.

```
<HUAWEI> system-view
[HUAWEI] vcmp device-id VLAN
```

5.11.11 vcmp disable

Function

The **vcmp disable** command disables VCMP on an interface.

The **undo vcmp disable** command enables VCMP on an interface.

By default, VCMP is enabled on all interfaces of a switch.

Format

vcmp disable

undo vcmp disable

Parameters

None

Views

Ethernet interface view, GE interface view, XGE interface view, 25GE interface view, 100GE interface view, 40GE interface view, MultiGE interface view, Eth-Trunk interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

By default, VCMP is enabled on all interfaces of a switch. If an edge switch in a VCMP domain requires VCMP management but its peer end does not require VCMP management, run the **vcmp disable** command on the edge switch Layer 2 interface connected to the peer end to disable VCMP. The peer end then does not receive VCMP packets.

Prerequisites

The interface connected to the peer end has been configured as a Layer 2 interface using the **portswitch** command.

Example

# Disable VCMP on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] vcmp disable
```

5.11.12 vcmp domain

Function

The **vcmp domain** command configures a VCMP domain.

The **undo vcmp domain** command deletes a VCMP domain.

By default, no VCMP domain is created.

Format

vcmp domain *domain-name*

undo vcmp domain

Parameters

Parameter	Description	Value
domain-name	Specifies the name of a VCMP domain.	The value is a string of 1 to 31 case-sensitive characters without spaces. When double quotation marks are used around the string, spaces are allowed in the string.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

VLANs created and deleted on the VCMP server are synchronized to VCMP clients in the local VCMP domain by sending VCMP packets.

A VCMP domain specifies the scope for managed switches. All VCMP clients are managed by the VCMP server. You can run the **vcmp domain** command to configure a VCMP domain.

Precautions

All switches in a VCMP domain must use the same domain name either through manual configuration or automatic learning. If the domain name is not set on a VCMP client, the VCMP client learns the domain name in the first received VCMP packet.

Each switch can be added to only one VCMP domain. Switches in different VCMP domains cannot synchronize VLAN information.

Example

# Configure a VCMP domain named **VLAN**.

```
<HUAWEI> system-view
[HUAWEI] vcmp domain VLAN
```

5.11.13 vcmp role

Function

The **vcmp role** command configures a role for a switch in a VCMP domain.

The **undo vcmp role** command restores the default role of a switch in a VCMP domain.

By default, switches in a VCMP domain are VCMP silent.

Format

vcmp role { **client** | **server** | **silent** | **transparent** }

undo vcmp role

Parameters

Parameter	Description	Value
client	Indicates the client role in a VCMP domain. As a managed role, a VCMP client synchronizes VLAN information with the VCMP server. After the VCMP server is specified on a Layer 2 network, VCMP clients in the same domain learn VLAN information in VCMP packets from the VCMP server and synchronize the VLAN information. You can create and delete VLAN information on VCMP clients. Local VLAN information on VCMP clients, however, are overwritten by VLAN information synchronized from the VCMP server.	-
server	Indicates the server role in a VCMP domain. You can create and delete VLAN information on the VCMP server. The VCMP server synchronizes VLAN information to other switches in the local VCMP domain by sending VCMP packets.	-

Parameter	Description	Value
silent	Indicates the silent role in a VCMP domain. Deployed at the edge of a VCMP domain, a VCMP silent switch prevents VCMP packets in a VCMP domain from being transmitted to other VCMP domains, saving unnecessary costs of devices in other VCMP domains. A VCMP silent switch directly discards received VCMP packets.	-
transparent	Indicates the transparent role in a VCMP domain. A VCMP transparent switch does not affect other switches in the local VCMP domain and is not affected by VCMP management behaviors such as VLAN creation and deletion. The VCMP transparent switch transparently forwards VCMP packets. Only trunk or hybrid interfaces in VLAN 1 can receive and forward VCMP packets. VLANs created and deleted on a VCMP transparent switch are not synchronized to other switches.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

VLANs created and deleted on the VCMP server are synchronized to VCMP clients in the local VCMP domain by sending VCMP packets.

You can run the **vcmp role** command to set roles of switches in a VCMP domain.

Precautions

In V200R021C10 and earlier versions, the VCMP role is **Client** by default. In V200R022C00 and later versions, the VCMP role is **Silent** by default. If a device is upgraded from V200R021C10 or an earlier version to V200R022C00 or a later version, the VCMP role does not change after the upgrade.

In V200R021C10 and earlier versions:

- The VCMP role of a device is Client by default and the device configuration file does not contain the vcmp role client command. After the device is upgraded to V200R022C00 or a later version, the device configuration file contains the vcmp role client command.
- If the vcmp role silent command has been run on a device to set the VCMP role to Silent, the device configuration file contains the vcmp role silent

command. After the device is upgraded to V200R022C00 or a later version, the device configuration file does not contain the vcmp role silent command.

Example

# Configure a switch as the VCMP server in a VCMP domain.

```
<HUAWEI> system-view
[HUAWEI] vcmp role server
Warning: Change the VCMP role from client to server.Continue? [Y/N]:y
```

5.12 STP/RSTP/MSTP/VBST Configuration Commands

5.12.1 Command Support

Commands provided in this section and all the parameters in the commands are supported by all switch models (except the S5731-L and S5731S-L), unless otherwise specified. For details, see specific commands.

5.12.2 active region-configuration

Function

The **active region-configuration** command activates the configuration of a multiple spanning tree (MST) region.

Format

active region-configuration

Parameters

None

Views

MST region view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Configuring MST region parameters, especially VLAN mapping tables for MST regions, is likely to cause network topology flapping. To reduce network flapping, make sure that newly configured MST region parameters take effect only after the **active region-configuration** command is run.

Precautions

Before running the **active region-configuration** command, you are recommended to run the **check region-configuration** command to check whether the region configurations that have not taken effect are correct. If the region configurations that have not taken effect are correct, run the **active region-configuration** command.

After the **active region-configuration** command is run, the configured MST region parameters will take effect and all spanning trees in the MST region will be recalculated.

If the VLAN to be mapped to an MSTP instance is the control VLAN for the SEP segment, the newly configured parameters of the MST region cannot be activated.

Example

# Map VLAN 5 to the spanning tree instance 2 and activate the configuration.

```
<HUAWEI> system-view
[HUAWEI] stp region-configuration
[HUAWEI-mst-region] instance 2 vlan 5
[HUAWEI-mst-region] active region-configuration
```

5.12.3 check region-configuration

Function

The **check region-configuration** command displays the configuration of an MST region such as the region name, revision level, and VLAN mapping table.

Format

check region-configuration

Parameters

None

Views

MST region view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

MSTP divides a switching network into multiple regions, each of which has multiple spanning trees that are independent of each other. Each region is called an MST region and each spanning tree is called a multiple spanning tree instance (MSTI).

Two switching devices belong to the same MST region only when they have the following same configurations:

- MST region name
- MST region revision level
- Mappings between MSTIs and VLANs

To ensure that MST region configurations on each switching device are correct, you are recommended to run the **check region-configuration** command to check the MST region configurations before running the **active region-configuration** command. If the MST region configurations are correct, run the **active region-configuration** command to activate them.

Precautions

By default, VLANs that are not mapped to any instances with non-zero IDs using the **instance** command are mapped to instance 0.

Example

# Display the configuration of an MST region.

```
<HUAWEI> system-view
[HUAWEI] stp region-configuration
[HUAWEI-mst-region] check region-configuration
 Admin configuration
   Format selector    :0
   Region name        :00b010000001
   Revision level     :0

   Instance   VLANs Mapped
     0       1 to 9, 11 to 4094
    16       10
```

Table 5-75 Description of the check region-configuration command output

Item	Description
Format selector	Selection factor defined by MSTP
Region name	Name of the MST region. To configure the name for an MST region, run the **region-name** command.
Revision level	Revision level of the MST region. To set the revision level of the MST region, run the **revision-level** command.
Instance VLANs Mapped	Mapping between MSTIs and VLANs. To configure the mapping between MSTIs and VLANs, run the **instance** or **vlan-mapping modulo**.

5.12.4 display ethernet-loop-protection ignored-vlan

Function

The **display ethernet-loop-protection ignored-vlan** command displays information about configured ignored VLANs.

Format

display ethernet-loop-protection ignored-vlan

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

After you configure an ignored VLAN using the **ethernet-loop-protection ignored-vlan** command, the **display ethernet-loop-protection ignored-vlan** command can be used to display information about the configured ignored VLAN.

Prerequisites

An ignored VLAN has been configured using the **ethernet-loop-protection ignored-vlan** command.

Example

# Display information about the configured ignored VLAN.

```
<HUAWEI> display ethernet-loop-protection ignored-vlan
 Ethernet-loop-protection ignored-vlan : 3 to 4
```

Table 5-76 Description of the **display ethernet-loop-protection ignored-vlan** command output

Item	Description
Ethernet-loop-protection ignored-vlan	ID of a configured ignored VLAN To specify the parameter, run the **ethernet-loop-protection ignored-vlan** command.

5.12.5 display stp

Function

The **display stp** command displays the status of and statistics on a spanning tree instance.

Format

STP/RSTP/MSTP: **display stp** [**process** *process-id*] [**instance** *instance-id*] [**interface** *interface-type interface-number* | **slot** *slot-id*] [**brief**]

VBST: **display stp** [**vlan** *vlan-id*] [**interface** *interface-type interface-number* | **slot** *slot-id*] [**brief**]

Parameters

Parameter	Description	Value
process *process-id*	Indicates the ID of an MSTP process. If **process** *process-id* is not specified, the status and statistics of an MSTP process with the ID 0 will be displayed.	The value is a decimal integer ranging from 1 to 31.
instance *instance-id*	Displays the status and statistics of a spanning tree instance. If **instance** *instance-id* is not specified, the status and statistics of all spanning tree instances will be displayed in the sequence of the interface numbers.	The value is an integer ranging from 0 to 4094. Value 0 refers to CIST. **NOTE** *instance-id* ranges from 0 to 4094. Each process supports a maximum of 65 instances.
interface *interface-type interface-number*	Displays the information of a spanning tree on a specified interface. If **interface** *interface-type interface-number* is not specified, the status and statistics of all interfaces will be displayed in the sequence of the interface numbers.	-
brief	Displays the brief status.	-
slot *slot-id*	Displays the status of and statistics on a spanning tree instance in a specified slot.	The value is an integer and must be an existing slot on the device.

Parameter	Description	Value
vlan *vlan-id*	Displays spanning tree configurations in a specified VLAN. If **vlan** *vlan-id* is not specified, configurations of spanning trees in all VLANs are displayed. **NOTE** If **vlan** *vlan-id* is specified, only VBST spanning tree configurations in a specified VLAN are displayed.	The value is an integer ranging from 1 to 4094.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

The **display stp** command is used to check whether STP/RSTP/MSTP/VBST is run in the existing switching device or specified interface.

- If the **Protocol Status** field value is **Disabled**, STP/RSTP/MSTP/VBST is not run.
- If STP/RSTP/MSTP has been run, information such as the working mode of STP/RSTP/MSTP/VBST will be displayed.

When the network planner has deployed STP/RSTP/MSTP/VBST on the network, you can run the **display stp** command to check the configurations and calculation result.

Precautions

- If you run this command in the system view without specifying an MSTP process, information about MSTP process 0 is displayed by default.
- If you run this command in the MSTP process view without specifying an MSTP process, information about the MSTP process in this view is displayed by default.
- In VBST, if NAC authentication is configured but user authentication fails on a port that is configured as an edge port and is in Active state, information about the port is not displayed.
- If a non-0 instance is mapped to a VLAN to which no interface is added, the following information is displayed when you query the status and statistics of the spanning tree instance:
  ```
  Info: No instance information is available.
  ```

NOTE

For description about MSTP process 0, see **stp process**.

Example

# When the **stp enable** command does not run, the status and statistics of STP are displayed.

```
<HUAWEI> display stp
 Protocol Status       :Disabled
 Protocol Standard     :IEEE 802.1s
 Version               :3
 CIST Bridge Priority  :32768
 MAC address           :00e0-6343-6800
 Max age(s)            :20
 Forward delay(s)      :15
 Hello time(s)         :2
 Max hops              :20
 Share region-configuration :Enabled
```

Table 5-77 Description table of the display stp command output

Item	Description
Protocol Status	Status of the protocol. ● Disabled ● Enabled
Protocol Standard	Standards of the protocol.
Version	Protocol version: ● 0: STP ● 2: RSTP ● 3: MSTP To set the protocol version, run the **stp mode** command.
CIST Bridge Priority	Priority of the switch in the CIST. To set the STP priority, run the **stp priority** command.
MAC address	MAC address of the switch.
Max age (s)	Maximum TTL of a BPDU. To set the value of Max Age, run the **stp timer max-age** command.
Forward delay (s)	Time taken by interface status transition. To set the value of Forward Delay, run the **stp timer forward-delay** command.
Hello time (s)	Interval for sending BPDUs from the root switch. To set the hello time, run the **stp timer hello** command.
Max hops	Maximum number of hops in an MST region. To set the maximum number of hops, run the **stp max-hops** command.
Share region-configuration	Status of sharing the region configuration of process 0. The status is fixed at Enable.

# Display the status of and statistics on a spanning tree instance when the **stp enable** command is configured.

```
<HUAWEI> display stp brief
 MSTID   Port                    Role  STP State     Protection
   0     GigabitEthernet0/0/1    DESI  FORWARDING      NONE
   0     GigabitEthernet0/0/2    DESI  FORWARDING      NONE
   0     GigabitEthernet0/0/4    ROOT  FORWARDING      NONE
```

Table 5-78 Description of the display stp brief command output

Item	Description
MSTID	MSTP instance ID.
Port	-
Role	Interface role: ● DESI: Designated port ● ROOT: Root port ● ALTE: Alternate port ● BACK: Backup port ● MAST: Master port ● DISA: The interface is in initialization state.
STP State	Interface status. In the CIST region, the statuses of interfaces are as follows: ● FORWARDING ● LEARNING ● DISCARDING
Protection	Protection function: ● ROOTPROTECTION ● LOOPPROTECTION ● NONE ● LOOPBACK: loopback detection ● PVIDCONSISTENCY: The PVID of the directly connected interface is inconsistent.

# Displays spanning tree configurations when VBST is running.

```
<HUAWEI> display stp
-------[VLAN 20 Global Info][Mode VBST]-------
Bridge ID           :32788.00e0-f068-0600
Bridge Diameter     :7
Config Times        :Hello 2s MaxAge 20s FwDly 15s
Active Times        :Hello 2s MaxAge 20s FwDly 15s
Root ID / RPC       :20   .00e0-c959-e700 / 20
RootPortId          :128.2 (GigabitEthernet0/0/2)
Root Type           :Normal
BPDU-Protection     :Disabled
```

```
STP Converge Mode   :Normal
Time since last TC  :0 days 0h:10m:46s
Number of TC        :1
Last TC occurred    :GigabitEthernet0/0/1
 ----[Port1(GigabitEthernet0/0/1)][DISCARDING]----
 Port Role          :Alternate Port
 Port Priority      :128
 Port Cost(Legacy)  :Config=20000 / Active=20000
 Desg. Bridge/Port  :32788.00e0-2539-c700 / 128.3
 Port Edged         :Config=Default / Active=Disabled
 Point-to-point     :Config=Auto / Active=true
 Transit Limit      :6 packets/hello
 Protection Type    :None
 Port STP Mode      :VBST
 BPDU Encapsulation :Config=VBST / Active=VBST
 BPDU Sent          :0
          TCN: 0, Config: 0, RST: 0
 BPDU Received      :0
          TCN: 0, Config: 0, RST: 0
```

Table 5-79 Description of the **display stp** command output

Item	Description
Bridge ID	Bridge ID.
Bridge Diameter	VBST network diameter.
Config Times	Time values in manually configured bridge protocol information: ● Hello: indicates the interval for sending BPDUs. ● MaxAge: indicates the maximum lifetime of BPDUs. ● FwDly: indicates the delay for port status transition.
Active Times	Time values in actual bridge protocol information: ● Hello: indicates the interval for sending BPDUs. ● MaxAge: indicates the maximum lifetime of BPDUs. ● FwDly: indicates the delay for port status transition.
Root ID / RPC	Root switch ID in a VLAN or external path cost from the local switch to the CIST root switch.
RootPortId	ID of the root port in a VLAN. The value 0.0 indicates that the switch is the root switch without the root port.
Root Type	Root bridge type.

Item	Description
BPDU-Protection	BPDU protection function: ● Disabled ● Enabled
STP Converge Mode	STP converge mode
Time since last TC	Period from the last topology change to now.
Number of TC	Topology change count.
Port Role	Role of the port.
Port Priority	Priority of the port. To set the priority for a port, run the **stp port priority** command.
Port Cost(Legacy)	Port path cost calculated using Huawei proprietary algorithm: ● Config: indicates the manually configured path cost. ● Active: indicates the actual path cost.
Desg. Bridge/Port	Designated bridge or port.
Port Edged	Edge port specified by the administrator: ● enabled: indicates that the edge port is enabled. ● disabled: indicates that the edge port is not enabled. Config indicates the value configured by the **stp edged-port** command; Active indicates the actual value.
Point-to-point	Link type of the port. Config indicates the link type configured by the **stp point-to-point** command; Active indicates the actual link type.
Transit Limit	Maximum number of BPDUs sent by the current interface in each Hello time. To set the maximum number of BPDUs sent per second on a port, run the **stp transmit-limit (interface view)** command.

Item	Description
Protection Type	Protection type: ● root-protection ● loop-protection ● None ● LoopBack: loopback detection
Port STP Mode	STP mode on an interface.
BPDU Encapsulation	Format of BPDUs that are sent and received on the interface. In STP/RSTP/MSTP mode, the value is stp. In VBST mode, the value is VBST.
BPDU Sent	Statistics about the packets sent by BPDU is as follows: ● TCN: topology change notification ● Config: STP packets ● RST: RSTP packets ● MST: MSTP packets
BPDU Received	Statistics about the packets received by BPDU.

# Display the status of and statistics on the spanning tree instance 0 on GE0/0/1.

```
<HUAWEI> display stp instance 0 interface gigabitethernet 0/0/1
-------[CIST Global Info][Mode MSTP]-------
CIST Bridge         :32768.00e0-fc0e-a421
Config Times        :Hello 2s MaxAge 20s FwDly 15s MaxHop 20
Active Times        :Hello 2s MaxAge 20s FwDly 15s MaxHop 20
CIST Root/ERPC      :32768.00e0-fc0e-a421 / 0 (This bridge is the root)
CIST RegRoot/IRPC   :32768.00e0-fc0e-a421 / 0 (This bridge is the root)
CIST RootPortId     :0.0
BPDU-Protection     :Disabled
TC or TCN received  :0
TC count per hello  :0
STP Converge Mode   :Normal
Share region-configuration :Enabled
Time since last TC  :0 days 23h:9m:30s
Number of TC        :1
Last TC occurred    :GigabitEthernet0/0/1
----[Port3(GigabitEthernet0/0/1)][FORWARDING]----
 Port Protocol       :Enabled
 Port Role           :Designated Port
 Port Priority       :128
 Port Cost(Legacy)   :Config=auto / Active=19
 Designated Bridge/Port   :32768.00e0-fc0e-a421 / 128.1229
 Port Edged          :Config=disabled / Active=disabled
 Point-to-point      :Config=auto / Active=true
 Transit Limit       :3 packets/hello-time
 Protection Type     :None
 Port STP Mode       :MSTP
 Config-digest-snoop :snooped=false
 Port Protocol Type  :Config=auto / Active=dot1s
 BPDU Encapsulation  :Config=stp / Active=stp
 PortTimes           :Hello 2s MaxAge 20s FwDly 15s RemHop 0
```

```
TC or TCN send      :0
TC or TCN received  :0
BPDU Sent           :147
         TCN: 0, Config: 0, RST: 0, MST: 147
BPDU Received       :0
         TCN: 0, Config: 0, RST: 0, MST: 0
```

Table 5-80 Description of the display stp instance command output

Item	Description
CIST Global Info	CIST global information.
Mode MSTP	The operation mode is MSTP. By default, the mode is MSTP. To set the operation mode, run the **stp mode** command.
CIST Bridge	ID of the CIST bridge. ● The previous 16 bits are the priority of the switch in CIST. ● The latter 48 bits is the MAC address of the switch. **NOTE** CIST Bridge is displayed when STP/RSTP/MSTP is running. Bridge ID is displayed when VBST is running.
Config Times	Value that is configured manually in the bridge protocol information: ● Hello: the period of sending BPDUs. ● MaxAge: the maximum life cycle of BPDU. ● FwDly: deferred time of the change of the port status. ● MaxHop: the maximum hops in the MST region.
Active Times	Value that is used actually in the bridge protocol information: ● Hello: the period of sending BPDUs. ● MaxAge: the maximum life cycle of BPDU. ● FwDly: deferred time of the change of the port status. ● MaxHop: the maximum hops in the MST region.
CIST Root/ERPC	CIST root bridge ID/External path cost (the path cost from the switch to the CIST root bridge.) **NOTE** CIST Root/ERPC is displayed when STP/RSTP/MSTP is running. Root ID / RPC is displayed when VBST is running.
CIST RegRoot/IRPC	Region root bridge ID/Internal path cost (the path cost from the switch to region root bridge.)

Item	Description
CIST RootPortId	CIST root port ID. "0.0" indicates the switch is a root bridge and has no root port. **NOTE** CIST RootPortId is displayed when STP/RSTP/MSTP is running. RootPortId is displayed when VBST is running.
BPDU-Protection	BPDU protection function: ● Disabled ● Enabled
TC or TCN received	Number of the received TC or TCN packets.
TC count per hello	Number of TC packets received within a hello interval.
STP Converge Mode	STP converge mode
Share region-configuration	The status of sharing the region configuration of process 0.
Time since last TC	Period from the last topology change to now.
Number of TC	Topology change count.
Last TC occurred	Interface which causes the last topology change **NOTE** This parameter does not appear when **Number of TC** is **0**.
Port Protocol	The status of the port protocol is as follows: ● Enable: STP is enabled on the port. ● disable: STP is disabled on the port.
Port Role	The port roles are as follows: ● Root Port ● Designated Port ● Alternate Port ● Backup Port ● Master port ● Disabled Port
Port Priority	Priority of the port. To set the priority for a port, run the **stp port priority** command.
Port Cost(Legacy)	Path cost of the port. It is calculated by dot1t algorithm. ● config: refers to the path cost that is configured manually. ● active: refers to the path cost actually.

Item	Description
Designated Bridge/ Port	ID of the designated switch and port. The first 16 bits of the switch ID represent the priority of the switch in the CIST region; the last 48 bits represent the MAC address of the switch. The first 4 bits of the port ID represent the priority and the last 12 bits represent the port number.
Port Edged	Edged port that is specified by the administrator: ● enabled ● disabled **Config** indicates that the value is configured by using the **stp edged-port** command. **Active** indicates the actual value.
Point-to-point	Link type of the port. **Config** indicates that the link type is configured by running the **stp point-to-point** command. **Active** indicates the actual link type.
Transit Limit	Limit of the BPDUs sent by the current port during each Hello time. To set the limit of the BPDUs sent by the current port during each Hello time, run the **stp transmit-limit (interface view)** command.
Protection Type	The protection type is as follows: ● root protection ● loop protection ● None ● LoopBack: loopback detection
Port STP Mode	STP mode on an interface.
Config-digest-snoop	The configuration digest snooping function. The command output is displayed only after the **stp config-digest-snoop** command is configured and the configuration digest snooping function is enabled on the port. If the port is not enabled with the function, the command output is not displayed: ● snooped=false: The configuration digest of the packets on the remote end is the same as that on the local end. ● snooped=true: The configuration digest of the packets on the remote end is different from that on the local end.

Item	Description
Port Protocol Type	Format of the packets that the interface receives and sends. The formats are as follows: ● auto ● legacy ● dot1s The default value is **auto**. **Config** indicates that the packet format is configured by running the **stp compliance** command. **Active** indicates the actual packet format.
BPDU Encapsulation	Format of BPDUs that are sent and received on the interface. In STP/RSTP/MSTP mode, the value is stp. In VBST mode, the value is VBST.
PortTimes	Values in the bridge protocol information of the interface: ● Hello: the period of sending BPDUs. ● MaxAge: the maximum life cycle of BPDU. ● FwDly: deferred time of the change of the port status. ● RemHop: the maximum hops in the MST region.
TC or TCN send	Number of BPDUs with TC flags or TCN BPDUs sent by the port.
TC or TCN received	Number of BPDUs with TC flags or TCN BPDUs received by the port.
BPDU Sent	Statistics about the packets sent by BPDU is as follows: ● TCN: topology change notification ● Config: STP packets ● RST: RSTP packets ● MST: MSTP packets
BPDU Received	Statistics about the packets received by BPDU.

5.12.6 display stp abnormal-interface

Function

The **display stp abnormal-interface** command displays information about abnormal interfaces running the Spanning Tree Protocol (STP).

Format

STP/RSTP/MSTP: **display stp** [**process** *process-id*] [**instance** *instance-id*] **abnormal-interface**

VBST: **display stp** [**vlan** *vlan-id*] **abnormal-interface**

Parameters

Parameter	Description	Value
process *process-id*	Displays the ID of a specified multi service transport platform (MSTP) process. If **process** *process-id* is not specified, the status and statistics of the MSTP process with ID 0 will be displayed.	The value is an integer in the range 1 to 31.
instance *instance-id*	Displays the status and statistics of a specified spanning tree instance. If **instance** *instance-id* is not specified, the status and statistics of all spanning tree instances will be displayed in the sequence of the interface numbers.	The value is an integer in the range 0 to 4094. The value **0** indicates a common and internal spanning tree (CIST) instance. **NOTE** *instance-id* ranges from 0 to 4094. Each process supports a maximum of 65 instances.
vlan *vlan-id*	Displays information about abnormal ports running STP in a specified VLAN. If **vlan** *vlan-id* is not specified, information about abnormal ports running STP in all VLANs is displayed. **NOTE** If **vlan** *vlan-id* is specified, only information about abnormal ports running VBST is displayed.	The value is an integer that ranges from 1 to 4094.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

If a device has many interfaces and the **display stp** command output displays vast information, viewing information about abnormal interfaces running STP is difficult.

You can use the **display stp abnormal-interface** command to view information about abnormal interfaces running STP.

Precautions

- If you run this command in the system view without specifying an MSTP process, information about MSTP process 0 is displayed by default.
- If you run this command in the MSTP process view without specifying an MSTP process, information about the MSTP process in this view is displayed by default.
- In VBST, if NAC authentication is configured but user authentication fails on a port that is configured as an edge port and is in Active state, information about the port is not displayed.

Example

# Display information about abnormal interfaces in process 0 running STP

```
<HUAWEI> display stp instance 0 abnormal-interface
MSTID    Interface                    Status          Reason
   0    GigabitEthernet0/0/0         DISCARDING      LOOP-Protected
   0    GigabitEthernet0/0/1         DOWN            BPDU-Protected
   0    GigabitEthernet0/0/2         DISCARDING      ROOT-Protected
   0    GigabitEthernet0/0/3         DISCARDING      LOOP-Detected
```

# Display information about abnormal ports running VBST in VLAN 5.

```
<HUAWEI> display stp vlan 5 abnormal-interface
VLAN    Interface                    Status          Reason
   5    GigabitEthernet0/0/0         DISCARDING      LOOP-Protected
   5    GigabitEthernet0/0/1         DOWN            BPDU-Protected
   5    GigabitEthernet0/0/2         DISCARDING      ROOT-Protected
   5    GigabitEthernet0/0/3         DISCARDING      LOOP-Detected
```

Table 5-81 Description of the **display stp abnormal-interface** command output

Item	Description
MSTID	MSTP instance ID
Interface	Interface type
Status	Status of an interface after the STP protection takes effect ● **DOWN**: indicates that the physical status of the interface is Down (including error-down). ● **DISCARDING**: indicates the blocked interface after the topology of the spanning tree becomes stable.

Item	Description
Reason	An interface running STP becomes abnormal due to one of the following: ● **ROOT-Protected**: indicates that the root protection takes effect. ● **LOOP-Protected**: indicates that the loop protection takes effect. ● **BPDU-Protected**: indicates that the BPDU protection takes effect. ● **LOOP-Detected**: indicates that the loop detection takes effect. ● **PVID-Inconsistency**: The PVID of the directly connected interface is inconsistent.
VLAN	VLAN ID.

5.12.7 display stp active

Function

The **display stp active** command displays the status of and statistics on spanning trees of all Up interfaces.

Format

STP/RSTP/MSTP: **display stp** [**process** *process-id*] **active**

VBST: **display stp** [**vlan** *vlan-id*] **active**

Parameters

Parameter	Description	Value
process *process-id*	Multiple Spanning Tree Protocol (MSTP) process ID If **process** *process-id* is not specified, the status of and statistics on process 0 will be displayed.	The value is an integer ranging from 1 to 31.

Parameter	Description	Value
vlan *vlan-id*	Displays details and statistics about spanning trees of all ports in Up state in a specified VLAN. If **vlan** *vlan-id* is not specified, details and statistics about spanning trees of all ports in Up state in all VLANs are displayed. **NOTE** If **vlan** *vlan-id* is specified, only details and statistics about spanning trees of all ports in Up state in a specified VLAN are displayed.	The value is an integer that ranges from 1 to 4094.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

The **display stp active** command displays information about spanning trees of Up interfaces only.

Precautions

- If you run this command in the system view without specifying an MSTP process ID, information about MSTP process 0 is displayed by default.
- If you run this command in the MSTP process view without specifying an MSTP process ID, information about the MSTP process in this view is displayed by default.
- In VBST, if NAC authentication is configured but user authentication fails on a port that is configured as an edge port and is in Active state, information about the port is not displayed.

Example

# Display information about spanning trees of all Up interfaces of MSTP process 0 when STP/RSTP/MSTP is running.

```
<HUAWEI> display stp active
-------[CIST Global Info][Mode MSTP]-------
CIST Bridge         :61440.781d-ba56-f06c
Config Times        :Hello 2s MaxAge 20s FwDly 15s MaxHop 20
Active Times        :Hello 2s MaxAge 20s FwDly 15s MaxHop 20
CIST Root/ERPC      :61440.781d-ba56-f06c / 0 (This bridge is the root)
CIST RegRoot/IRPC   :61440.781d-ba56-f06c / 0 (This bridge is the root)
CIST RootPortId     :0.0
BPDU-Protection     :Disabled
TC or TCN received  :85
TC count per hello  :0
STP Converge Mode   :Normal
Share region-configuration :Enabled
Time since last TC  :0 days 9h:10m:8s
Number of TC        :13
Last TC occurred    :GigabitEthernet0/0/4
----[Port18(GigabitEthernet0/0/10)][FORWARDING]----
 Port Protocol       :Enabled
 Port Role           :Designated Port
 Port Priority       :128
 Port Cost(Dot1T )   :Config=auto / Active=20000
 Designated Bridge/Port   :61440.781d-ba56-f06c / 128.18
 Port Edged          :Config=default / Active=enabled
 Point-to-point      :Config=auto / Active=true
 Transit Limit       :10 packets/s
 Protection Type     :None
 Port STP Mode       :MSTP
 Port Protocol Type  :Config=auto / Active=dot1s
 BPDU Encapsulation  :Config=stp / Active=stp
 PortTimes           :Hello 2s MaxAge 20s FwDly 15s RemHop 20
 TC or TCN send      :5
 TC or TCN received  :0
 BPDU Sent           :178445
          TCN: 0, Config: 0, RST: 0, MST: 178445
 BPDU Received       :0
          TCN: 0, Config: 0, RST: 0, MST: 0
 Last forwarding time: 2012/04/19 16:58:37 UTC+08:00
----[Port19(GigabitEthernet0/0/17)][FORWARDING]----
 Port Protocol       :Enabled
 Port Role           :Designated Port
 Port Priority       :128
 Port Cost(Dot1T )   :Config=auto / Active=20000
 Designated Bridge/Port   :61440.781d-ba56-f06c / 128.19
 Port Edged          :Config=default / Active=enabled
 Point-to-point      :Config=auto / Active=true
 Transit Limit       :10 packets/s
 Protection Type     :None
 Port STP Mode       :MSTP
 Port Protocol Type  :Config=auto / Active=dot1s
 BPDU Encapsulation  :Config=stp / Active=stp
 PortTimes           :Hello 2s MaxAge 20s FwDly 15s RemHop 20
 TC or TCN send      :0
 TC or TCN received  :0
 BPDU Sent           :5
          TCN: 0, Config: 0, RST: 0, MST: 5
 BPDU Received       :0
          TCN: 0, Config: 0, RST: 0, MST: 0
 Last forwarding time: 2012/04/23 20:06:08 UTC+08:00

-------[MSTI 1 Global Info]-------
MSTI Bridge ID      :61440.781d-ba56-f06c
MSTI RegRoot/IRPC   :61440.781d-ba56-f06c / 0(This bridge is the root)
MSTI RootPortId     :0.0
Master Bridge       :61440.781d-ba56-f06c
Cost to Master      :0
TC received         :2
TC count per hello  :0
Time since last TC  :0 days 9h:10m:8s
Number of TC        :9
Last TC occurred    :GigabitEthernet0/0/4
```

# Display details and statistics about spanning trees of all ports in Up state in VLAN 10 when VBST is running.

```
<HUAWEI> display stp vlan 10 active
-------[VLAN 10 Global Info][Mode VBST]-------
Bridge ID             :10   .00e0-5553-9900
Bridge Diameter        :7
Config Times           :Hello 2s MaxAge 20s FwDly 15s
Active Times           :Hello 2s MaxAge 20s FwDly 15s
```

```
Root ID / RPC          :10   .00e0-5553-9900 / 0 (This bridge is the root)
RootPortId             :0.0
Root Type              :Primary
BPDU-Protection        :Disabled
STP Converge Mode      :Normal
Time since last TC     :0 days 0h:10m:46s
Number of TC           :1
 ----[Port1(GigabitEthernet0/0/1)][FORWARDING]----
 Port Role             :Designated Port
 Port Priority         :128
 Port Cost(Legacy)     :Config=Auto / Active=20
 Desg. Bridge/Port     :10   .00e0-5553-9900 / 128.1
 Port Edged            :Config=Default / Active=Disabled
 Point-to-point        :Config=Auto / Active=True
 Port Revert Slow      :Disabled
 Port Agreement Legacy :Disabled
 Transit Limit         :6 packets/hello
 Protection Type       :None
 Port STP Mode         :VBST
 BPDU Encapsulation    :Config=VBST / Active=VBST
 BPDU Sent             :0
          TCN: 0, Config: 0, RST: 0
 BPDU Received         :0
          TCN: 0, Config: 0, RST: 0
```

Table 5-82 Description of the **display stp active** command output

Item	Description
CIST Bridge Bridge ID	CIST bridge: Bridge ID: **NOTE** CIST Bridge is displayed when STP/RSTP/MSTP is running. Bridge ID is displayed when VBST is running.
Bridge Diameter	VBST network diameter.
Config Times	Configured bridge protocol parameters: ● **Hello**: interval at which Bridge Protocol Data Units (BPDUs) are sent. To specify the parameter, run the **stp timer hello** command. ● **MaxAge**: maximum TTL of a BPDU. To specify the parameter, run the **stp timer max-age** command. ● **FwDly**: delay in interface status transition. To specify the parameter, run the **stp timer forward-delay** command. ● **MaxHop**: maximum number of hops in the MST region. To specify the parameter, run the **stp max-hops** command.
Active Times	Bridge protocol parameters that are being used: ● **Hello**: interval at which BPDUs are sent ● **MaxAge**: maximum TTL of a BPDU ● **FwDly**: delay in interface status transition ● **MaxHop**: maximum number of hops in the MST region

Item	Description
CIST Root/ERPC Root ID/RPC	CIST Root/ERPC indicates the CIST root bridge ID/ external path cost from the switch to the root bridge. Root ID/RPC indicates the root bridge ID in a VLAN/ external path cost from the switch to the root bridge. **NOTE** CIST Root/ERPC is displayed when STP/RSTP/MSTP is running. Root ID/RPC is displayed when VBST is running.
CIST RegRoot/IRPC	ID of the CIST region root bridge or cost of the path from the switch to the CIST region root switch.
CIST RootPortId RootPortId	CIST RootPortId indicates the CIST root port ID. "0.0" indicates that the switch is the root switch without the root port. RootPortId indicates the root port ID in a VLAN. "0.0" indicates that the switch is the root switch without the root port. **NOTE** CIST RootPortId is displayed when STP/RSTP/MSTP is running. RootPortId is displayed when VBST is running.
BPDU-Protection	Whether BPDU protection is enabled: ● **Disabled**: BPDU protection is disabled. ● **Enabled**: BPDU protection is enabled. To specify the parameter, run the **stp bpdu-protection** command.
TC or TCN received	Number of received topology change (TC) or topology change notification (TCN) BPDUs.
TC count per hello	Number of TC BPDUs received per Hello time.
STP Converge Mode	Convergence mode of the Spanning Tree Protocol (SPT), which can be **fast** or **normal**. For details, see **stp converge**.
Share region-configuration	The status of sharing the region configuration of process 0. The status is fixed as Enabled.
Time since last TC	Time since the last topology change.
Number of TC	Number of topology changes.
Last TC occurred	Interface which causes the last topology change. **NOTE** This parameter does not appear when **Number of TC** is **0**.

Item	Description
Port Protocol	STP status on the interface: ● **Enabled**: STP is enabled on the interface. ● **Disabled**: STP is disabled on the interface. To specify the parameter, run the **stp enable** command.
Port Role	Role of an interface: ● Root Port ● Designated Port ● Alternate Port ● Backup Port ● Master port ● Disabled Port
Port Priority	Interface priority. To configure the interface priority, run the **stp port priority** command.
Port Cost(Dot1T)	Path cost (calculated by dot1t) of an interface: ● **Config**: configured path cost ● **Active**: path cost that is being used To specify the parameter, run the **stp pathcost-standard** and **stp cost** commands.
Designated Bridge/ Port	Switch ID/Port ID The first 16 bits represent the switch's priority in the CIST region, and the last 48 bits represent the switch's MAC address. The first 4 bits of the port ID represent the port's priority, and the last 12 bits represent the port number.
Port Edged	Whether the edge interface (specified by the administrator) is enabled: ● **enabled**: The edge interface is enabled. ● **disabled**: The edge interface is disabled. **Config** indicates the value that is specified in the **stp edged-port** command, and **Active** indicates the value in use.
Point-to-point	Link type of the interface. **Config** indicates the link type that is specified in the **stp point-to-point** command, and **Active** indicates the link type that is being used.

Item	Description
Port Revert Slow	Delay in revertive switching during VBST calculation. - Enabled: The delay in revertive switching during VBST calculation is enabled on the interface. You can run the **stp revertive slow** command to enable this function. - Disabled: The delay in revertive switching during VBST calculation is disabled on the interface.
Port Agreement Legacy	Whether to discard non-standard STP/RSTP packets sent by a HanDreamnet switch. - Enabled: The interface discards non-standard STP/RSTP packets sent by a Handreamnet switch. You can run the **stp agreement-legacy** command to configure the interface to discard non-standard STP/RSTP packets sent by a HanDreamnet switch. - Disabled: The interface does not discard non-standard STP/RSTP packets sent by a Handreamnet switch.
Transit Limit	Maximum number of BPDUs that the current interface can send per second. For details, see **stp transmit-limit**.
Protection Type	Protection type, which can be: - Root: Enable the root protection. Protection takes effect only on the specified interface.To specify the parameter, run the **stp root-protection** command. - Loop: Enable loop protection. Protection takes effect only on the root interface or alternate interface.To specify the parameter, run the **stp loop-protection** command. - None. - Loopback: Enable loopback detection.
Port STP Mode	STP mode of the interface. To specify the parameter, run the **stp mode** command.
Port Protocol Type	Format of BPDUs sent and received on the interface, which can be: - auto - legacy - dot1s The default value is **auto**. **Config** indicates the packet format that is specified in the **stp compliance** command, and **Active** indicates the packet format in use.

Item	Description
BPDU Encapsulation	Format of BPDUs that are sent and received on the interface. In STP/RSTP/MSTP mode, the value is stp. In VBST mode, the value is VBST.
PortTimes	Bridge protocol parameters of the interface: ● **Hello**: interval at which BPDUs are sent. To specify the parameter, run the **stp timer hello** command. ● **MaxAge**: maximum TTL of a BPDU. To specify the parameter, run the **stp timer max-age** command. ● **FwDly**: delay in interface status transition. To specify the parameter, run the **stp timer forward-delay** command. ● **RemHop**: maximum number of hops in the MST region. To specify the parameter, run the **stp max-hops** command.
TC or TCN send	Number of TC or TCN BPDUs sent on the interface.
TC or TCN received	Number of TC or TCN BPDUs received on the interface.
BPDU Sent	Statistics on sent BPDUs, including: ● **TCN**: TCN BPDUs ● **Config**: STP BPDUs ● **RST**: Rapid Spanning Tree Protocol (RSTP) BPDUs ● **MST**: MSTP BPDUs
BPDU Received	Statistics on received BPDUs.
MSTI Bridge ID	Multiple Spanning Tree instance (MSTI) bridge ID.
MSTI RegRoot/IRPC	MSTI root bridge ID/Cost of the internal path (path from the switch to the MSTI root switch).
MSTI RootPortId	ID of the MSTI root interface. **0.0** indicates that the switch is the root switch and does not provide any root interface.
Master Bridge	ID of the bridge where the master interface is located. ● The first 16 bits represent the switch's priority in the CIST. ● The last 48 bits represent the switch's MAC address.
Cost to Master	Cost of the path from the switch to the bridge where the master interface is located. **0** indicates that the master interface is located at the current bridge.
TC received	Number of received TC BPDU.

5.12.8 display stp bridge

Function

The **display stp bridge** command displays details about the spanning tree of a bridge.

Format

STP/RSTP/MSTP: **display stp** [**process** *process-id*] **bridge** { **root** | **local** }

VBST: **display stp** [**vlan** *vlan-id*] **bridge** { **root** | **local** }

Parameters

Parameter	Description	Value
process *process-id*	Multiple Spanning Tree Protocol (MSTP) process ID If **process** *process-id* is not specified, details about the spanning tree of MSTP process 0 will be displayed.	The value is an integer ranging from 1 to 31.
root	Displays details about the spanning tree of the root bridge.	-
local	Displays details about the spanning tree of the local bridge.	-
vlan *vlan-id*	Displays details about the spanning tree of a bridge in a specified VLAN. If **vlan** *vlan-id* is not specified, details about the spanning trees of bridges in all VLANs are displayed. **NOTE** If **vlan** *vlan-id* is specified, only information about bridges running VBST is displayed.	The value is an integer that ranges from 1 to 4094.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

When a device provides many interfaces, running the **display stp** command displays a large amount of information, and it is difficult to find information about the spanning trees of the root and local bridges.

Using the **display stp bridge** command, you can easily view details about the spanning trees of the root and local bridges.

Precautions

- If you run this command in the system view without specifying an MSTP process ID, information about MSTP process 0 is displayed by default.
- If you run this command in the MSTP process view without specifying an MSTP process ID, information about the MSTP process in this view is displayed by default.

Example

# Display details about the spanning tree of the root bridge of MSTP process 0 when STP/RSTP/MSTP is running.

```
<HUAWEI> display stp bridge root
MSTID              Root ID  Root Cost Hello Max Forward Root Port
                                      Time Age   Delay
----- ------------------- ---------- ----- --- ------- -----------------
    0 61440.781d-ba56-f06c          0     2  20      15
    1 61440.781d-ba56-f06c          0     2  20      15
```

# Display details about the spanning tree of the root bridge running VBST in VLAN 5.

```
<HUAWEI> display stp vlan 5 bridge root
 VLAN-ID           Root ID  Root Cost Hello Max Forward Root
Port
                                      Time Age   Delay
----- ------------------- ---------- ----- --- ------- -----------------
    5 32773.5489-9876-a2b0      20000     2  20      15 GigabitEthernet0/0/5
```

Table 5-83 Description of the **display stp bridge** command output

Item	Description
MSTID	MSTP instance ID
Root ID	Root bridge ID
Root Cost	Root path cost
Hello Time	Interval at which Bridge Protocol Data Units (BPDUs) are sent from the root switch. To specify the parameter, run the **stp timer hello** command
Max Age	Maximum TTL of a BPDU. To specify the parameter, run the **stp timer max-age** command
Forward Delay	Delay in interface status transition. To specify the parameter, run the **stp timer forward-delay** command
Root Port	Root interface
VLAN-ID	VLAN ID.

5.12.9 display stp error packet

Function

The **display stp error packet** command displays the statistics about error packets received by MSTP and the contents of recently received packets.

Format

display stp error packet

Parameters

None.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

If a device on a Layer 2 network runs MSTP is attacked by MSTP error packets, the **display stp error packet** command can be used to view recently received MSTP error packets. Check the cause at the peer end.

Example

# Display the statistics about error packets received by MSTP and the contents of recently received packets.

```
<HUAWEI> display stp error packet
 4 error-packet(s) have been received and the last one is received at 2011/05/02 12:45:31.
01 80 C2 00 00 00 38 AA D2 11 11 10 00 69 42 42
03 00 00 03 02 7C 00 00 38 AA D2 11 11 10 00 00
00 00 00 00 38 AA D2 11 11 10 80 01 00 00 14 00
02 00 0F 00 00 00 40 00 33 38 61 61 64 32 31 31
31 31 31 30 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 AC 36 17 7F 50 28
3C D4 B8 38 21 D8 AB 26 DE 62 00 00 00 00 00 00
38 AA D2 11 11 10 14
```

5.12.10 display stp global

Function

The **display stp global** command displays global Spanning Tree Protocol (STP) information.

Format

display stp [**process** *process-id*] **global**

Parameters

Parameter	Description	Value
process *process-id*	Multiple Spanning Tree Protocol (MSTP) process ID If **process** *process-id* is not specified, the global STP information of MSTP process 0 will be displayed. VBST does not support processes. Therefore, this parameter cannot be specified when the spanning tree protocol is VBST.	The value is an integer ranging from 1 to 31.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

When a device provides many interfaces, the **display stp** command output contains a large amount of information, and it is difficult to find the desired information quickly and view global information at a glance. The **display stp brief** command output, by comparison, displays information about spanning trees on interfaces, but not global information.

Using the **display stp global** command, you can view global STP information conveniently.

Precautions

- If you run this command in the system view without specifying an MSTP process ID, information about MSTP process 0 is displayed by default.
- If you run this command in the MSTP process view without specifying an MSTP process ID, information about the MSTP process in this view is displayed by default.

Example

# Display brief STP information about MSTP process 0 when STP/RSTP/MSTP is running.

```
<HUAWEI> display stp global
Protocol Status            : Enabled
Bpdu-filter default        : Disabled
Tc-protection              : Enabled
Tc-protection threshold    : 1
Tc-protection interval     : 2s
Edged port default         : Enabled
Pathcost-standard          : Dot1t
```

```
Timer-factor               : 3
Transmit-limit             : 10
Bridge-diameter            : 7
-------[CIST Global Info][Mode MSTP]-------
CIST Bridge         :61440.781d-ba56-f06c
Config Times        :Hello 2s MaxAge 20s FwDly 15s MaxHop 20
Active Times        :Hello 2s MaxAge 20s FwDly 15s MaxHop 20
CIST Root/ERPC      :61440.781d-ba56-f06c / 0
CIST RegRoot/IRPC   :61440.781d-ba56-f06c / 0
CIST RootPortId     :0.0
BPDU-Protection     :Disabled
TC or TCN received  :85
TC count per hello  :0
STP Converge Mode   :Normal
Share region-configuration :Enabled
Time since last TC  :0 days 9h:12m:34s
Number of TC        :13
Last TC occurred    :GigabitEthernet0/0/4
```

# Display brief STP information when VBST is running.

```
<HUAWEI> display stp global
Protocol Status            : Enabled
Bpdu-filter default        : Disabled
Tc-protection              : Enabled
Tc-protection threshold    : 1
Tc-protection interval     : 2s
Edged port default         : Disabled
Pathcost-standard          : Dot1t
Timer-factor               : 3
Transmit-limit             : 6
STP Converge Mode          : Normal
```

Table 5-84 Description of the **display stp global** command output

Item	Description
Protocol Status	Spanning Tree Protocol (STP) status: ● **Enabled**: STP is enabled. ● **Disabled**: STP is disabled. To specify the parameter, run the **stp enable** command.
Bpdu-filter default	Whether the function of configuring device interfaces as Bridge Protocol Data Unit (BPDU) filter interfaces is enabled: ● **Enabled**: The function is enabled. ● **Disabled**: The function is disabled. To specify the parameter, run the **stp bpdu-filter default** command.
Tc-protection	Topology change (TC) protection status. This function is permanently enabled.
Tc-protection threshold	Threshold of TC packets that the device can handle and immediately refresh forwarding entries in a given period. To specify the parameter, run the **stp tc-protection threshold** command.

Item	Description
Tc-protection interval	Time the MSTP takes to handle a given number of TC packets and immediately refresh forwarding entries. To specify the parameter, run the **stp tc-protection interval** command.
Edged port default	Whether the function of configuring all ports of the switch as edge ports is enabled: ● **Enabled**: The function is enabled. ● **Disabled**: The function is disabled. To specify the parameter, run the **stp edged-port default** command.
Pathcost-standard	Method of calculating the MSTP path cost To specify the parameter, run the **stp pathcost-standard** command.
Timer-factor	Multiplier of Hello time To specify the parameter, run the **stp timer-factor** command.
Transmit-limit	Maximum number of BPDUs that the current interface can send per Hello time. For details, see **stp transmit-limit**.
Bridge-diameter	Network diameter of the MSTP To specify the parameter, run the **stp bridge-diameter** command.
CIST Bridge	Common and internal spanning tree (CIST) bridge ID ● The first 16 bits represent the switch's priority in the CIST. ● The last 48 bits represent the switch's MAC address.
Config Times	Configured bridge protocol parameters: ● **Hello**: interval at which BPDUs are sent. To specify the parameter, run the **stp timer hello** command. ● **MaxAge**: maximum TTL of a BPDU. To specify the parameter, run the **stp timer max-age** command. ● **FwDly**: delay in interface status transition. To specify the parameter, run the **stp timer forward-delay** command. ● **MaxHop**: maximum number of hops in the MST region. To specify the parameter, run the **stp max-hops** command.

Item	Description
Active Times	Bridge protocol parameters that are being used: ● **Hello**: interval at which BPDUs are sent ● **MaxAge**: maximum TTL of a BPDU ● **FwDly**: delay in interface status transition ● **MaxHop**: maximum number of hops in the MST region
CIST Root/ERPC	CIST root switch ID/Cost of the external path (path from the switch to the CIST root switch)
CIST RegRoot/IRPC	ID of the CIST region root bridge/Cost of the internal path (path from the switch to the CIST region root switch)
CIST RootPortId	ID of the CIST root interface. **0.0** indicates that the switch is the root switch and does not provide any root interface.
BPDU-Protection	Whether BPDU protection is enabled: ● **Disabled**: BPDU protection is disabled. ● **Enabled**: BPDU protection is enabled. To specify the parameter, run the **stp bpdu-protection** command.
TC or TCN received	Number of received TC or topology change notification (TCN) packets
TC count per hello	Number of TC packets received per Hello time
STP Converge Mode	Convergence mode of the Spanning Tree Protocol (SPT), which can be **fast** or **normal**. For details, see **stp converge**.
Share region-configuration	The status of sharing the region configuration of process 0. The status is fixed as Enabled.
Time since last TC	Time since the last topology change
Number of TC	Number of topology changes
Last TC occurred	Interface which causes the last topology change **NOTE** This parameter does not appear when **Number of TC** is **0**.

5.12.11 display stp region-configuration

Function

The **display stp region-configuration** command displays the effective configuration of the MST region on the switching device. The configuration includes the region name, revision level and mapping relationship between VLANs and spanning tree instances.

Format

display stp [**process** *process-id*] **region-configuration** [**digest**]

Parameters

Parameter	Description	Value
process *process-id*	Indicates the ID of an MSTP process. VBST does not support processes. Therefore, this parameter cannot be specified when the spanning tree protocol is VBST.	The value is an integer ranging from 1 to 31.
digest	Displays brief information about the effective MST region.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

After an MST region is configured and takes effect on the network running MSTP, you can run the **display stp region-configuration** command to view the name, revision level, STP instance, and inter-VLAN mapping of the MST region.

Precautions

- If you run this command in the system view without specifying an MSTP process, information about MSTP process 0 is displayed by default.
- If you run this command in the MSTP process view without specifying an MSTP process, information about the MSTP process in this view is displayed by default.

NOTE

For description about MSTP process 0, see **stp process**.

Example

# Display the configuration of MST regions when STP/RSTP/MSTP is running.

```
<HUAWEI> display stp region-configuration
Oper configuration
```

```
   Format selector :0
   Region name     :huawei
   Revision level  :0
   Instance   VLANs Mapped
      0       21 to 4094
      1       1 to 10
      2       11 to 20
```

# Display brief information about the effective MST region when STP/RSTP/MSTP is running.

```
<HUAWEI> display stp region-configuration digest
 Oper configuration
   Format selector    :0
   Region name        :huawei
   Revision level     :0
   Digest             :0xAC36177F50283CD4B83821D8AB26DE62
```

# Display the mapping between VLANs and MSTIs when VBST is running.

```
<HUAWEI> display stp region-configuration
 Oper configuration
   Format selector    :0
   Region name        :00e055539900
   Revision level     :0

   Instance Mode    VLANs Mapped
      0     default 1 to 9, 11 to 19, 21 to 29, 31 to 39, 41 to 4094
     10     static  10
     20     static  20
     30     static  30
     40     static  40
```

Table 5-85 Description of the display stp region-configuration command output

Item	Description
Format selector	Selection factors defined by the MSTP protocol.
Region name	Name of the MST region. For the related commands, see **region-name**.
Revision level	Revision level of the MST region. For the related commands, see **revision-level**.
Instance VLANs Mapped	Mapping between the spanning tree instance and VLANs of the MST region. For the related commands, see **instance** or **vlan-mapping modulo**. If the mapping is incorrect, run the **instance** command to re-map the specified VLAN to the specified MSTI and run the **active region-configuration** command to activate the mapping.
Digest	Brief information about the MST region.

Item	Description
Mode	Mode for the mapping between MSTIs and VLANs: ● Static ● Dynamic ● Default **NOTE** The mapping between MSTIs and VLANs can be statically configured or dynamically specified. The configuration of **instance** is static. The system dynamically allocates an instance ID to a new VLAN in ascending order. If an instance ID is statically configured for this VLAN, the statically configured one takes effect. That is, static configuration takes precedence over dynamic configuration.

5.12.12 display stp tc-bpdu statistics

Function

The **display stp tc-bpdu statistics** command displays statistics of sent and received topology change (TC) and topology change notification (TCN) BPDUs on interfaces.

Format

STP/RSTP/MSTP: **display stp** [**process** *process-id*] [**instance** *instance-id*] [**interface** *interface-type interface-number* | **slot** *slot-id*] **tc-bpdu statistics**

VBST: **display stp** [**vlan** *vlan-id*] [**interface** *interface-type interface-number* | **slot** *slot-id*] **tc-bpdu statistics**

Parameters

Parameter	Description	Value
process *process-id*	Specifies the ID of an MSTP process of which statistics of TC and TCN BPDUs are displayed. If the parameter **process** *process-id* is not specified, statistics of TC and TCN BPDUs in MSTP process 0 are displayed.	The value is an integer ranging from 1 to 31.

Parameter	Description	Value
instance *instance-id*	Specifies the ID of an MSTP instance of which statistics of TC and TCN BPDUs are displayed. If the parameter **instance** *instance-id* is not specified, statistics of TC and TCN BPDUs on all interfaces are displayed in the sequence of the interface numbers.	The value is an integer that ranges from 0 to 4094. The value 0 indicates a CIST instance. **NOTE** *instance-id* ranges from 0 to 4094. Each process supports a maximum of 65 instances.
interface *interface-type interface-number*	Specifies the interface on which statistics of TC and TCN BPDUs are displayed. If the parameter **interface** *interface-type interface-number* is not specified, statistics of TC and TCN BPDUs on all interfaces are displayed in the sequence of the interface numbers.	-
slot *slot-id*	Displays the statistics of TC and TCN BPDUs on a spanning tree instance in a specified slot.	The value is an integer and must be an existing slot on the device.
vlan *vlan-id*	Display statistics on sent and received TC and TCN BPDUs on ports in a specified VLAN. If **vlan** *vlan-id* is not specified, statistics on sent and received TC and TCN BPDUs on ports in all VLANs are displayed. **NOTE** If **vlan** *vlan-id* is specified, only statistics on sent and received TC and TCN BPDUs on ports running VBST are displayed.	The value is an integer that ranges from 1 to 4094.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

If you need to know whether a fault has occurred on interfaces that send and receive TC/TCN BPDUs, you can run this command to view statistics of these BPDUs and locate the fault.

Prerequisites

In VBST, if NAC authentication is configured but user authentication fails on a port that is configured as an edge port and is in Active state, information about the port is not displayed.

Example

# Display the statistics of TC/TCN BPDUs on interfaces of an MSTP instance when STP/RSTP/MSTP is running.

```
<HUAWEI> display stp tc-bpdu statistics
 -------------------------- STP TC/TCN information --------------------------
 MSTID Port                    TC(Send/Receive)      TCN(Send/Receive)
 0     GigabitEthernet0/0/9              3/2                  0/0
 0     GigabitEthernet0/0/10             1/0                  0/0
 1     GigabitEthernet0/0/9              14/9                 -/-
 1     GigabitEthernet0/0/10             8/10                 -/-
 2     GigabitEthernet0/0/9              3/2                  -/-
 2     GigabitEthernet0/0/10             1/0                  -/-
```

# Display statistics on sent and received TC and TCN BPDUs on ports running VBST.

```
<HUAWEI> display stp vlan 5 tc-bpdu statistics
 -------------------------- STP TC/TCN information
--------------------------
 VLAN-ID  Port                    TC(Send/Receive)      TCN(Send/
Receive)
      5  GigabitEthernet0/0/5        1/615                 0/0
```

Table 5-86 Description of the **display stp tc-bpdu statistics** command output

Item	Description
MSTID	ID of an MSTP instance.
Port	Interface name.
TC(Send/Receive)	Statistics of sent and received TC BPDUs.
TCN(Send/Receive)	Statistics of send and received TCN BPDUs. ("-" indicates that MSTP instances except MSTP instance 0 do not have TCN BPDUs sent and received.)
VLAN-ID	VLAN ID.

5.12.13 display stp topology-change

Function

The **display stp topology-change** command displays the statistics about topology changes.

Format

STP/RSTP/MSTP: **display stp** [**process** *process-id*] [**instance** *instance-id*] **topology-change**

VBST: **display stp** [**vlan** *vlan-id*] **topology-change**

Parameters

Parameter	Description	Value
process *process-id*	Displays statistics about the topology changes of a specified MSTP process. If this parameter is not specified, the statistics about the topology changes of MSTP process 0 are displayed.	The value is an integer ranging from 1 to 31.
instance *instance-id*	Displays statistics about the topology changes of a specified STP instance. If this parameter is not specified, the statistics about the topology changes of a CIST instance are displayed.	The value is an integer ranging from 0 to 4094. Value 0 refers to CIST. **NOTE** *instance-id* ranges from 0 to 4094. Each process supports a maximum of 65 instances.
vlan *vlan-id*	Displays statistics on topology changes in a specified VLAN. If **vlan** *vlan-id* is not specified, statistics on topology changes in all VLANs are displayed. **NOTE** If **vlan** *vlan-id* is specified, only statistics on topology changes of VBST are displayed.	The value is an integer that ranges from 1 to 4094.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

On a Layer 2 network running MSTP, a device clears ARP entries and MAC entries after receiving topology change packets. If a device receives too many topology change packets, the device will frequently clear ARP entries and MAC entries, causing high CPU usage. As a result, network traffic is instable.

The **display stp topology-change** command can be used to display the statistics about MSTP/VBST topology changes. If the statistics increase, network flapping occurs.

Prerequisites

In the case of a non-zero process, the **stp process** *process-id* command must be used to create a process.

Example

# Display statistics about MSTP topology changes when MSTP is running.

```
<HUAWEI> display stp topology-change
CIST topology change information
   Number of topology changes             :5
   Time since last topology change        :0 days 0h:23m:19s
   Topology change initiator(detected)    :GigabitEthernet0/0/1
   Topology change last received from     :00e0-5b3c-c100
   Number of generated topologychange traps :   5
   Number of suppressed topologychange traps:   3

 MSTI 1 topology change information
   Number of topology changes             :5
   Time since last topology change        :0 days 0h:23m:19s
   Topology change initiator(detected)    :GigabitEthernet0/0/2
   Number of generated topologychange traps :   5
   Number of suppressed topologychange traps:   3

 MSTI 2 topology change information
   Number of topology changes             :5
   Time since last topology change        :0 days 0h:23m:19s
   Topology change initiator(notified)    :GigabitEthernet0/0/3
   Number of generated topologychange traps :   5
   Number of suppressed topologychange traps:   3

 MSTI 3 topology change information
   Number of topology changes             :5
   Time since last topology change        :0 days 0h:23m:19s
```

# Display statistics on topology changes in VLAN 5 when VBST is running.

```
<HUAWEI> display stp vlan 5 topology-change
 VLAN 5 topology change information
   Number of topology changes             :316
   Topology change initiator(notified)    :GigabitEthernet0/0/5
   Time since last topology change        :0 days 0h:3m:18s
   Topology change last received from     :5489-9876-a2b0
```

Table 5-87 Description of the display stp topology-change command output

Item	Description
Number of topology changes	Total number of topology changes since initialization. **NOTE** The number of received and sent TC BPDUs in each VLAN may be different during topology convergence, so the number of topology changes in each VLAN may be different.
Time since last topology change	Time since the last topology change.

Item	Description
Topology change initiator(detected)	Interface that initiates a topology change because the interface status changes to detected.
Topology change initiator(notified)	Interface that initiates a topology change after receiving a topology change packet.
Topology change last received from	Source bridge MAC address contained in a topology change packet.
Number of generated topologychange traps	Total number of generated topology-change traps.
Number of suppressed topologychange traps	Total number of suppressed topology-change traps.

5.12.14 display stp vlan

Function

The **display stp vlan** command displays the STP status on an interface added to a specified VLAN.

Format

display stp vlan *vlan-id*

Parameters

Parameter	Description	Value
vlan-id	Displays the STP status on an interface added to a specified VLAN.	The value is an integer ranging from 1 to 4094.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

After an interface is added to a VLAN, the **display stp vlan** command can be used to the display the STP status on the interface. In this case, the mapping between VLANs and instances does not need to be concerned with.

Prerequisites

In VBST, if NAC authentication is configured but user authentication fails on a port that is configured as an edge port and is in Active state, information about the port is not displayed.

Example

# Display the STP status on an interface added to a specified VLAN when STP/RSTP/MSTP is running.

```
<HUAWEI> display stp vlan 1
     ProcessId   InstanceId   Port                     Role  State
 -------------------------------------------------------------------
       0           0       GE0/0/1                  DESI  FORWARDING
```

Table 5-88 Description of the **display stp vlan 1** command output

Item	Description
ProcessId	Process ID
InstanceId.	Instance ID
Port	Interface
Role	Interface role: ● DESI: Designated port ● ROOT: Root port ● ALTE: Alternate port ● BACK: Backup port ● MAST: Master port ● DISA: The interface is in initialization state.
State	Interface status: ● FORWARDING ● DISCARDING

# Display the spanning tree status on a port in a specified VLAN when VBST is running.

```
<HUAWEI> display stp vlan 20
-------[VLAN 20 Global Info][Mode VBST]-------
Bridge ID              :32788.4c1f-cc6b-c208
Bridge Diameter        :7
Config Times           :Hello 2s MaxAge 20s FwDly 15s
Active Times           :Hello 2s MaxAge 20s FwDly 15s
Root ID / RPC          :20   .781d-bacc-8bc0 / 199
RootPortId             :128.191 (GigabitEthernet0/0/7)
Root Type              :Normal
BPDU-Protection        :Disabled
STP Converge Mode      :Normal
Time since last TC     :0 days 0h:10m:46s
Number of TC           :1
 ----[Port190(GigabitEthernet0/0/6)][DISCARDING]----
 Port Role             :Designated Port
 Port Priority         :128
 Port Cost(Legacy)      :Config=20000 / Active=20000
 Desg. Bridge/Port      :32788.4c1f-cc6b-c208 / 128.190
 Port Edged             :Config=Default / Active=Disabled
 Point-to-point         :Config=Auto / Active=true
 Port Revert Slow       :Disabled
 Port Agreement Legacy :Disabled
 Transit Limit          :6 packets/hello
 Protection Type        :None
 Port STP Mode          :VBST
 BPDU Encapsulation     :Config=VBST / Active=VBST
 BPDU Sent              :0
          TCN: 0, Config: 0, RST: 0
 BPDU Received          :0
          TCN: 0, Config: 0, RST: 0
```

Table 5-89 Description of the **display stp vlan** command output

Item	Description
VLAN	VLAN ID.
Bridge ID	Bridge ID: ● The first 16 bits represent the switch's priority. ● The last 48 bits represent the switch's MAC address.
Bridge Diameter	VBST network diameter. To specify the parameter, run the **stp bridge-diameter** command.
Config Times	Configured bridge protocol parameters: ● **Hello**: interval at which Bridge Protocol Data Units (BPDUs) are sent. To specify the parameter, run the **stp timer hello** command. ● **MaxAge**: maximum TTL of a BPDU. To specify the parameter, run the **stp timer max-age** command. ● **FwDly**: delay in interface status transition. To specify the parameter, run the **stp timer forward-delay** command.
Active Times	Bridge protocol parameters that are being used: ● **Hello**: interval at which BPDUs are sent ● **MaxAge**: maximum TTL of a BPDU ● **FwDly**: delay in interface status transition
Root ID / RPC	Root switch ID or external cost of the path from the switch to the root switch.
RootPortId	Root port ID. The value 0.0 indicates that the root switch has no root port.
Root Type	Root bridge type.

Item	Description
BPDU-Protection	BPDU protection function: ● Disabled ● Enabled To specify the parameter, run the **stp bpdu-protection** command.
STP Converge Mode	STP converge mode. To specify the parameter, run the **stp converge** command.
Time since last TC	Period from the last topology change to now.
Number of TC	Topology change count.
Port Role	Role of a port: ● Root Port ● Designated Port ● Alternate Port ● Backup Port ● Disabled Port
Port Priority	Priority of the port. To set the priority for a port, run the **stp port priority** command.
Port Cost(Legacy)	Path cost of the port, which is calculated using Huawei proprietary algorithm: ● config: indicates the path cost that is manually configured. ● active: indicates the path cost that is actually used. To specify the parameter, run the **stp pathcost-standard** and **stp cost** commands.
Desg. Bridge/Port	IDs of the designated switch and designated port. In the switch ID, the first 16 bits represent the switch's priority, and the last 48 bits represent the switch's MAC address. In the port ID, the first 4 bits represents the port priority, and the last 12 bits represent the port number.
Port Edged	Status of the edge port that is specified by the administrator: ● enabled: The edge port is enabled. ● disabled: The edge port is disabled. Config indicates the value configured using the **stp edged-port** command, and Active indicates the actual value.
Point-to-point	Link type of the port. Config indicates link type configured using the **stp point-to-point** command, and Active indicates the actual link type.

Item	Description
Port Revert Slow	The delay in revertive switching during VBST calculation on a port: ● enabled: The delay in revertive switching is enabled. ● disabled: The delay in revertive switching is disabled. To specify the parameter, run the **stp revertive slow** command.
Port Agreement Legacy	Whether the interface discards non-standard STP/RSTP packets sent by the HanDreamnet switch: ● enabled: The interface discards non-standard STP/ RSTP packets sent by the HanDreamnet switch ● disabled: The interface does not discard non-standard STP/RSTP packets sent by the HanDreamnet switch
Transmit Limit	Maximum number of BPDUs sent by the port per second. To set the maximum number of BPDUs sent by the port per second, run the **stp transmit-limit (interface view)** command.
Protection Type	Protection type of the port: ● root-protection: takes effect only on the designated port. ● loop-protection: takes effect only on the root port or alternate port. To specify the parameter, run the **stp root-protection** or **stp loop-protection** command.
Port STP Mode	STP mode on an interface. To specify the parameter, run the **stp mode** command.
BPDU Encapsulation	Format of BPDUs that are sent and received on the interface.In VBST mode, the value is VBST.
BPDU Sent	Statistics about the packets sent by BPDU is as follows: ● TCN: topology change notification ● Config: STP packets ● RST: RSTP packets
BPDU Received	Statistics about the packets received by BPDU.

5.12.15 display vbst bpdu-statistics

Function

The **display vbst bpdu-statistics** command displays VBST BPDU statistics.

Format

display vbst bpdu-statistics [**vlan** *vlan-id*] [**interface** *interface-type interface-number* | **slot** *slot-id*]

Parameters

Parameter	Description	Value
vlan *vlan-id*	Displays VBST BPDU statistics in a specified VLAN. If **vlan** *vlan-id* is not specified, VBST BPDU statistics in all VLANs are displayed.	The value is an integer that ranges from 1 to 4094.
interface *interface-type interface-number*	Displays VBST BPDU statistics on a specified interface.	-
slot *slot-id*	Displays VBST BPDU statistics on a specified card.	The value is an integer and must be the slot ID of a running card.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

To check statistics on BPDUs on the switch running VBST, run the **display vbst bpdu-statistics** command.

Prerequisites

In VBST, if NAC authentication is configured but user authentication fails on a port that is configured as an edge port and is in Active state, information about the port is not displayed.

Example

# Display VBST BPDU statistics in VLAN 2.

```
<HUAWEI> display vbst bpdu-statistics vlan 2
-------[VLAN 2 ]-------
 ----[Port1010(GigabitEthernet0/0/17)]---
 BPDU Sent            :0
          TCN: 0, Config: 0, RST: 0
 BPDU Received        :0
          TCN: 0, Config: 0, RST: 0
```

```
----[Port1011(GigabitEthernet0/0/18)]---
BPDU Sent           :0
        TCN: 0, Config: 0, RST: 0
BPDU Received       :0
        TCN: 0, Config: 0, RST: 0
----[Port1012(GigabitEthernet0/0/19)]---
BPDU Sent           :0
        TCN: 0, Config: 0, RST: 0
BPDU Received       :0
        TCN: 0, Config: 0, RST: 0
----[Port1031(GigabitEthernet0/0/20)]---
BPDU Sent           :0
        TCN: 0, Config: 0, RST: 0
BPDU Received       :0
        TCN: 0, Config: 0, RST: 0
----[Port1033(GigabitEthernet0/0/21)]---
BPDU Sent           :14664
        TCN: 0, Config: 0, RST: 14664
BPDU Received       :3
        TCN: 0, Config: 0, RST: 3
----[Port1047(GigabitEthernet0/0/22)]---
BPDU Sent           :14643
        TCN: 0, Config: 0, RST: 14643
BPDU Received       :0
        TCN: 0, Config: 0, RST: 0
```

Table 5-90 Description of the **display vbst bpdu-statistics** command output

Item	Description
VLAN	VLAN ID.
Port	Port name.
BPDU Sent	Number of sent BPDUs. The number of sent BPDUs contains the number of sent TCP BPDUs, configuration BPDUs, and RST BPDUs.
TCN	Number of sent/received TCN BPDUs.
Config	Number of sent/received configuration BPDUs.
RST	Number of sent/received RST BPDUs.
BPDU Received	Number of received BPDUs. The number of received BPDUs contains the number of received TCP BPDUs, configuration BPDUs, and RST BPDUs.

5.12.16 display vbst port-vlan statistics

Function

The **display vbst port-vlan statistics** command displays statistics about the PV number of VBST.

Format

display vbst port-vlan statistics

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The PV number is the total number of VLANs in which VBST has been enabled and into which all VBST-enabled interfaces are added. For example, if VBST is enabled on 10 interfaces and each interface is added into 100 VLANs in which VBST is enabled, the number of PVs occupied by all interfaces on the switch is 1000. If the number of occupied PVs exceeds the specifications, the CPU usage may be high. As a result, the switch cannot process tasks in a timely manner, protocol calculation is affected, and the switch cannot be managed by the NMS.

After VBST is enabled on a switch, you can run the **display vbst port-vlan statistics** command to check statistics on the PV number, including the number of occupied PVs and the maximum number of PVs supported by the switch.

Example

# Display statistics on the PV number after VBST is enabled on a switch.

```
<HUAWEI> display vbst port-vlan statistics
  Statistics on Eth-Trunk:
--------------------------------------------------
Current PV Num : 6
Support PV Num : 1200
--------------------------------------------------
  Statistics on Slots:
--------------------------------------------------
Slot      Current PV Num      Support PV Num
--------------------------------------------------
0         317                 1200
```

Table 5-91 Description of the **display vbst port-vlan statistics** command output

Item	Description
Statistics on Eth-Trunk	Statistics on the PV number of Eth-Trunks.
Current PV Num	Number of PVs occupied by Eth-Trunks.
Support PV Num	Maximum number of PVs that can be occupied by Eth-Trunks on a switch.
Statistics on Slots	Statistics on the PV number of physical interfaces.

Item	Description
Slot	Slot ID.
Current PV Num	On a standalone switch, this field indicates the number of PVs occupied by physical interfaces. In a stack, this field indicates the number of PVs occupied by physical interfaces of member switches.
Support PV Num	On a standalone switch, this field indicates the maximum number of PVs that can be occupied by physical interfaces. In a stack, this field indicates the maximum number of PVs that can be occupied by physical interfaces of member switches.

5.12.17 ethernet-loop-protection ignored-vlan

Function

The **ethernet-loop-protection ignored-vlan** command configures ignored VLANs for a device. Through the loop protocol calculation, the interface on which the ignored VLAN is configured does not enter the blocked state but stays in the forwarding state.

The **undo ethernet-loop-protection ignored-vlan** command restores the ignored VLAN to the default setting.

By default, no ignored VLAN is configured for a device.

Format

ethernet-loop-protection ignored-vlan { *vlan-id1* [**to** *vlan-id2*] } &<1-10>

undo ethernet-loop-protection ignored-vlan { { *vlan-id1* [**to** *vlan-id2*] } &<1-10> | **all** }

Parameters

Parameter	Description	Value
vlan-id1	Specifies the ID of a start VLAN.	The value is an integer ranging from 1 to 4094.
to *vlan-id2*	Specifies the ID of an end VLAN. *vlan-id2* and *vlan-id1* together specify a VLAN range. If you do not specify **to** *vlan-id2*, only the VLAN with ID of *vlan-id1* is configured to the ignored VLAN.	The value is an integer ranging from 1 to 4094. The value of *vlan-id2* must be greater than that of *vlan-id1*.

Parameter	Description	Value
all	Restore all the ignored VLAN to the default setting.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If a device uses a specific VLAN to create a VLANIF interface and configure it as the management network port, Layer 2 loop protocols (MSTP/RRPP/SEP/ERPS/Smart Link) are enabled on the device to prevent network loops. After the device starts or the Layer 2 loop protocols are enabled, the VLANIF interface enters the blocked state and needs to wait a long time to enter the forwarding state through the protocol calculation. During this period, services are interrupted, and users who use the VLANIF interface cannot operate the device.

To resolve the problem, the **ethernet-loop-protection ignored-vlan** command can be used to configure the specific VLAN to an ignored VLAN. Through loop protocol calculation, the interface on which the ignored VLAN is configured does not enter the blocked state but stays in the forwarding state.

Precautions

If the **ethernet-loop-protection ignored-vlan** command is run more than once, all configurations take effect.

If an ignored VLAN is configured on a ring network, a loop occurs. Therefore, you cannot configure an ignored VLAN in a ring topology.

After the **ethernet-loop-protection ignored-vlan** command is executed, the configuration file shows that STP has been disabled in the VLAN, for example, **stp vlan 100 disable**.

After the **undo ethernet-loop-protection ignored-vlan** command is executed, the system checks whether the number of instances exceeds the limit. If so, the system restores the VBST status in the VLAN. If not, the system displays a message about a failure to restore the VBST status in the VLAN.

Example

# Configure VLAN 2 as an ignored VLAN.

```
<HUAWEI> system-view
[HUAWEI] ethernet-loop-protection ignored-vlan 2
Warning: This operation may result in bridging loops. Please make sure there are
 no bridging loops in the VLAN(s). Continue?[Y/N]:Y
```

5.12.18 instance

Function

The **instance** command maps a VLAN to a spanning tree instance.

The **undo instance** command deletes the mapping between a VLAN and a spanning tree instance.

By default, all VLANs are mapped to CIST, that is, instance 0.

Format

instance *instance-id* **vlan** { *vlan-id1* [**to** *vlan-id2*] } &<1-10>

undo instance *instance-id* [**vlan** { *vlan-id1* [**to** *vlan-id2*] } &<1-10>]

Parameters

Parameter	Description	Value
instance-id	Specifies the number of a spanning tree instance.	The value is an integer ranging from 0 to 4094. Value 0 refers to CIST. **NOTE** *instance-id* ranges from 0 to 4094. Each process supports a maximum of 65 instances.
vlan *vlan-id1*	Specifies a start VLAN ID.	The value is an integer ranging from 1 to 4094. The start VLAN ID must be smaller than the end VLAN ID.
to *vlan-id2*	Specifies an end VLAN ID. **NOTE** ● VBST maps one VLAN to one instance. Therefore, this parameter cannot be specified when the spanning tree protocol is VBST. ● The 1:1 mapping between MSTIs and VLANs are used only by the switch to determine the VBST forwarding status. This does not mean that VBST supports multi-instance. **instance** in other commands cannot be specified when VBST is running.	The value is an integer that ranges from 1 to 4094.

Views

MST region view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

MSTP divides a switching network into multiple regions, each of which has multiple spanning trees that are independent of each other. Each spanning tree is called an MSTI and each region is called an MST region.

Two switching devices belong to the same MST region only when they have the following same configurations:

- MST region name
- Mappings between MSTIs and VLANs
- MST region revision level

The **instance** command is used to set mappings between spanning tree instances and VLANs.

Precautions

When using the **undo instance** command, note the following points:

- After the mapping between specified VLANs and a specified spanning tree instance is deleted, these VLANs will be mapped to a CIST, namely, instance 0.
- If no VLAN is specified, all VLANs that have established mappings with the spanning tree instance will be mapped to a CIST.

If the **instance** command is run more than once, all configurations take effect.

A VLAN cannot be mapped to different spanning tree instances. If the **instance** command is run several times, the latest configuration overrides the previous one.

To map the MUX VLAN to a spanning tree instance, you are advised to configure the principal VLAN, subordinate group VLAN, and subordinate separate VLAN in the MUX VLAN in the same spanning tree instance.

Example

# Map VLAN 2 to spanning tree instance 1.

```
<HUAWEI> system-view
[HUAWEI] stp region-configuration
[HUAWEI-mst-region] instance 1 vlan 2
```

5.12.19 max bandwidth-affected-linknumber

Function

The **max bandwidth-affected-linknumber** command sets the upper threshold for the number of interfaces that determine the bandwidth of an Eth-Trunk.

The **undo max bandwidth-affected-linknumber** command restores the default upper threshold for the number of interfaces that determine the bandwidth of an Eth-Trunk.

By default, the upper threshold for the number of interfaces that determine the bandwidth of an Eth-Trunk is 32 on the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S, 16 on the S5735S-H, S5736-S, and S6720S-S, and 8 on other models.

Format

max bandwidth-affected-linknumber *link-number*

undo max bandwidth-affected-linknumber

Parameters

Parameter	Description	Value
link-number	Specifies the upper threshold for the number of interfaces that determine the bandwidth of an Eth-Trunk.	The value is an integer that ranges from 1 to 32 on the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S, 1 to 16 on the S5735S-H, S5736-S, and S6720S-S, and 1 to 8 on other models. On the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, S6730S-S, S6735-S, S6720-EI, and S6720S-EI, you can run the **assign trunk** command to set the value, and run the **display trunk configuration** command to check the configuration.

Views

Eth-Trunk interface view

Default Level

2: Configuration level

Usage Guidelines

The upper threshold for the number of interfaces that determine the bandwidth of an Eth-Trunk is used for STP calculation.

For example, device A and device B are connected by two Eth-Trunks. Eth-Trunk1 has three member links that are Up; the Eth-Trunk2 has two member links that are Up. The bandwidth of each member link is 1 Gbit/s, so the bandwidth of Eth-Trunk1 is 3 Gbit/s and the bandwidth of Eth-Trunk2 is 2 Gbit/s. If device A is the root bridge during STP calculation, Eth-Trunk1 on device B is the root port and Eth-Trunk2 is the alternate port. You can run this command to set the upper threshold to 1. Then the bandwidth of Eth-Trunk1 becomes 1 Gbit/s during STP calculation. Bandwidth decrease affects the interface cost, causing STP recalculation. The **max bandwidth-affected-linknumber** command does not affect traffic forwarding on the Eth-Trunk. The bandwidth used to forward traffic is still 3 Gbit/s.

Example

# Set the upper threshold to 3.

```
<HUAWEI> system-view
[HUAWEI] interface eth-trunk 1
[HUAWEI-Eth-Trunk1] max bandwidth-affected-linknumber 3
```

5.12.20 region-name

Function

The **region-name** command configures the MST region name of the switching device.

The **undo region-name** command restores the default name.

By default, the MST region name is the MAC address of the bridge MAC of the switching device.

Format

region-name *name*

undo region-name

Parameters

Parameter	Description	Value
name	Specifies the region name of the switching device.	The value is a case-sensitive string of 1 to 32 characters without spaces. **NOTE** When double quotation marks are used around the string, spaces are allowed in the string.

Views

MST region view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

MSTP divides a switching network into multiple regions, each of which has multiple spanning trees that are independent of each other. Each spanning tree is called an MSTI and each region is called an MST region.

Two switching devices belong to the same MST region only when they have the following same configurations:

- MST region name
- Mappings between MSTIs and VLANs
- MST region revision level

The **region-name** command is used to configure MST region names in order to identify different regions.

VBST does not support regions. Therefore, this command does not take effect when the spanning tree protocol is VBST.

Follow-up Procedure

After configuring MST region parameters, run the **active region-configuration** command to activate the MST region configurations.

Precautions

If an MST region name is changed several times, only the last configuration activated using the **active region-configuration** command takes effect.

Example

# Set the MST region name of the switch to "huawei".

```
<HUAWEI> system-view
[HUAWEI] stp region-configuration
[HUAWEI-mst-region] region-name huawei
```

5.12.21 reset stp error packet statistics

Function

The **reset stp error packet statistics** command clears the statistics of error STP packets.

Format

reset stp error packet statistics

Parameters

None

Views

All views

Default Level

3: Management level

Usage Guidelines

Applicable Scenario

You can use the **reset stp error packet statistics** command to clear the history statistics when you need to observe the statistics of error STP packets in a period from the current time.

Precautions

The **reset stp error packet statistics** command clears the statistics about error STP packets are cleared and cannot be restored. Therefore, confirm the action before you use the command.

Example

# Clear the statistics about error STP packets.

```
<HUAWEI> reset stp error packet statistics
```

5.12.22 reset stp statistics

Function

The **reset stp statistics** command clears the statistics of a spanning tree.

Format

reset stp [**interface** *interface-type interface-number*] **statistics**

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Specifies an interface type and the number of the interface.	-

Views

User view

Default Level

3: Management level

Usage Guidelines

Sometimes, traffic statistics within a certain period are needed. In this situation, clear the existing statistics before restarting the count.

When you run the **reset stp statistics** command:

- If you specify an interface, you can clear the statistics of a spanning tree on the interface.
- If you do not specify an interface, you can clear the statistics of spanning trees on all interfaces.

Example

# Clear the statistics of spanning trees on GE0/0/1.

```
<HUAWEI> reset stp interface gigabitethernet 0/0/1 statistics
```

5.12.23 reset vbst bpdu-statistics

Function

The **reset vbst bpdu-statistics** command clears VBST BPDU statistics.

Format

reset vbst bpdu-statistics [**interface** *interface-type interface-number* | **slot** *slot-id*]

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Clears BPDU statistics on a specified interface running VBST.	-
slot *slot-id*	Clears BPDU statistics on interfaces running VBST on the card in a specified slot.	The value is an integer and must be an existing slot on the device.

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

Before re-collecting VBST BPDU statistics on a specified interface or on the card in a specified slot in a specified period of time, run the **reset vbst bpdu-statistics** command to clear existing VBST BPDU statistics.

Configuration Impact

The cleared VBST BPDU statistics on a specified interface or on the card in a specified slot cannot be restored. Exercise caution when running the **reset vbst bpdu-statistics** command.

Example

# Clear VBST BPDU statistics on GE 0/0/1.

```
<HUAWEI> reset vbst bpdu-statistics interface gigabitethernet 0/0/1
```

5.12.24 revision-level

Function

The **revision-level** command configures the revision level of MST region of a switching device.

The **undo revision-level** command restores the default level.

By default, the revision level of MST region is 0.

Format

revision-level *level*

undo revision-level

Parameters

Parameter	Description	Value
level	Specifies the revision level of the MST region.	The value is an integer ranging from 0 to 65535.

Views

MST region view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

MSTP divides a switching network into multiple regions, each of which has multiple spanning trees that are independent of each other. Each region is called an MST region and each spanning tree is called a multiple spanning tree instance (MSTI).

Two switching devices belong to the same MST region only when they have the following same configurations:

- MST region name

- Mappings between MSTIs and VLANs
- MST region revision level

To perform tree calculation in an MST region, multiple devices in this region must have the same value for the three parameters. If the parameters are changed after MSTP is deployed, the change will cause spanning tree recalculation and route flapping on the network. As a result, you are advised not to change the MST region parameters after MSTP is deployed.

If two switching devices have the same region name and VLAN mapping table, the **revision-level** command can be used to set different revision levels for the two devices so that the two devices belong to different MST regions.

MSTP is a standard protocol; therefore, the MSTP revision level of a device is 0 by default. If the revision level of some devices from a specified manufacturer is not 0, you must change the MSTP revision level of devices to be the same to facilitate tree calculation in an MST region.

VBST does not support regions. Therefore, this command does not take effect when the spanning tree protocol is VBST.

Follow-up Procedure

After configuring MST region parameters, run the **active region-configuration** command to activate the MST region configurations.

Precautions

If an MST region revision level is changed several times, only the latest configuration activated using the **active region-configuration** command takes effect.

Example

# Set the MSTP revision level of the switching device to 5.

```
<HUAWEI> system-view
[HUAWEI] stp region-configuration
[HUAWEI-mst-region] revision-level 5
```

5.12.25 stp agreement-legacy

Function

The **stp agreement-legacy** command configures an interface to discard non-standard STP/RSTP packets sent by the HanDreamnet switch.

The **undo stp agreement-legacy** command cancels the configuration.

By default, an interface does not discard non-standard STP/RSTP packets sent by the HanDreamnet switch.

Format

stp agreement-legacy

undo stp agreement-legacy

Parameters

None

Views

Ethernet interface view, GE interface view, XGE interface view, MultiGE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, port group view, 25GE interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If Huawei datacom device and HanDreamnet switch are deployed on the VBST network, non-standard STP/RSTP packets sent by the HanDreamnet switch may cause temporary loops. You can run the **stp agreement-legacy** command to configure the interface to discard non-standard STP/RSTP packets to prevent temporary loops.

Example

# Configure the GE0/0/1 to discard non-standard STP/RSTP packets sent by the HanDreamnet switch.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] stp agreement-legacy
```

5.12.26 stp binding process

Function

The **stp binding process** command adds the current interface to a specified MSTP process.

The **undo stp binding process** command removes the current interface from the specified MSTP process.

By default, the interface belongs to MSTP process with ID 0.

Format

stp binding process *process-id*

undo stp binding process *process-id*

Parameters

Parameter	Description	Value
process-id	Specifies the ID of an MSTP process.	The value is an integer ranging from 1 to 31.

Views

Ethernet interface view, GE interface view, XGE interface view, MultiGE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, port group view, 25GE interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After an MSTP device properly starts, each port of this device belongs to MSTP process 0 by default. Links connecting MSTP devices and access rings are called access links. If multiple processes are required to isolate services on access rings, the **stp binding process** command can be used to add ports on access links to specified MSTP processes.

Prerequisites

The **stp process** command has been run to configure the corresponding MSTP process. This means that the MSTP process to which a port will be added already exists.

Precautions

A port on an access link can be added to only one MSTP process. If the **stp binding process** command is run several times to add a port to different MSTP processes, only the latest configuration takes effect.

Example

# Add a port to MSTP process 1.

```
<HUAWEI> system-view
[HUAWEI] stp process 1
[HUAWEI-mst-process-1] quit
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] stp binding process 1
```

5.12.27 stp binding process link-share

Function

The **stp binding process link-share** command adds an interface to multiple MSTP processes for status calculation.

The **undo stp binding process** command removes the interface from status calculation of a certain MSTP process.

By default, an interface enabled with MSTP participates only in the status calculation of MSTP process 0.

Format

stp binding process *process-id1* [**to** *process-id2*] **link-share**

undo stp binding process *process-id1* [**to** *process-id2*]

Parameters

Parameter	Description	Value
process-id1	Specifies the ID of the start MSTP process.	The value is an integer ranging from 1 to 31.
to *process-id2*	Specifies the ID of the end MSTP process.	The value is an integer ranging from 1 to 31.

Views

Ethernet interface view, GE interface view, XGE interface view, MultiGE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, port group view, 25GE interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On a Layer 2 network running MSTP, the link shared by multiple access rings is called a public link. A port on a public link participates in the spanning tree calculation for multiple MSTP processes and access rings. As a result, the port may have multiple statuses. Which spanning tree status can be used as the port status cannot be determined. To prevent this situation, the **stp binding process link-share** command can be used to add this port to an MSTP process. Then, the port always uses its status in MSTP process 0 after participating in the calculation for multiple MSTP processes.

Precautions

After the **stp binding process link-share** command is run on a port, the port will perform the following operations:

- Participates in the status calculation of a specified MSTP process without affecting packet forwarding of this MSTP process.
- Participates in the status calculation of MSTP process 0, affecting packet forwarding of this MSTP process.

If the **stp binding process link-share** command is run more than once, all configurations take effect.

The port configured with the **stp binding process link-share** command must be a port on the public link between devices configured with MSTP multi-process, but not a port that connects an access ring and a device.

If a process has a public link, the **stp enable** command must be run in the view of this process to enable MSTP globally.

For a port that is added to the process in link-share mode, you must run the **stp enable** command in the interface view to enable MSTP.

For a port that is added to the process in link-share mode, the port participates in status calculation of MSTP process 0. Therefore, you must run the **stp enable** command to enable MSTP for process 0.

Example

# Configure the port to participate in the status calculation of MSTP process 1 and MSTP process 2.

```
<HUAWEI> system-view
[HUAWEI] stp process 1
[HUAWEI-mst-process-1] quit
[HUAWEI] stp process 2
[HUAWEI-mst-process-2] quit
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] stp binding process 1 to 2 link-share
```

5.12.28 stp bpdu-filter

Function

The **stp bpdu-filter enable** command specifies a port as a BPDU-filter port.

The **stp bpdu-filter disable** command specifies a port as a non-BPDU-filter port.

The **undo stp bpdu-filter** command restores the default attribute of a BPDU-filter port.

By default, a port is a non-BPDU-filter port.

Format

stp bpdu-filter { **enable** | **disable** }

undo stp bpdu-filter

Parameters

None

Views

Ethernet interface view, GE interface view, XGE interface view, MultiGE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, port group view, 25GE interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On a network running a spanning tree protocol, if the **stp edged-port enable** command is used to configure a port as an edge port, the port will not participate in the spanning tree calculation. This speeds up network convergence and improves network stability. This port, however, will still send BPDUs. This may cause BPDUs to be sent to other networks. As a result, these networks flap.

The **stp bpdu-filter enable** command can be used on the port to address this problem. After the **stp bpdu-filter enable** command is used on the port, the port will become a BPDU-filter port, and will not process BPDUs.

NOTICE

If the **stp bpdu-filter enable** command is run on a port, the port will not transmit or process BPDUs. The port cannot negotiate the STP status with the directly connected port on the remote device. Therefore, exercise cautions when using the **stp bpdu-filter enable** command. Running the **stp bpdu-filter enable** command only on edge ports is recommended.

Running the **stp bpdu-filter enable** command in the interface view configures only the current port as a BPDU-filter port. If multiple BPDU-filter ports are required on a device, the **stp bpdu-filter default** command can be used in the system view to configure all the ports as BPDU-filter ports. If some ports need to participate in spanning tree calculation but do not need to be configured as BPDU-filter ports, the **stp bpdu-filter disable** command can be used in the view of these ports to configure them as non-BPDU-filter ports. Similarly, if the **stp bpdu-filter disable** command has been run on a port, the non-BPDU filter port attributes of the port will not change after the **stp bpdu-filter default** command is run.

Precautions

After the **stp bpdu-filter disable** command is run on a port, the port becomes a non-BPDU-filter port. The port is still a non-BPDU-filter port even if the **stp bpdu-filter default** command is run in the system view. After the **undo stp bpdu-filter** command is run on the port, the BPDU-filter attributes of the port restore to the default ones.

Example

# On a network edge device, specify GE0/0/1 as a non-BPDU-filter port.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] stp bpdu-filter disable
```

# On a network edge device, specify GE0/0/1 as a BPDU-filter port.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
```

```
[HUAWEI-GigabitEthernet0/0/1] stp bpdu-filter enable
```

5.12.29 stp bpdu-filter default

Function

The **stp bpdu-filter default** command specifies all edge ports of a device as BPDU filter ports.

The **undo stp bpdu-filter default** command specifies all edge ports of a device as non-BPDU filter ports.

By default, a port is a non-BPDU filter port.

Format

stp bpdu-filter default

undo stp bpdu-filter default

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On a network running a spanning tree protocol, if the **stp edged-port enable** command is used to configure a port as an edge port, the port will not participate in the spanning tree calculation. This speeds up network convergence and improves network stability. This port, however, will still send BPDUs. This may cause BPDUs to be sent to other networks. As a result, these networks flap.

The **stp bpdu-filter enable** command can be used on the port to address this problem. After the **stp bpdu-filter enable** command is used on the port, the port will become a BPDU filter port, and will not process BPDUs.

Running the **stp bpdu-filter enable** command in the interface view configures only the current edge port as a BPDU filter port. If multiple BPDU filter ports are required on a device, the **stp bpdu-filter default** command can be used in the system view to configure all edge ports as BPDU filter ports. Then run the **stp bpdu-filter disable** command in the interface view to change the interfaces that do not need to be configured as BPDU filter interfaces into non-BPDU filter interfaces.

Precautions

After the **stp bpdu-filter default** command is run, a port that has been configured with the **undo stp bpdu-filter** command will become a BPDU filter port. After the **stp bpdu-filter disable** command is run, the port that has been configured with the **undo stp bpdu-filter** command, however, will still serve as a non-BPDU filter port.

NOTICE

After the **stp bpdu-filter default** and **stp edged-port default** commands are run in the system view, none of the ports on the device will initiate any BPDUs or initiate a negotiation with the remote device, and all the ports are in the forwarding state. This may lead to a loop and cause a broadcast storm. Exercise caution when using the **stp bpdu-filter default** and **stp edged-port default** commands in the system view.

Example

# On a network edge device, specify all ports as BPDU filter ports.

```
<HUAWEI> system-view
[HUAWEI] stp bpdu-filter default
```

5.12.30 stp bpdu-protection

Function

The **stp bpdu-protection** command enables BPDU protection on a switching device.

The **undo stp bpdu-protection** command disables BPDU protection on a switching device.

By default, the BPDU protection is disabled.

Format

stp bpdu-protection

undo stp bpdu-protection

Parameters

None.

Views

System view or MSTP process view

NOTE

VBST does not support processes. When VBST is running, you cannot run the **stp bpdu-protection** command in the MSTP process view.

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On a Layer 2 network running a spanning tree protocol, a port connected to terminals does not need to participate in spanning tree calculation. If the port participates in spanning tree calculation, the network convergence speed will be affected. In addition, status changes of the port may cause network flapping, interrupting user traffic. To address this problem, you can run the **stp edged-port enable** command to configure the port as an edge port. Then, the port will not participate in the spanning tree calculation. This speeds up network convergence and improves network stability.

An edge port will lose edge port attributes after receiving BPDUs. To prevent attackers from forging BPDUs to change edge ports to non-edge ports, you can run the **stp bpdu-protection** command to configure BPDU protection on a switching device.

Configuration Impact

After BPDU protection is enabled on a switching device, the switching device shuts down the edge port if the edge port receives a BPDU. The attributes of the edge port are not changed.

Precautions

After BPDU protection is enabled, a switching device sets an edge port to error down state if the edge port receives a BPDU and retains the port as an edge port. To configure the edge port in error-down state to automatically restore to the Up state, run the **error-down auto-recovery cause bpdu-protection interval** *interval-value* command in the system view.

By default, an interface cannot automatically restore to Up state after it is shut down. To restore the interface, run the **shutdown** and **undo shutdown** commands on the interface in sequence. Alternatively, run the **restart** command on the interface to restart the interface.

To configure the interface to go Up automatically, run the **error-down auto-recovery cause bpdu-protection interval** *interval-value* command in the system view to set a recovery delay. After the delay, the interface goes Up automatically.

The edge port generated by automatic detection is not protected by BPDUs. When the edge port receives BPDUs, the port is not shutdown.

Example

# Enable the BPDU protection on the switching device.

```
<HUAWEI> system-view
[HUAWEI] stp bpdu-protection
```

5.12.31 stp bridge-diameter

Function

The **stp bridge-diameter** command configures the diameter of the spanning tree.

The **undo stp bridge-diameter** command restores the default diameter.

By default, the diameter of the spanning tree is 7.

Format

stp [**vlan** { *vlan-id1* [**to** *vlan-id2*] } &<1-10>] **bridge-diameter** *diameter*

undo stp [**vlan** { *vlan-id1* [**to** *vlan-id2*] } &<1-10>] **bridge-diameter**

Parameters

Parameter	Description	Value
vlan *vlan-id1* [**to** *vlan-id2*]	Configures the diameter of a spanning tree in VLANs. ● *vlan-id1* specifies the start VLAN ID. ● **to** *vlan-id2* specifies the end VLAN ID. *vlan-id2* must be greater than or equal to *vlan-id1*. *vlan-id2* and *vlan-id1* specify a VLAN range. ● If **to** *vlan-id2* is not specified, the diameter is configured only for the VLAN specified by *vlan-id1*. In the **stp bridge-diameter** command, you can specify a maximum of 10 VLAN ranges. **NOTE** VLANs can be specified only when VBST is running.	The value is an integer that ranges from 1 to 4094.
diameter	Specifies the diameter.	The value is an integer ranging from 2 to 7.

Views

System view or MSTP process view

NOTE

VBST does not support processes. When VBST is running, you cannot run the **stp bridge-diameter** command in the MSTP process view.

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On a network running a spanning tree protocol, the network diameter is the maximum number of devices between two switching devices. If the network diameter is improperly set, network converge may slow down, affecting users' normal communication.

The **stp bridge-diameter** command can be used to set a proper network diameter based on the network scale. This helps to accelerate network convergence.

The following time parameters are related to the network scale:

- Hello Time
- Forward Delay
- Max Age

Precautions

After the **stp bridge-diameter** command is used on a switching device, the switching device will automatically set proper values for Hello Time, Forward Delay, and Max Age based on the configured network diameter.

On an MSTP network, the network diameter configured using the **stp bridge-diameter** command is valid only for CISTs.

Example

# Set the network diameter to 5 when STP/RSTP/MSTP is running.

```
<HUAWEI> system-view
[HUAWEI] stp bridge-diameter 5
```

# Set the diameter to 5 for VLAN 10 when VBST is running.

```
<HUAWEI> system-view
[HUAWEI] stp vlan 10 bridge-diameter 5
```

5.12.32 stp compliance

Function

The **stp compliance** command configures the format for the MSTP packets that are received and sent on the switching device.

The **undo stp compliance** command restores the default format for the MSTP packets that are received and sent on the switching device.

By default, the MSTP packet format is **auto**.

Format

stp compliance { **auto** | **dot1s** | **legacy** }

undo stp compliance

Parameters

Parameter	Description	Value
auto	Indicates that the protocol format is self-adaptive.	-
dot1s	Indicates that the format is standard IEEE 802.1s.	-
legacy	Indicates the private packet format.	-

Views

Ethernet interface view, GE interface view, XGE interface view, MultiGE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, port group view, 25GE interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

MSTP protocol packets have two formats: dot1s (IEEE 802.1s standard packets) and legacy (proprietary protocol packets). The **stp compliance** command can be used on a device to set an MSTP packet format based on the format of the MSTP packet received from a remote device so that this device can better communicate with the remote device.

The auto mode is set to allow a port to automatically switch to the MSTP protocol packet format used by the remote end based on the MSTP protocol packet format received from the remote end. This enables the two interfaces to use the same MSTP protocol packet format.

Precautions

If you configure different packet formats on the same interface in the system view and the interface view, the latest configuration overrides the previous one.

If the **auto** parameter is set, the device preferentially sends IEEE·802.1s-compliant MSTP packets and can process IEEE·802.1s-compliant and vendor-specific MSTP packets. After an interface receives an MSTP packet from a non-Huawei device, the interface automatically switches to the packet format supported by the peer device based on the format of the received packet.

If the **dot1s** parameter is set, the device preferentially sends IEEE·802.1s-compliant MSTP packets and can process IEEE·802.1s-compliant and vendor-specific MSTP packets. After an interface receives an MSTP packet from a non-Huawei device, the interface automatically switches to the packet format supported by the peer device based on the format of the received packet.

If the **legacy** parameter is set, the device preferentially sends vendor-specific MSTP packets and can process IEEE·802.1s-compliant and vendor-specific MSTP packets. After an interface receives an MSTP packet from a non-Huawei device, the interface automatically switches to the packet format supported by the peer device based on the format of the received packet.

Example

# Set the format of the MSTP packets to the standard format of the interface.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] stp compliance dot1s
```

# Restore the self-adaptive format of the MSTP packets that are received and sent by the switching device.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo stp compliance
```

5.12.33 stp config-digest-snoop

Function

The **stp config-digest-snoop** command enables digest snooping.

The **undo stp config-digest-snoop** command disables digest snooping.

By default, the digest snooping is disabled.

Format

stp config-digest-snoop

undo stp config-digest-snoop

Parameters

None

Views

Ethernet interface view, GE interface view, XGE interface view, MultiGE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, port group view, 25GE interface view

Default Level

2: Configuration level

Usage Guidelines

On an MSTP network where Huawei and non-Huawei devices are interconnected, if the Huawei and non-Huawei devices have the same region name, revision level, and VLAN mapping table but have different BPDU keys, you can run this command to enable the Huawei and non-Huawei devices to exchange BPDUs.

Example

# Enable digest snooping on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] stp config-digest-snoop
```

5.12.34 stp converge

Function

The **stp converge** command sets the converging mode of a spanning tree protocol.

The **undo stp converge** command restores the default mode.

By default, the converging mode of the spanning tree protocol is **normal**.

Format

stp converge { **fast** | **normal** }

undo stp converge

Parameters

Parameter	Description	Value
fast	Indicates ARP entries that will be directly deleted.	-
normal	Indicates ARP entries that will age quickly.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On a Layer 2 network running a spanning tree protocol, if the topology of a spanning tree instance changes, the forwarding paths of VLANs that are mapped to this instance change. As a result, ARP entries related to these VLANs need to be updated. Based on methods for processing ARP entries, the converging modes of a spanning tree protocol are classified into fast and normal:

- In fast mode, entries that need to be updated in an ARP table are directly deleted.
- In normal mode, entries that need to be updated in an ARP table quickly age. A switching device sets the EXPIRE time of these ARP entries to 0 in order to age them. If the number of detection times for aging out ARP entries is

greater than 0, the switching device detects these ARP entries before deleting them.

The **stp converge** command can be used to set a converging mode based on the method for processing ARP entries.

Precautions

If the **stp converge fast** command is run on a switching device and the topology of a spanning tree instance changes, the switching device will directly delete the ARP entries that need to be updated in the ARP table.

If the **stp converge normal** command is run on a switching device and the topology of a spanning tree instance changes, the switching device will age the ARP entries that need to be updated in the ARP table.

Setting the converging mode of a spanning tree protocol to **normal** is recommended. If the fast mode is used, frequent ARP entry deletion will affect services and even may cause the CPU usage of the device to reach 100%. As a result, packet processing will time out, causing network flapping.

In either fast or normal mode, MAC address entries that need to be updated are deleted.

Example

# Set the converging mode of the spanning tree protocol on the Ethernet switch as normal.

```
<HUAWEI> system-view
[HUAWEI] stp converge normal
```

5.12.35 stp cost

Function

The **stp cost** command sets the path cost of a port in a spanning tree.

The **undo stp cost** command restores the default path cost.

By default, the path cost of a port in a spanning tree is the path cost corresponding to the port rate.

Format

STP/RSTP/MSTP: **stp** [**process** *process-id*] [**instance** *instance-id*] **cost** *cost*

VBST: **stp** [**vlan** { *vlan-id1* [**to** *vlan-id2*] } &<1-10>] **cost** *cost*

STP/RSTP/MSTP: **undo stp** [**process** *process-id*] [**instance** *instance-id*] **cost**

VBST: **undo stp** [**vlan** { *vlan-id1* [**to** *vlan-id2*] } &<1-10>] **cost**

Parameters

Parameter	Description	Value
process *process-id*	Indicates the ID of an MSTP process. If **process** *process-id* is not specified, the status and statistics of an MSTP process with the ID 0 will be displayed.	The value is a decimal integer ranging from 1 to 31.
instance *instance-id*	Specifies the number of a spanning tree instance. If **instance** *instance-id* is not specified, it indicates the path cost of an interface in CIST.	The value is an integer ranging from 0 to 4094. Value 0 refers to CIST. **NOTE** *instance-id* ranges from 0 to 4094. Each process supports a maximum of 65 instances.
cost	Specifies the path cost of an interface.	According to different calculation standards, the value ranges are as follows: ● Huawei legacy standard: 1 to 200,000 ● IEEE 802.1d-1998 standard: 1 to 65535 ● IEEE 802.1t standard: 1 to 200,000,000
vlan *vlan-id1* [**to** *vlan-id2*]	Specifies one or more VLANs in which the port path cost is set. ● *vlan-id1* specifies the start VLAN ID. ● **to** *vlan-id2* specifies the end VLAN ID. *vlan-id2* must be greater than or equal to *vlan-id1*. *vlan-id2* and *vlan-id1* specify a VLAN range. ● If **to** *vlan-id2* is not specified, the port path cost is configured only for the VLAN specified by *vlan-id1*. In the **stp cost** command, you can specify a maximum of 10 VLAN ranges. **NOTE** VLANs can be specified only when VBST is running.	The value is an integer that ranges from 1 to 4094.

Views

Ethernet interface view, GE interface view, XGE interface view, MultiGE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, port group view, 25GE interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The path cost of a port is an important basis for calculating a spanning tree. Path costs determine root port selection. In a spanning tree, the port with the lowest path cost to the root bridge is selected as a root port.

If different path costs are set for a port on an MSTP device in different spanning tree instances, traffic of different VLANs will be forwarded along different physical links and VLAN-based load balancing can be carried out.

Path costs depend on path cost calculation standards. After the path cost calculation standard is determined, set a relatively small path cost within a specified range for a port that has a high link rate. In the Huawei legacy standard, default path costs for ports with different link rates are different, as shown in the following table.

Table 5-92 Mappings between link rates and path costs (Huawei legacy standard)

Link Rate	Recommended Value Default, Value	Recommended Value Range	Value Range
10 Mbit/s	2000	200-20000	1-200,000
100 Mbit/s	200	20-2000	1-200,000
1 Gbit/s	20	2-200	1-200,000
10 Gbit/s	2	2-20	1-200,000
Over 10 Gbit/s	1	1-2	1-200,000

Prerequisites

A path cost calculation standard has been set using the **stp pathcost-standard** command.

Precautions

If the path cost of a port, the spanning tree where the port resides needs to be recalculated.

If the **stp pathcost-standard** command is used to change the path cost calculation standard, the path cost set using the **stp cost** command for a port will be restored to the default value.

Example

# Set the path cost of GE0/0/1 in spanning tree instance 2 to 200 when STP/RSTP/MSTP is running.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] stp instance 2 cost 200
```

# Set the path cost of GE0/0/1 in VLAN 10 to 300 when VBST is running.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] stp vlan 10 cost 300
```

5.12.36 stp edged-port

Function

The **stp edged-port enable** command sets the current port as an edge port.

The **stp edged-port disable** command sets the current port as a non-edge port.

The **undo stp edged-port** command restores the default attribute of an edge port.

By default, all the ports on the switching device are non-edge ports.

NOTE

After STP is enabled on a port, edge-port detecting is started automatically. If the port fails to receive BPDU packets within (2 x Hello Timer + 1) seconds, the port is set to an edge port. Otherwise, the port is set to a non-edge port. If the **stp edged-port enable** or **stp edged-port disable** command is executed in the interface view or the **stp edged-port default** command is configured in the system view, automatic detection of the edge port becomes invalid.

Format

stp edged-port { **enable** | **disable** }

undo stp edged-port

Parameters

Parameter	Description	Value
enable	Sets the current port as an edge port.	-
disable	Sets the current port as a non-edge port.	-

Views

Ethernet interface view, GE interface view, XGE interface view, MultiGE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, port group view, 25GE interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On a Layer 2 network running a spanning tree protocol, a port connected to terminals does not need to participate in spanning tree calculation. If the port participates in spanning tree calculation, the network convergence speed will be affected. In addition, status changes of the port may cause network flapping, interrupting user traffic. To address this problem, you can run the **stp edged-port enable** command to configure the port as an edge port. Then, the port will not participate in the spanning tree calculation. This speeds up network convergence and improves network stability.

Precautions

An edge port does not participate in spanning tree calculation. The edge port can transition from Disable to Forwarding state immediately without a delay. The switch automatically configures an edge port as a non-edge port once the edge port receives a configuration BPDU. Then the spanning tree is recalculated.

After the **stp edged-port default** command is run, a port that has been configured with the **undo stp edged-port** command will become an edge port. After the **stp edged-port disable** command is run, the port that has been configured with the **undo stp edged-port** command, however, will still serve as a non-edge port.

NOTE

The device supports automatic detection of the edge port. When the port connected to the terminal changes from Down to Up, the port enters the forwarding state after (2 x Hello Timer + 1) seconds. If automatic detection is not configured, the port enters the forwarding state after 30s.

A device configured with automatic edge port detection may fail to detect edge ports when the CPU usage is high. Therefore, you are advised to manually configure edge ports when the device's CPU usage is high.

Example

# Configure GE0/0/1 as an edge port.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] stp edged-port enable
```

5.12.37 stp edged-port default

Function

The **stp edged-port default** command configures the ports on a switching device as edge ports.

The **undo stp edged-port default** command restores the default setting.

By default, the ports on a switching device are non-edge ports.

NOTE

After STP is enabled on a port, edge-port detecting is started automatically. If the port fails to receive BPDU packets within (2 x Hello Timer + 1) seconds, the port is set to an edge port. Otherwise, the port is set to a non-edge port.

Format

stp edged-port default

undo stp edged-port default

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On a Layer 2 network running a spanning tree protocol, a port connected to terminals does not need to participate in spanning tree calculation. If the port participates in spanning tree calculation, the network convergence speed will be affected. In addition, status changes of the port may cause network flapping, interrupting user traffic. To address this problem, you can run the **stp edged-port enable** command to configure the port as an edge port. Then, the port will not participate in the spanning tree calculation. This speeds up network convergence and improves network stability.

NOTICE

After the **stp edged-port default** command is run on a device, all ports of the device will be become edge ports. During network topology calculation, running the **stp edged-port default** command may cause a loop. Exercise caution when using this command.

Precautions

If a port of a switching device receives a BPDU after being configured as an edge port, the switching device will automatically set the port as a non-edge port and recalculate the spanning tree.

To prevent attackers from forging BPDUs to change edge ports on a switching device to non-edge ports, you can run the **stp bpdu-protection** command in the system view to configure BPDU protection on the switching device. After BPDU protection is enabled on a switching device, the switching device shuts down the edge port if the edge port receives a BPDU. The attributes of the edge port are not changed.

After the **stp edged-port default** command is run, a port that has been configured with the **undo stp edged-port** command will become an edge port. After the **stp edged-port disable** command is run, the port that has been configured with the **undo stp edged-port** command, however, will still serve as a non-edge port.

Example

# Configure all ports on an edge device as edge ports.

```
<HUAWEI> system-view
[HUAWEI] stp edged-port default
```

5.12.38 stp enable

Function

The **stp enable** command enables STP/RSTP/MSTP/VBST on a switching device or an interface.

The **undo stp enable** command disables STP/RSTP/MSTP/VBST on a switching device or an interface.

The **stp disable** command disables STP/RSTP/MSTP/VBST on a switching device or an interface.

The **undo stp disable** command enables STP/RSTP/MSTP/VBST on a switching device or an interface.

By default, STP/RSTP/MSTP/VBST is enabled globally and on an interface.

Format

stp enable

undo stp enable

stp disable

undo stp disable

Parameters

None

Views

System view, MSTP process view, Ethernet interface view, GE interface view, XGE interface view, MultiGE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, port group view, 25GE interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On a complex Layer 2 network, to prevent loops or break loops, STP/RSTP/MSTP/VBST can be configured on switching devices.

Running the **stp enable** command enables STP/RSTP/MSTP/VBST. The devices running STP/RSTP/MSTP/VBST discover loops on the network by exchanging information with each other and trim the ring topology into a loop-free tree topology by blocking a certain interface. In this manner, replication and circular propagation of packets are prevented on the network. In addition, the processing performance of devices is prevented from deteriorating.

Enabling STP/RSTP/MSTP/VBST consumes system resources so that you can run the **stp disable** command to disable STP/RSTP/MSTP/VBST on devices or interfaces that do not participate in the spanning tree calculation.

NOTE

To prevent the CPU from being affected and faults such as network flapping from occurring, the following lists the recommended maximum number of STP-enabled ports in Up state for different models:

SS1720GW-E, S1720GWR-E, S5720-LI, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5720S-LI, S5735S-H, S5736-S, S6720S-S, S5720I-SI, S5735-S, S500, S5735S-S, and S5735-S-I: 128

S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S: 256

Pre-configuration Tasks

After STP/RSTP/MSTP is enabled on a ring network, STP/RSTP/MSTP immediately calculates spanning trees on the network. Configurations on a switching device, such as, the switching device priority and port priority, will affect spanning tree calculation. Any change of the configurations may cause network flapping. Therefore, to ensure rapid and stable spanning tree calculation, before enabling STP/RSTP/MSTP, perform basic configurations on the switching device and its interfaces. For example:

- Run the **stp mode** { **mstp** | **rstp** | **stp** } command to set the working mode of the switching device.
- Run the **stp** [**instance** *instance-id*] **priority** *priority* command to set the priority of the switching device in the spanning tree.
- Run the **stp** [**process** *process-id*] [**instance** *instance-id*] **port priority** *priority* command to set the priority of the interface in the spanning tree instance.

- Run the **stp** [**instance** *instance-id*] **root primary** command to set the switching device as the primary root bridge of the spanning tree.
- Run the **stp** [**instance** *instance-id*] **root secondary** command to set the switching device as the secondary root bridge of the spanning tree.
- Run the **stp** [**process** *process-id*] [**instance** *instance-id*] **cost** *cost* command to set the path cost of the interface in the spanning tree instance.
- If the spanning tree protocol is MSTP, run the **region-name** *name*, **instance** *instance-id* **vlan** { *vlan-id* [**to** *vlan-id*] } &<1-10>, **vlan-mapping modulo**, and **revision-level** *level* commands to configure the MST region.

When VBST is enabled on a ring network, VBST immediately starts spanning tree calculation. Parameters such as the switch priority and port priority affect spanning tree calculation, and change of these parameters may cause network flapping. To ensure fast and stable spanning tree calculation, perform basic configurations on the switch and ports before enabling VBST.

- Run the **stp mode vbst** command to set the working mode of the switch.
- Run the **stp vlan** { *vlan-id1* [**to** *vlan-id2*] } &<1-10> **priority** *priority* command to set the priority of the switch in the spanning tree.
- Run the **stp vlan** { *vlan-id1* [**to** *vlan-id2*] } &<1-10> **port priority** *priority* command to set the priority of the port in the spanning tree instance.
- Run the **stp vlan** { *vlan-id1* [**to** *vlan-id2*] } &<1-10> **root primary** command to set the switch as the root bridge of the spanning tree instance.
- Run the **stp vlan** { *vlan-id1* [**to** *vlan-id2*] } &<1-10> **root secondary** command to set the switch as the secondary root bridge of the spanning tree.
- Run the **stp vlan** { *vlan-id1* [**to** *vlan-id2*] } &<1-10> **cost** *cost* command to set the path cost of the port in the spanning tree instance.
- Run the **instance** *instance-id* **vlan** *vlan-id* command to configure 1:1 mapping between MSTIs and VLANs.

Other configurations are needed based on real-world situations.

Precautions

- If STP/RSTP/MSTP/VBST is enabled on an interface, the interface participates in the spanning tree calculation and determines whether it is in the forwarding state according to the calculation result.
- If STP/RSTP/MSTP/VBST is disabled on an interface, the interface does not participate in the spanning tree calculation and it is always in the forwarding state.
- STP/RSTP/MSTP/VBST must be enabled on all interfaces that participate in the spanning tree calculation. Otherwise, a loop may occur.
- Spanning tree calculation may result in network flapping. Before network convergence, packets cannot be correctly forwarded. In this case, if the DHCP server is configured on a VLANIF interface, DHCP clients obtain IP addresses slowly. To solve the problem, disable STP or configure the device interface connected to a terminal as the edge interface.
- If the **undo stp enable** or **stp disable** command is run in the system view, the global STP function is disabled, which may cause a loop.
- If the **undo stp enable** or **stp disable** command is run in the MSTP process view, the STP function in the MSTP process is disabled, which may cause a loop in the MSTP process.

Follow-up Procedure

After STP is enabled globally and on an interface, run the **stp vlan enable** command to enable STP in a VLAN so that VBST can take effect.

Example

# Enable STP/RSTP/MSTP/VBST on a switching device.

```
<HUAWEI> system-view
[HUAWEI] stp enable
```

# Disable STP/RSTP/MSTP/VBST on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] stp disable
```

5.12.39 stp link-share-protection

Function

The **stp link-share-protection** command enables the shared-link protection for an MSTP process.

The **undo stp link-share-protection** command disables the shared-link protection of an MSTP process.

By default, the shared-link protection of an MSTP process is disabled.

Format

stp link-share-protection

undo stp link-share-protection

Parameters

None

Views

MSTP process view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In networking with a switching device dual-homed to an upper-layer network, if a public link becomes faulty, rings that the public link accesses may unblock their blocked ports. As a result, a permanent network loop is generated.

The **stp link-share-protection** command can be used to enable shared-link protection in a specified process in order to prevent this problem. Then, when a public link becomes faulty, the working mode of each device on the public link will be forcibly switched to RSTP. After shared-link protection and root protection are deployed, a port will still be in blocked state even after receiving packets of a higher priority from a downstream device. This prevents network loops.

Precautions

Shared-link protection is valid only in processes. Before running the **stp link-share-protection** command, check that relevant ports have been correctly bound to the corresponding process using the **stp binding process** command.

Example

# Enable the shared-link protection for MSTP process 1.

```
<HUAWEI> system-view
[HUAWEI] stp process 1
[HUAWEI-mst-process-1] stp link-share-protection
```

5.12.40 stp loop-protection

Function

The **stp loop-protection** command enables loop protection on the current port.

The **undo stp loop-protection** command disables loop protection on the current port.

By default, loop protection on ports is disabled.

Format

stp loop-protection

undo stp loop-protection

Parameters

None.

Views

Ethernet interface view, GE interface view, XGE interface view, MultiGE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, port group view, 25GE interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On a network running a spanning tree protocol, a switching device maintains the status of the root port and blocked port by continually receiving BPDUs from the upstream switching device. If ports cannot receive BPDUs from the upstream switching device due to link congestion or unidirectional link failures, the switching device will re-select a root port. Then, the previous root port becomes a designated port and the previous blocked port enters the Forwarding state. As a result, loops may occur on the network.

To prevent the preceding problems, deploy loop protection. If the root port or alternate port does not receive BPDUs from the upstream device for a long time, the switch enabled with loop protection sends a notification to the NMS. If the root port is used, the root port enters the Discarding state and becomes the designated port. If the alternate port is used, the alternate port keeps blocked and becomes the designated port. In this case, loops will not occur. After the link is not congested or unidirectional link failures are rectified, the port receives BPDUs for negotiation and restores its original role and status.

NOTE

- An alternate port is the backup of the root port. When the root port can normally send and receive BPDUs, the alternate port is in the blocked state.
- Between two interconnected switching devices in a spanning tree, the switching device nearer to the root bridge is the upstream device of the other devices.

Precautions

Loop protection and root protection cannot be configured on the same interface simultaneously.

If loop protection needs to be configured on an interface in a process with a non-zero ID, the **stp binding process** command must have been run to bind this interface to the process.

Example

# Enable loop protection on the GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] stp loop-protection
```

5.12.41 stp max-hops

Function

The **stp max-hops** command sets the maximum hops of a spanning tree in an MST region.

The **undo stp max-hops** command restores the default value of the maximum hops of a spanning tree.

By default, the maximum hops in an MST region is 20.

Format

stp max-hops *hop*

undo stp max-hops

Parameters

Parameter	Description	Value
hop	Specifies the maximum hops.	The value ranges from 1 to 40.

Views

System view or MSTP process view

NOTE

VBST does not support processes. When VBST is running, you cannot run the **stp max-hops** command in the MSTP process view.

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Switching devices on a Layer 2 network running MSTP communicate with each other by exchanging MST BPDUs. An MST BPDU has a field that indicates the number of remaining hops.

- The number of remaining hops in a BPDU sent by the root switching device equals the maximum number of hops.
- The number of remaining hops in a BPDU sent by a non-root switching device equals the maximum number of hops minus the number of hops from the non-root switching device to the root switching device.
- If a switching device receives a BPDU in which the number of remaining hops is 0, the switching device will discard the BPDU.

Therefore, the maximum number of hops of a spanning tree in an MST region determines the network scale. The **stp max-hops** command can be used to set the maximum number of hops in an MST domain so that the network scale of a spanning tree can be controlled.

Precautions

In an MST region, the maximum number of hops set on the root switching device in a CIST or an MSTI is the maximum number of hops in the CIST or MSTI.

Example

# Set the maximum hops in the MST region to 35.

```
<HUAWEI> system-view
[HUAWEI] stp max-hops 35
```

5.12.42 stp mcheck

Function

The **stp mcheck** command configures a port to switch from the STP mode back to the RSTP/MSTP/VBST mode.

By default, a port transitions from the STP mode to the RSTP/MSTP/VBST mode by receiving BPDUs. A port that does not receive BPDUs cannot transition from the STP mode to the RSTP/MSTP/VBST mode.

Format

stp mcheck

Parameters

None

Views

System view, MSTP process view, Ethernet interface view, Eth-Trunk interface view, GE interface view, XGE interface view, MultiGE interface view, 40GE interface view, 100GE interface view, port group view, 25GE interface view

NOTE

VBST does not support processes. When VBST is running, you cannot run the **stp mcheck** command in the MSTP process view.

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If a port of an RSTP/MSTP/VBST switching device is directly connected to an STP switching device, the port automatically switches to the STP mode and then sends BPDUs. This ensures that the two switching devices properly communicate with each other. If the STP switching device is powered off or removed, the port on the RSTP/MSTP/VBST switching device cannot switch back to the RSTP/MSTP/VBST mode. As a result, the RSTP/MSTP/VBST device cannot communicate with other RSTP/MSTP/VBST switching devices.

The **stp mcheck** command can be used to address this problem. After this command is run on a port, the port will switch from the STP mode back to the RSTP/MSTP/VBST mode.

When a VBST-enabled switch connects to an MSTP-enabled switch, the connected port of the MSTP-enabled switch automatically switches to the RSTP mode through negotiation. When the VBST-enabled switch switches to the MSTP mode, the connected ports of the two switches may still work in RSTP mode due to the time sequence problem. You can perform the following operations to manually switch the ports to the MSTP mode.

Prerequisites

If a port in a process with a non-zero ID needs to be configured to switch from the STP mode back to the RSTP/MSTP mode, the port must have been bound to the corresponding process using the **stp binding process** *process-id* command.

Precautions

This command does not take effect on a port in Down state.

Running the **stp mcheck** command in the system view configures all ports on the device to switch back to the RSTP/MSTP/VBST mode.

Running the **stp mcheck** command in the MSTP process view configures all ports bound to the current MSTP process to switch back to the RSTP/MSTP mode.

Running the **stp mcheck** command in the interface view configures only the current port to switch back to the RSTP/MSTP/VBST mode.

Example

# Perform MCheck on GE0/0/1 and switch it to the MSTP mode.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] stp mcheck
```

5.12.43 stp mode (MSTP process view)

Function

The **stp mode** command sets the operation mode of spanning tree protocol for the current MSTP process.

The **undo stp mode** command restores the default operation mode of the current MSTP process.

By default, the operation mode of spanning tree protocol for the current MSTP process is MSTP.

Format

stp mode { **mstp** | **rstp** | **stp** }

undo stp mode

Parameters

Parameter	Description	Value
mstp	Indicates the MSTP operation mode for the ports bound to the current MSTP process.	-
rstp	Indicates the RSTP operation mode for the ports bound to the current MSTP process.	-

Parameter	Description	Value
stp	Indicates the STP operation mode for the ports bound to the current MSTP process.	-

Views

MSTP process view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After an MSTP process is created on an MSTP network, all ports bound to the MSTP process operate in MSTP mode by default. These ports may be connected to STP/RSTP devices. As a result, spanning trees cannot be properly calculated, because devices running different spanning tree protocols cannot exchange packets.

To address this problem, the **stp mode** command can be set an operation mode for a switching device. The operation mode can be MSTP, RSTP, or STP.

By default, if a port on a switching device is bound to a process and is connected to an STP switching device, the switching device automatically sets the operation mode of this port to STP and the operation mode of the other ports to MSTP.

Precautions

- After the **stp mode mstp** command is run in an MSTP process, all ports that are running MSTP and are bound to the MSTP process, excluding the ports directly connected to STP switching devices, operate in MSTP mode and can send MST BPDUs. The ports directly connected to STP switching devices operate in STP mode.
- After the **stp mode rstp** command is run in an MSTP process, all ports that are running MSTP and are bound to the MSTP process, excluding the ports directly connected to STP switching devices, operate in RSTP mode and can send RST BPDUs. The ports directly connected to STP switching devices operate in STP mode.
- After the **stp mode stp** command is run in an MSTP process, all ports bound to the MSTP process operate in STP mode and send configured BPDUs.

A port operating in MSTP mode can communicate with a port operating in RSTP mode.

Running the **stp mode rstp** command on a device that supports MSTP is not recommended. The function of the **stp mode rstp** command can be implemented by the **stp mode mstp** command by default.

Example

# Set the operation mode of MSTP process 1 to the STP mode.

```
<HUAWEI> system-view
[HUAWEI] stp process 1
[HUAWEI-mst-process-1] stp mode stp
```

5.12.44 stp mode (system view)

Function

The **stp mode** command sets the operation mode of the spanning tree protocol on a switching device.

The **undo stp mode** command restores the default operation mode of the spanning tree protocol.

By default, the switching device operates in MSTP mode.

Format

stp mode { **mstp** | **rstp** | **stp** | **vbst** }

undo stp mode

Parameters

Parameter	Description	Value
mstp	Indicates the MSTP mode.	-
rstp	Indicates the RSTP mode.	-
stp	Indicates the STP mode.	-
vbst	Indicates the VBST mode.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On the network running a spanning tree protocol, switches running different spanning tree protocols cannot communicate with each other. As a result, spanning trees cannot be properly calculated. A switch has four operation modes: VBST, MSTP, RSTP, and STP.

The **stp mode** command can be used to set a proper operation mode for a spanning tree protocol on a switching device and enables the switching device to identify BPDUs sent by a switching device that runs a different spanning tree protocol during communication.

By default, all ports on a switching device operate in MSTP mode. When a switching device finds that it is directly connected to an STP switching device, it automatically switches the operation mode and the port directly connected to the STP switching device to STP.

Configuration Impact

- After the **stp mode vbst** command is run on a switch, all ports running VBST on the switch, excluding the ports directly connected to STP switches, operate in VBST mode and can send VBST BPDUs. The ports directly connected to STP switches operate in STP mode.
- After the **stp mode mstp** command is run on a switching device, all ports running MSTP on the switching device, excluding the ports directly connected to STP switching devices, operate in MSTP mode and can send MSTP BPDUs. The ports directly connected to STP switching devices operate in STP mode.
- After the **stp mode rstp** command is run on a switching device, all ports running RSTP on the switching device, excluding the ports directly connected to STP switching devices, operate in RSTP mode and can send RSTP BPDUs. The ports directly connected to STP switching devices operate in STP mode.
- After the **stp mode stp** command is run on a switching device, all ports of the switching device operate in STP mode and send configured BPDUs.

Precautions

- A port operating in MSTP mode can communicate with a port operating in RSTP mode.
- VBST BPDUs and RST BPDUs can be used at the same time.
- The **stp mode rstp** command can be used to enable a switch that does not support MSTP to communicate with an STP switch.
- In VBST mode, the MAC address 0100-0CCC-CCCD is displayed in the **display bpdu mac-address** command output. In STP/RSTP/MSTP mode, the MAC address 0100-0CCC-CCCD is not displayed unless the **bpdu mac-address** command specifies the MAC address as 0100-0CCC-CCCD.
- An Eth-Trunk on the S6735-S, S6720-EI, and S6720S-EI can meet at most three of the following conditions simultaneously:
  - The Eth-Trunk is a Layer 2 interface, or the working mode of the Eth-Trunk is changed from Layer 3 to Layer 2 using the **portswitch** or **portswitch batch** command.
  - The Eth-Trunk is configured as a Layer 2 remote observing port using the **observe-port** command.
  - The operating mode of the spanning tree protocol is set to VBST on the switch using the **stp mode** command.
  - VBST is enabled on the Eth-Trunk using the **stp enable** command.

Example

# Set the operation mode of the switching device to the STP mode.

```
<HUAWEI> system-view
```

```
[HUAWEI] stp mode stp
```

5.12.45 stp no-agreement-check

Function

The **stp no-agreement-check** command configures the common fast transition mechanism on an interface.

The **undo stp no-agreement-check** command restores the default fast transition mechanism on an interface.

STP does not support fast transition. By default, for RSTP, MSTP, and VBST, fast transition in enhanced mode is used on a port.

Format

stp no-agreement-check

undo stp no-agreement-check

Parameters

None

Views

Ethernet interface view, GE interface view, XGE interface view, MultiGE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, port group view, 25GE interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If Huawei and non-Huawei data communication devices are deployed on a network running a spanning tree protocol, the Huawei devices and non-Huawei devices may fail to communicate with each other, because they have different Proposal/Agreement mechanisms. To address this problem, the **stp no-agreement-check** command can be used to set a common fast transition mechanism or an enhanced transition mechanism on a port.

- Running the **stp no-agreement-check** command configures a common fast transition mechanism on a port.
- Running the **undo stp no-agreement-check** command configures an enhanced fast transition mechanism on a port.

Precautions

The fast transition mechanism is also called the Proposal/Agreement mechanism. The device currently supports the following modes:

- Enhanced mode: The current interface counts a root port when it computes the synchronization flag bit.
  1. An upstream device sends a Proposal message to a downstream device requesting fast transition. After receiving the message, the downstream device sets the port connected to the upstream device as the root port and blocks all non-edge ports.
  2. The upstream device then sends an Agreement message to the downstream device. After the downstream device receives the message, the root port transitions to the Forwarding state.
  3. The downstream device then responds with an Agreement message. After receiving the message, the upstream device sets the port connected to the downstream device as the designated port, and then the status of the designated port changes to Forwarding.
- Common mode: The current interface ignores the root port when it computes the synchronization flag bit.
  1. An upstream device sends a Proposal message to a downstream device requesting fast transition. After receiving the message, the downstream device sets the port connected to the upstream device as the root port and blocks all non-edge ports. Then, the status of the root port changes to Forwarding.
  2. The downstream device then responds with an Agreement message. After receiving the message, the upstream device sets the port connected to the downstream device as the designated port, and then the status of the designated port changes to Forwarding.

NOTE

Between two interconnected switching devices in a spanning tree, the switching device nearer to the root bridge is the upstream device of the other devices.

Example

# Configure the common fast transition mechanism for the GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] stp no-agreement-check
```

5.12.46 stp pathcost-standard

Function

The **stp pathcost-standard** command sets the standard used to calculate the path cost.

The **undo stp pathcost-standard** command restores the default standard used to calculate the path cost.

By default, the IEEE 802.1t is used to calculate the path cost.

Format

stp pathcost-standard { **dot1d-1998** | **dot1t** | **legacy** }

undo stp pathcost-standard

Parameters

Parameter	Description	Value
dot1d-1998	Indicates IEEE 802.1D standard that is used to calculate the path cost.	-
dot1t	Indicates IEEE 802.1t standard that is used to calculate the path cost.	-
legacy	Indicates Huawei legacy standard that is used to calculate the path cost.	-

Views

System view or MSTP process view

NOTE

VBST does not support processes. When VBST is running, you cannot run the **stp pathcost-standard** command in the MSTP process view.

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A path cost is a port parameter, and is used by a spanning tree protocol to select a link. By calculating path costs, a spanning tree protocol selects stable links, blocks redundant paths, and trims a network into a loop-free network. The path cost range is determined by the path cost calculation standard.

Table 5-93 lists path costs defined by the IEEE 802.1D-1998 standard, IEEE 802.1t standard, and Huawei legacy standard. Different vendors use different standards.

Table 5-93 Path cost list

Interface Rate	Interface Mode	Recommended STP Path Cost		
		IEEE 802.1D-1998 Standard	IEEE 802.1t Standard	Huawei Legacy Standard
0	-	65535	200,000,000	200,000
10 Mbit/s	Half-Duplex	100	2,000,000	2000
	Full-Duplex	99	1,999,999	1999

Interface Rate	Interface Mode	Recommended STP Path Cost		
		IEEE 802.1D-1998 Standard	IEEE 802.1t Standard	Huawei Legacy Standard
	Aggregated Link 2 Ports	95	1,000,000	1800
	Aggregated Link 3 Ports	95	666,666	1600
	Aggregated Link 4 Ports	95	500,000	1400
100 Mbit/s	Half-Duplex	19	200,000	200
	Full-Duplex	18	199,999	199
	Aggregated Link 2 Ports	15	100,000	180
	Aggregated Link 3 Ports	15	66,666	160
	Aggregated Link 4 Ports	15	50,000	140
1000 Mbit/s	Full-Duplex	4	20,000	20
	Aggregated Link 2 Ports	3	10,000	18
	Aggregated Link 3 Ports	3	6666	16
	Aggregated Link 4 Ports	3	5000	14
2500 Mbit/s	Full-Duplex	3	8000	17
	Aggregated Link 2 Ports	3	4000	12
	Aggregated Link 3 Ports	3	2666	7
	Aggregated Link 4 Ports	2	2000	2
10 Gbit/s	Full-Duplex	2	2000	2
	Aggregated Link 2 Ports	1	1000	1
	Aggregated Link 3 Ports	1	666	1

Interface Rate	Interface Mode	Recommended STP Path Cost		
		IEEE 802.1D-1998 Standard	IEEE 802.1t Standard	Huawei Legacy Standard
	Aggregated Link 4 Ports	1	500	1
40 Gbit/s	Full-Duplex	1	500	1
	Aggregated Link 2 Ports	1	250	1
	Aggregated Link 3 Ports	1	166	1
	Aggregated Link 4 Ports	1	125	1

Precautions

If the path cost calculation standard is changed on a port, the path cost of the port is restored to the default value. The **stp cost** command can be used to set a path cost for a port.

Usually, all switching devices on the same network use the same path cost calculation standard.

Example

# Use the IEEE 802.1d-1998 to calculate the path cost.

```
<HUAWEI> system-view
[HUAWEI] stp pathcost-standard dot1d-1998
```

5.12.47 stp point-to-point

Function

The **stp point-to-point** command sets the link type of a port.

The **undo stp point-to-point** command restores the default link type.

By default, the link type of the ports on the switching device is **auto**. That is, the spanning tree protocol detects whether a port is connected to a P2P link.

Format

stp point-to-point { **auto** | **force-false** | **force-true** }

undo stp point-to-point

Parameters

Parameter	Description	Value
force-true	Indicates the link type is P2P.	-
force-false	Indicates the link type is non-P2P.	-
auto	Indicates that the spanning tree protocol detects automatically whether the port is connected to a P2P link.	-

Views

Ethernet interface view, GE interface view, XGE interface view, MultiGE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, port group view, 25GE interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On a Layer 2 network running a spanning tree protocol, if a port of a switching device is connected to a non-P2P link, the port cannot perform fast status transition.

If a port works in full-duplex mode, the port is connected to a P2P link, and **force-true** can be set in the **stp point-to-point** command.

If a port works in half-duplex mode, the **stp point-to-point force-true** command can be used to forcibly set the type of the link to which the port is connected to P2P, implementing rapid network convergence.

Precautions

The **stp point-to-point** command configuration on a port takes effect in all spanning tree instances where the port resides.

Example

# Set the link type of GE0/0/1 as P2P.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] stp point-to-point force-true
```

5.12.48 stp port priority

Function

The **stp port priority** command sets the priority of a port in a spanning tree.

The **undo stp port priority** command restores the default priority.

By default, the priority of a port in a spanning tree is 128.

Format

STP/RSTP/MSTP: **stp** [**process** *process-id*] [**instance** *instance-id*] **port priority** *priority*

VBST: **stp** [**vlan** { *vlan-id1* [**to** *vlan-id2*] } &<1-10>] **port priority** *priority*

STP/RSTP/MSTP: **undo stp** [**process** *process-id*] [**instance** *instance-id*] **port priority**

VBST: **undo stp** [**vlan** { *vlan-id1* [**to** *vlan-id2*] } &<1-10>] **port priority**

Parameters

Parameter	Description	Value
process *process-id*	Indicates the ID of an MSTP process. If **process** *process-id* is not specified, the status and statistics of an MSTP process with the ID 0 will be displayed.	The value is an integer ranging from 1 to 31.
instance *instance-id*	Specifies the spanning tree instance. If this parameter is not specified, the statistics about the topology changes of a CIST are displayed.	The value is an integer ranging from 0 to 4094. Value 0 refers to CIST. *instance-id* ranges from 0 to 4094. Each process supports a maximum of 65 instances.
priority	Specifies the priority of a port.	The priority ranks from 0 to 240 in descending order. The value is an integer multiple of 16, such as, 0, 16, and 32.
vlan *vlan-id1* [**to** *vlan-id2*]	Specifies one or more VLANs in which the port priority is configured. ● *vlan-id1* specifies the start VLAN ID. ● **to** *vlan-id2* specifies the end VLAN ID. *vlan-id2* must be greater than or equal to *vlan-id1*. *vlan-id2* and *vlan-id1* specify a VLAN range. ● If **to** *vlan-id2* is not specified, the port priority is configured only for the VLAN specified by *vlan-id1*. In the **stp priority** command, you can specify a maximum of 10 VLAN ranges. **NOTE** VLANs can be specified only when VBST is running.	The value is an integer that ranges from 1 to 4094.

Views

Ethernet interface view, GE interface view, XGE interface view, MultiGE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, port group view, 25GE interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When ports participate in spanning tree calculation, the PIDs of these ports on switching devices may affect the designated port election result. During spanning tree calculation, the port with the smallest PID is elected as the designated port.

NOTE

A PID is the ID of a port, and consists of a 4-bit priority and a 12-bit port number.

The **stp port priority** command can be used to change the priority of a port. This affects the PID of the port and determines whether the port can be elected as the designated port.

Precautions

When the priority of a port changes, a spanning tree protocol recalculates the role of the port and performs status transition for the port.

The priority of a port determines the role of the port in a specified spanning tree instance and process. You can set different priorities for a port in different spanning tree instances or processes so that user traffic can be forwarded along different links and traffic load balancing can be implemented.

Enabling MSTP on a ring network immediately triggers spanning tree calculation. If basic configurations are not performed on switches and interfaces before MSTP is enabled, network flapping may occur upon changes to parameters such as device priority and interface priority.

Example

# Set the priority of GE0/0/1 to 16 in the spanning tree instance 2 when MSTP is running.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] stp instance 2 port priority 16
```

# Set the priority of GE 0/0/1 in VLAN 10 to 32 when VBST is running.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] stp vlan 10 port priority 32
```

5.12.49 stp priority

Function

The **stp priority** command sets the priority of the switching device in a spanning tree.

The **undo stp priority** command restores the default priority.

By default, the priority of the switching device in a spanning tree is 32768.

Format

STP/RSTP/MSTP: **stp** [**instance** *instance-id*] **priority** *priority*

STP/RSTP/MSTP: **undo stp** [**instance** *instance-id*] **priority**

VBST: **stp** [**vlan** { *vlan-id1* [**to** *vlan-id2*] } &<1-10>] **priority** *priority*

VBST: **undo stp** [**vlan** { *vlan-id1* [**to** *vlan-id2*] } &<1-10>] **priority**

Parameters

Parameter	Description	Value
instance *instance-id*	Specifies the ID of a spanning tree instance. If the parameter **instance** *instance-id* is not specified, the configuration takes effect on a CIST instance.	The value is an integer ranging from 0 to 4094. Value 0 refers to CIST. *instance-id* ranges from 0 to 4094. Each process supports a maximum of 65 instances.
priority	Specifies the priority of the switching device in a spanning tree. The smaller the value is, the higher the switch priority is.	The priority ranks from 0 to 61440. The value is an integer multiple of 4096, such as 0, 4096 and 8192. The default is 32768.

Parameter	Description	Value
vlan *vlan-id1* [**to** *vlan-id2*]	Specifies one or more VLANs in which the switch priority is configured. ● *vlan-id1* specifies the start VLAN ID. ● **to** *vlan-id2* specifies the end VLAN ID. *vlan-id2* must be greater than or equal to *vlan-id1*. *vlan-id2* and *vlan-id1* specify a VLAN range. ● If **to** *vlan-id2* is not specified, the switch priority is configured only for the VLAN specified by *vlan-id1*. In the **stp priority** command, you can specify a maximum of 10 VLAN ranges. **NOTE** VLANs can be specified only when VBST is running.	The value is an integer that ranges from 1 to 4094.

Views

System view or MSTP process view

NOTE

VBST does not support processes. When VBST is running, you cannot run the **stp priority** command in the MSTP process view.

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Priorities of switching devices are an important factor to calculate a spanning tree and determine the selection of the root bridge.

On an STP/RSTP/MSTP/VBST network, each spanning tree has only one root bridge, which is responsible for sending BPDUs. Owning to the importance of the root bridge, the switching device with high performance and network hierarchy is generally chosen as the root bridge. The priority of such a switching device, however, may not be that high. Therefore, setting a high priority for the switching device is necessary so that the device can function as a root bridge.

Other devices with low performance and network hierarchy are not fit to be a root bridge. Therefore, set low priorities for these devices.

On an MSTP network, each switching device can be set with a distinct priority in each spanning tree instance. On a VBST network, each switch can be set with a priority for the spanning tree in each VLAN.

Precautions

The smaller the priority value of a switching device is, the higher the possibility that the switching device is selected as the root bridge.

If a switching device has been configured as the primary or secondary root bridge, before changing the priority of the switching device, run the **undo stp** [**instance** *instance-id*] **root** command to disable the root bridge or secondary root bridge function.

If the **stp root primary** command is run to set a switching device as the primary root bridge, the priority value of the switching device is 0.

If the **stp root secondary** command is run to set a switching device as the secondary root bridge, the priority value of the switching device is 4096.

Enabling MSTP on a ring network immediately triggers spanning tree calculation. If basic configurations are not performed on switches and interfaces before MSTP is enabled, network flapping may occur upon changes to parameters such as device priority and interface priority.

Example

# Set the priority of the switching device in spanning tree instance 1 to 4096 when MSTP is running.

```
<HUAWEI> system-view
[HUAWEI] stp instance 1 priority 4096
```

# Set the priority of the switch in VLAN 10 to 4096 when VBST is running.

```
<HUAWEI> system-view
[HUAWEI] stp vlan 10 priority 4096
```

5.12.50 stp process

Function

The **stp process** command has the following functions:

- Create an MSTP process with a specified ID and enter the MSTP process view if the specified MSTP process does not exist.
- Display the MSTP process view if the specified MSTP process exists.

The **undo stp process** command deletes a specified MSTP process.

By default, all MSTP configurations on a device belong to MSTP process 0.

Format

stp process *process-id*

undo stp process *process-id*

Parameters

Parameter	Description	Value
process-id	Indicates the ID of an MSTP process.	The value is an integer ranging from 1 to 31.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On a Layer 2 network where MSTP is run, if devices belong to multiple access rings that are isolated from each other and these access rings do not need intercommunication, MSTP cannot be used to calculate one spanning tree for all these access rings. Instead, MSTP must be enabled on each access ring to calculate the spanning trees independently.

Each switching device on these access rings can be configured with multiple MSTP processes. After ports of each switching device are bound to different MSTP processes, they participate in the MSTP calculations of different MSTP processes. MSTP calculations in different MSTP processes are independent of each other.

Follow-up Procedure

After an MSTP process is created, run the **stp binding process** command to bind relevant interfaces to the MSTP process.

Precautions

After a switching device that runs MSTP starts correctly, MSTP process 0 exists by default. MSTP configurations in the system view and interface view both belong to this process.

VBST does not support processes. Therefore, this command does not take effect when the spanning tree protocol is VBST. If this command has been run in MSTP mode, switching the MSTP mode to VBST mode fails, and the system displays a message indicating switching failure.

Example

# Create MSTP process 1.

```
<HUAWEI> system-view
[HUAWEI] stp process 1
```

5.12.51 stp pvid-consistency protection mode

Function

The **stp pvid-consistency protection mode** command configures a protection mode for PVID inconsistency between directly connected ports in VLAN-based Spanning Tree (VBST).

The **undo stp pvid-consistency protection mode** command deletes the protection mode for PVID inconsistency between directly connected ports in VBST.

By default, no protection mode is configured for PVID inconsistency between directly connected ports. That is, the switch only prints log information when the PVIDs of directly connected ports are different.

Format

stp pvid-consistency protection mode block

undo stp pvid-consistency protection mode

Parameters

Parameter	Description	Value
block	Specifies the block mode.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

VBST checks whether PVIDs of two directly connected ports are the same. If they are different, the processing method varies as follows:

- If the protection mode is **block**, VBST will block the PVIDs.
- If no protection mode is configured, VBST will print log information but not block the PVIDs.

Precautions

When the PVID of the interface is inconsistent and the PVID needs to be blocked, the **stp pvid-consistency protection mode** command must be configured on the two directly connected ports and their link types must be both trunk.

Example

# Set the protection mode for PVID inconsistency between directly connected ports to **block**.

```
<HUAWEI> system-view
[HUAWEI] stp pvid-consistency protection mode block
```

5.12.52 stp region-configuration

Function

The **stp region-configuration** command displays the MST region view.

The **undo stp region-configuration** command restores the default configuration of the MST region.

The default parameters of the MST regions are as follows:

- MST region name: MAC address of the switching device.
- MSTP revision level 0.
- VLAN mapping table: all VLANs are mapped to CIST.

Format

stp region-configuration

undo stp region-configuration

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

MSTP divides a switching network into multiple regions, each of which has multiple spanning trees and these spanning trees are independent of each other. Each spanning tree is called a multiple spanning tree instance (MSTI) and each region is called a multiple spanning tree (MST) region.

Two switching devices belong to the same MST region if they have the following parameters the same:

- MST region name
- Mappings between VLANs and MSTIs

- Revision level of the MST region

If the preceding parameters need to be set for the current switching device or the current process, run the **stp region-configuration** command to enter the MST region view first.

Follow-up Procedure

After the **stp region-configuration** command is run to enter the MST region view, run the following commands:

- Run the **region-name** command to set the MST region name.
- Run the **instance** or the **vlan-mapping modulo** command to set the mappings between VLANs and MSTIs.
- Run the **revision-level** name command to set the revision level of the MST region.

After entering the MST region view and setting the preceding parameters, run the **active region-configuration** command to activate the configurations of the MST region.

Precautions

Modifying the configuration in the MST region view will cause STP recalculation.

Example

# Enter the MST region view.

```
<HUAWEI> system-view
[HUAWEI] stp region-configuration
[HUAWEI-mst-region]
```

5.12.53 stp revertive slow

Function

The **stp revertive slow** command enables the delay in revertive switching during VBST calculation on a port.

The **undo stp revertive slow** command disables the delay in revertive switching during VBST calculation on a port.

By default, the delay in revertive switching disabled during VBST calculation on a port.

Format

stp revertive slow

undo stp revertive slow

Parameters

None

Views

Ethernet interface view, GE interface view, XGE interface view, MultiGE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, port group view, 25GE interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When a VBST-enabled switch interworks with a PVST-enabled third-party device that does not support P/A negotiation, negotiation is asynchronous. As a result, the network convergence time is long. If the remote device is the root bridge and the VBST-enabled switch provides the alternate port in addition to the interconnected port, you can enable the delay in revertive switching on the interconnected interface. The delay is calculated as follows: 2 * Forward Delay + 8s After the delay function is enabled, the remote interface first completes spanning tree calculation when the port status changes. Then the local interface performs spanning tree status switching. During status switching, services are not interrupted.

Precautions

After the delay in revertive switching is enabled on a port, this function takes effect for all VLANs that the interface join. If there is no alternate port in the VLAN where the interconnected port belongs, the port needs to wait for the delay for recovery. Exercise caution when you run this command in this situation.

Example

```
<HUAWEI> system-view
[HUAWEI] stp mode vbst
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] stp revertive slow
```

5.12.54 stp root

Function

The **stp root** command configures the switch as a root bridge or secondary root bridge of a spanning tree.

The **undo stp root** command cancels the configuration.

By default, the switch does not function as the root bridge or secondary root bridge of a spanning tree.

Format

STP/RSTP/MSTP: **stp** [**instance** *instance-id*] **root** { **primary** | **secondary** }

STP/RSTP/MSTP: **undo stp** [**instance** *instance-id*] **root**

VBST: **stp** [**vlan** { *vlan-id1* [**to** *vlan-id2*] } &<1-10>] **root** { **primary** | **secondary** }

VBST: **undo stp** [**vlan** { *vlan-id1* [**to** *vlan-id2*] } &<1-10>] **root**

Parameters

Parameter	Description	Value
instance *instance-id*	Specifies the ID of a spanning tree instance. If the parameter **instance** *instance-id* is not specified, the configuration takes effect on a CIST instance.	The value is an integer ranging from 0 to 4094. Value 0 refers to CIST. **NOTE** *instance-id* ranges from 0 to 4094. Each process supports a maximum of 65 instances.
primary	Indicates that the switch functions as the root bridge of a spanning tree.	-
secondary	Indicates that the switch functions as the secondary root bridge of a spanning tree.	-
vlan *vlan-id1* [**to** *vlan-id2*]	Specifies the VLAN to which the switch used as the root bridge or secondary root bridge belongs. ● *vlan-id1* specifies the first VLAN to which the switch used as the root bridge or secondary root bridge belongs. ● **to** *vlan-id2* specifies the last VLAN to which the switch used as the root bridge or secondary root bridge belongs. *vlan-id2* must be greater than or equal to *vlan-id1*. *vlan-id2* and *vlan-id1* determine a VLAN range. ● If **to** *vlan-id2* is not specified, the VLAN specified by *vlan-id1* is used. In the **stp root secondary** command, you can specify a maximum of 10 VLAN ranges. **NOTE** VLANs can be specified only when VBST is running.	The value is an integer that ranges from 1 to 4094.

Views

System view or MSTP process view

NOTE

VBST does not support processes. When VBST is running, you cannot run the **stp root** command in the MSTP process view.

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On a spanning tree protocol network, each spanning tree has only one root bridge, which is responsible for sending BPDUs. Owning to the importance of the root bridge, the switch with high performance and network hierarchy is generally chosen as a root bridge. The priority of such a device, however, may be not that high. Therefore, setting a high priority for the switch is necessary so that the switch can function as a root bridge.

To ensure nonstop traffic transmission, run the **stp root** command to configure the switch as the secondary root bridge. When the root bridge is faulty or is powered off, the secondary root bridge becomes the root bridge during spanning tree calculation.

NOTE

After the **stp root primary** command is run to set the switch to be the primary root bridge, the priority value of the switch is 0 in the spanning tree and the priority cannot be modified.

The secondary root bridge specified using the **stp root secondary** command has the priority value of 4096 and the priority cannot be modified.

Precautions

A spanning tree has only one root bridge.

A switch in a spanning tree cannot function both as the primary root bridge and as the secondary root bridge.

If multiple secondary root bridges are set in a spanning tree, the one with the smallest MAC address functions as the secondary root bridge of the spanning tree.

When the device connects to a non-Huawei device, you are advised to run the **stp vlan** { *vlan-id1* [**to** *vlan-id2*] } &<1-10> **priority** *priority* command to set the device priority to ensure that the root bridge is selected correctly.

When multiple MSTIs are configured, the root bridges in MSTI 0 and all other MSTIs must be specified. When the root bridge of MSTI 0 is not configured and is preempted by another device, the MSTP status of all MSTIs other than MSTI 0 will be re-converged, causing MSTP flapping.

Example

# Configure the switch as the root bridge of spanning tree instance 1 when MSTP is running.

```
<HUAWEI> system-view
[HUAWEI] stp instance 1 root primary
```

# Configure the switch as the root bridge in VLAN 10 when VBST is running.

```
<HUAWEI> system-view
[HUAWEI] stp vlan 10 root primary
```

# Configure the switch as the secondary root bridge of spanning tree instance 4 when MSTP is running.

```
<HUAWEI> system-view
[HUAWEI] stp instance 4 root secondary
```

# Configure the switch as the secondary root bridge in VLAN 10 when VBST is running.

```
<HUAWEI> system-view
[HUAWEI] stp vlan 10 root secondary
```

5.12.55 stp root-protection

Function

The **stp root-protection** command enables root protection at the current port.

The **undo stp root-protection** command restores the default setting of root protection.

By default, root protection is disabled at all ports.

Format

stp root-protection

undo stp root-protection

Parameters

None

Views

Ethernet interface view, GE interface view, XGE interface view, MultiGE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, port group view, 25GE interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Owning to incorrect configurations or malicious attacks on the network, a root bridge may receive BPDUs with a higher priority. Consequently, the root bridge is no longer able to serve as the root bridge, and the network topology is changed, triggering a spanning tree recalculation. This spanning tree recalculation may transfer traffic from high-speed links to low-speed links, causing traffic congestion.

If a designated port is enabled with the root protection function, the port role cannot be changed. Once a designated port that is enabled with root protection receives BPDUs with a higher priority, the port enters the Discarding state and does not forward packets. If the port does not receive any BPDUs with a higher priority before a period (generally two Forward Delay periods) expires, the port automatically enters the Forwarding state.

NOTE

You can run the **stp timer forward-delay** command to set the Forward Delay period.

Precautions

The root protection function takes effect only on a designated port. In addition, configuring the root protection function on a port that functions as the designated port in all instances is recommended. Generally, root protection is configured on the interfaces of the root bridge.

If the **stp root-protection** command is run on other types of ports, the root protection function does not take effect.

Loop protection and root protection cannot be configured on the same interface.

Example

# Enable the root protection function on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] stp root-protection
```

5.12.56 stp tc-notify process 0

Function

The **stp tc-notify process 0** command enables the current MSTP process to notify the specified STP instances in MSTP process 0 of receiving a TC message.

The **undo stp tc-notify process 0** command forbids the current MSTP process from notifying the specified STP instances in MSTP process 0 of receiving a TC message.

By default, the current MSTP process is disabled from notifying the STP instances in MSTP process 0 of receiving a TC message.

Format

stp tc-notify process 0

undo stp tc-notify process 0

Parameters

None

Views

MSTP process view

Default Level

2: Configuration level

Usage Guidelines

After the **stp tc-notify process 0** command is run, the current MSTP process, after receiving a TC message, notifies the MSTIs in MSTP process 0 to update MAC entries and ARP entries. This prevents user services from being interrupted.

Example

# Configure MSTP process 1 to notify MSTP process 0 of receiving a TC message.

```
<HUAWEI> system-view
[HUAWEI] stp process 1
[HUAWEI-mst-process-1] stp tc-notify process 0
```

5.12.57 stp tc-protection interval

Function

The **stp tc-protection interval** command sets the time for a device to process the maximum number of TC BPDUs.

The **undo stp tc-protection interval** command restores the default value.

By default, the time is the Hello timer length.

NOTE

When STP works in VBST mode, the default time for the device to process the maximum number of TC BPDUs is 10s.

Format

stp tc-protection interval *interval-value*

undo stp tc-protection interval

Parameters

Parameter	Description	Value
interval-value	Specifies the time for a device to process the maximum number of TC BPDUs.	The value is an integer ranging from 1 to 600, in seconds.

Views

System view or MST process region view

NOTE

VBST does not support processes. When VBST is running, you cannot run the **stp tc-protection interval** command in the MSTP process view.

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On a Layer 2 network running a spanning tree protocol, a device deletes MAC address entries and ARP entries after receiving TC packets. Frequent entry deletion may cause high CPU usage.

The TC attack defense function is enabled by default. You can configure the time, which the device takes to handle a given number of TC packets and immediately refresh forwarding entries, by running the **stp tc-protection interval** command. Within the time specified by *interval-value*, the device handles a given number of TC packets. Excess TC packets are processed by the device at once after the timer (whose length is the configured time) expires. This mechanism ensures that the device does not frequently delete its MAC entries and ARP entries, and therefore does not have excessive CPU usage.

NOTE

You can specify the maximum number of TC packets that the device processes can handle in the specified time by running the **stp tc-protection threshold** command.

Example

# Configure the time that MSTP takes to handle a given number of TC packets and immediately refreshes forwarding entries, to 10 seconds.

```
<HUAWEI> system-view
[HUAWEI] stp tc-protection interval 10
```

5.12.58 stp tc-protection threshold

Function

The **stp tc-protection threshold** command sets the number of times that a device handles received TC BPDUs and updates forwarding entries within a unit time.

The **undo stp tc-protection threshold** command restores the default setting.

By default, after a device receives TC BPDUs, the default number of times that the device handles the TC BPDUs and updates forwarding entries is 1 within a unit time.

Format

stp tc-protection threshold *threshold*

undo stp tc-protection threshold

Parameters

Parameter	Description	Value
threshold	Indicates the number of times that a device handles the TC BPDU and updates forwarding entries per unit of time.	The value is an integer ranging from 1 to 255.

Views

System view or MST process region view

NOTE

VBST does not support processes. When VBST is running, you cannot run the **stp tc-protection threshold** command in the MSTP process view.

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On a Layer 2 network where MSTP is run, a switching device that receives TC BPDUs will delete the corresponding MAC entries and ARP entries. Frequent deletion operations will greatly affect the CPU, leading to a high CPU usage.

The TC attack defense function is enabled by default, the number of times that TC BPDUs are processed by the switching device within a unit time is configurable (the default unit time is 2s, and the default number of times is 1). If the number of TC BPDUs that the switching device receives within a unit time exceeds the specified threshold, the switching device handles TC BPDUs only for the specified number of times. Additional TC BPDUs are processed by the switching device as a whole for once after the timer (that is, the specified time period) expires. In this manner, the switching device is prevented from frequently deleting its MAC entries and ARP entries so that the CPU is protected against overburden.

NOTE

The value of the unit time is consistent with the Hello time and can be set using the **stp timer hello** command.

Example

# Set the threshold update forwarding entries to 5.

```
<HUAWEI> system-view
[HUAWEI] stp tc-protection threshold 5
```

5.12.59 stp tc-restriction enable

Function

The **stp tc-restriction enable** command enables the TC restriction function.

The **undo stp tc-restriction enable** command disables the TC restriction function.

By default, the TC restriction function is disabled.

Format

stp tc-restriction enable

undo stp tc-restriction enable

Parameters

None

Views

Ethernet interface view, GE interface view, XGE interface view, MultiGE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, port group view, 25GE interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If link flapping occurs on an STP-enabled Layer 2 network, the flapping port sends BPDUs carrying the TC flag (or TCN flag in STP mode) to instruct other devices on the Layer 2 network to update ARP and MAC entries. In special scenarios, however, the customer does not want a port to update ARP or MAC entries after it receives TC or TCN packets. In this case, you can run the **stp tc-restriction enable** command on the port to enable the TC restriction function. After this function is enabled, the port neither updates its local ARP or MAC entries after receiving TC or TCN packets, nor advertises the TC or TCN information to other devices through other ports.

Precautions

After the command is run, ARP and MAC entries may fail to be updated correctly, causing a long packet loss duration in the case of topology changes. Therefore, exercise caution when you run this command.

Example

# Enable the TC restriction function on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] stp tc-restriction enable
```

5.12.60 stp timer forward-delay

Function

The **stp timer forward-delay** command sets the value of the Forward Delay of a switching device.

The **undo stp timer forward-delay** command restores the default value of the Forward Delay.

By default, the value of the Forward Delay of a switching device is 1500 centiseconds (15 seconds).

Format

stp [**vlan** { *vlan-id1* [**to** *vlan-id2*] } &<1-10>] **timer forward-delay** *forward-delay*

undo stp [**vlan** { *vlan-id1* [**to** *vlan-id2*] } &<1-10>] **timer forward-delay**

Parameters

Parameter	Description	Value
vlan *vlan-id1* [**to** *vlan-id2*]	Specifies one or more VLANs in which the Forward Delay value is set. • *vlan-id1* specifies the start VLAN ID. • **to** *vlan-id2* specifies the end VLAN ID. *vlan-id2* must be greater than or equal to *vlan-id1*. *vlan-id2* and *vlan-id1* specify a VLAN range. • If **to** *vlan-id2* is not specified, the Forward Delay value is configured for only the VLAN specified by *vlan-id1*. In the **stp timer forward-delay** command, you can specify a maximum of 10 VLAN ranges. **NOTE** VLANs can be specified only when VBST is running.	The value is an integer that ranges from 1 to 4094.
forward-delay	Specifies the value of the Forward Delay.	The value ranges from 400 to 3000 centiseconds by a step of 100.

Views

System view or MSTP process view

NOTE

VBST does not support processes. When VBST is running, you cannot run the **stp timer forward-delay** command in the MSTP process view.

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On a network running a spanning tree algorithm, if the network topology is changed, it takes time to advertise new BPDU configuration messages on the network. During this period, interfaces to be blocked may not be blocked in time and interface ever blocked may not be blocked. As a result, a temporary loop may be formed. To prevent this problem, you can use the Forward Delay timer to set a delay time. During the delay time, all interfaces are blocked temporarily.

The **stp timer forward-delay** command is used to set the Forward Delay timer.

Precautions

The value of the Forward Delay timer set on the root bridge is advertised to other devices of the same spanning tree using BPDUs. Then it becomes the value of the Forward Delay timer of all devices in the spanning tree.

The relationships between the Hello Time, Forward Delay, and MaxAge are as follows. The spanning tree functions properly only if the correct relationships are established. Otherwise, frequent network flapping occurs.

- 2 x (Forward Delay - 1.0 second) ≥ Max Age
- Max Age ≥ 2 x (Hello Time + 1.0 second)

Running the **stp bridge-diameter** command to set the network diameter is recommended. After the **stp bridge-diameter** command is run, the switching device sets optimum values for the three parameters, Hello Time, Forward Delay, and Max Age.

Example

# Set the Forward Delay to 2000 centiseconds (20 seconds) when STP/RSTP/MSTP is running.

```
<HUAWEI> system-view
[HUAWEI] stp timer forward-delay 2000
```

# Set the Forward Delay value to 2000 centiseconds (20 seconds) for VLAN 10 when VBST is running.

```
<HUAWEI> system-view
[HUAWEI] stp vlan 10 timer forward-delay 2000
```

5.12.61 stp timer hello

Function

The **stp timer hello** command sets the interval of the switching device to send BPDUs, that is, the value of the Hello Time.

The **undo stp timer hello** command restores the default setting.

By default, the interval of the switch to send BPDUs is 200 centiseconds (2 seconds).

Format

stp [**vlan** { *vlan-id1* [**to** *vlan-id2*] } &<1-10>] **timer hello** *hello-time*

undo stp [**vlan** { *vlan-id1* [**to** *vlan-id2*] } &<1-10>] **timer hello**

Parameters

Parameter	Description	Value
vlan *vlan-id1* [**to** *vlan-id2*]	Specifies one or more VLANs in which the Hello timer value is set. ● *vlan-id1* specifies the start VLAN ID. ● **to** *vlan-id2* specifies the end VLAN ID. *vlan-id2* must be greater than or equal to *vlan-id1*. *vlan-id2* and *vlan-id1* specify a VLAN range. ● If **to** *vlan-id2* is not specified, the Hello timer value is configured for only the VLAN specified by *vlan-id1*. In the **stp timer hello** command, you can specify a maximum of 10 VLAN ranges. **NOTE** VLANs can be specified only when VBST is running.	The value is an integer that ranges from 1 to 4094.
hello-time	Specifies the interval of the switch to send BPDUs.	The value ranges from 100 to 1000, in centiseconds by a step of 100.

Views

System view or MSTP process view

NOTE

VBST does not support processes. When VBST is running, you cannot run the **stp timer hello** command in the MSTP process view.

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On a network where a spanning tree protocol is enabled, a switching device periodically sends BPDUs to other devices in the same spanning tree at the interval of the Hello Time. Sending BPDUs periodically ensures that the spanning tree is stable. The **stp timer hello** command can be used to set the BPDU sending interval, that is, the Hello Time.

If no BPDUs are received by the switching device within the timeout period (timeout period = Hello Time x 3 x Timer Factor), the spanning tree is calculated again.

NOTE

In a spanning tree, the device closer to the root bridge is the upstream device of another connected device.

Precautions

The value of the Hello Time set on the root bridge is advertised to other devices of the same spanning tree using BPDUs. Then it becomes the value of the Hello Time of all devices in the spanning tree.

The relationships between the Hello Time, Forward Delay, and Max Age are as follows. The spanning tree works properly only if the relationships are correctly established. Otherwise, frequent network flapping occurs.

- 2 x (Forward Delay - 1.0 second) ≥ Max Age
- Max Age ≥ 2 x (Hello Time + 1.0 second)

Running the **stp bridge-diameter** command to set the network diameter is recommended. After the **stp bridge-diameter** command is run, the switching device sets optimum values for the three parameters, Hello Time, Forward Delay, and Max Age.

Example

# Set the Hello Time to 400 centiseconds (4 seconds) when STP/RSTP/MSTP is running.

```
<HUAWEI> system-view
[HUAWEI] stp timer hello 400
```

# Set the Hello time to 400 centiseconds (4 seconds) for VLAN 10 when VBST is running.

```
<HUAWEI> system-view
[HUAWEI] stp vlan 10 timer hello 400
```

5.12.62 stp timer max-age

Function

The **stp timer max-age** command sets the Max Age of a switching device, that is, the BPDU aging time on a port of the switching device.

The **undo stp timer max-age** command restores the default setting.

By default, the Max Age of a switching device is 2000 centiseconds (20 seconds).

Format

stp [**vlan** { *vlan-id1* [**to** *vlan-id2*] } &<1-10>] **timer max-age** *max-age*

undo stp [**vlan** { *vlan-id1* [**to** *vlan-id2*] } &<1-10>] **timer max-age**

Parameters

Parameter	Description	Value
vlan *vlan-id1* [**to** *vlan-id2*]	Specifies one or more VLANs in which the Max Age value is set. ● *vlan-id1* specifies the start VLAN ID. ● **to** *vlan-id2* specifies the end VLAN ID. *vlan-id2* must be greater than or equal to *vlan-id1*. *vlan-id2* and *vlan-id1* specify a VLAN range. ● If **to** *vlan-id2* is not specified, the Max Age value is configured only for the VLAN specified by *vlan-id1*. In the **stp timer max-age** command, you can specify a maximum of 10 VLAN ranges. **NOTE** VLANs can be specified only when VBST is running.	The value is an integer that ranges from 1 to 4094.
max-age	Specifies the BPDU aging time on a port of the switch.	The value ranges from 600 to 4000 in centiseconds with a step of 100.

Views

System view or MST process region view

NOTE

VBST does not support processes. When VBST is running, you cannot run the **stp timer max-age** command in the MSTP process view.

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On a network where a spanning tree protocol is enabled, a switching device checks whether the BPDUs received from an upstream switching device time out based on the set Max Age value. If the received BPDUs time out, the switching device ages the BPDUs and blocks the port that receives the BPDUs. Then, the switching device sends the BPDUs with the switching device as the root bridge. This aging mechanism effectively controls the diameter of the spanning tree. After the **stp timer max-age** command is run, the Max Age value is set to control the timeout period of received BPDUs.

NOTE

In a spanning tree, the device closer to the root bridge is the upstream device of another connected device.

Precautions

The value of the Max Age set on the root bridge is advertised to other devices of the same spanning tree using BPDUs. Then it becomes the MaxAge value of all devices in the spanning tree.

The relationships between the Hello Time, Forward Delay, and Max Age are as follows. The spanning tree functions properly only if the relationships are correctly established. Otherwise, frequent network flapping occurs.

- 2 x (Forward Delay - 1.0 second) ≥ Max Age
- Max Age ≥ 2 x (Hello Time + 1.0 second)

Running the **stp bridge-diameter** command to set the network diameter is recommended. After the **stp bridge-diameter** command is run, the switching device sets optimum values for the three parameters, Hello Time, Forward Delay, and Max Age.

Example

# Set the Max Age to 1000 centiseconds (10 seconds) when STP/RSTP/MSTP is running.

```
<HUAWEI> system-view
[HUAWEI] stp timer max-age 1000
```

# Set the Max Age value to 1000 centiseconds (10 seconds) for VLAN 10 when VBST is running.

```
<HUAWEI> system-view
[HUAWEI] stp vlan 10 timer max-age 1000
```

5.12.63 stp timer-factor

Function

The **stp timer-factor** command sets the timer factor of the timeout period of a switching device to the Hello Time.

The **undo stp timer-factor** command restores the default setting.

By default, the timer factor is 3.

NOTE

If a switching device does not receive BPDUs from an upstream device within the timeout period (timeout period = Hello Time × 3 × Timer Factor), the spanning tree is calculated again.

Format

stp timer-factor *factor*

undo stp timer-factor

Parameters

Parameter	Description	Value
factor	Specifies the timer factor.	The value ranges from 1 to 10.

Views

System view or MSTP process view

NOTE

VBST does not support processes. When VBST is running, you cannot run the **stp timer-factor** command in the MSTP process view.

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On a network where a spanning tree protocol is enabled, if a switching device does not receive BPDUs from an upstream device within the timeout period, it considers that the upstream device becomes faulty, and will recalculate the spanning tree.

Sometimes, however, the failure of the upstream device to send BPDUs within the timeout period is only because it is busy processing services. In this case, the spanning tree cannot be calculated. Therefore, you can set a long timeout period on a stable network to avoid the waste of network resources.

NOTE

In a spanning tree, the device closer to the root bridge is the upstream device of another connected device.

Precautions

If the parameter *factor* is set smaller, the timeout period of the switching device to re-calculate the spanning tree is shorter. In this case, there is a higher probability that the switching device incorrectly considers the upstream device as being faulty.

If the parameter *factor* is set larger, the timeout period of the switching device to re-calculate the spanning tree is longer. In this case, there is a higher probability that the traffic becomes interrupted because the upstream device has become faulty.

Example

# Set the timer factor of the switching device to 6.

```
<HUAWEI> system-view
[HUAWEI] stp timer-factor 6
```

5.12.64 stp transmit-limit (interface view)

Function

The **stp transmit-limit** command sets the maximum number of BPDUs that the current port can send in a specified period.

The **undo stp transmit-limit** command restores the default maximum BPDUs.

By default, the maximum number of BPDUs that a port sends is 6 per second.

Format

stp transmit-limit *packet-number*

undo stp transmit-limit

Parameters

Parameter	Description	Value
packet-number	Specifies the maximum number of BPDUs that a port can send in a specified period.	The value is an integer that ranges from 1 to 255.

Views

Ethernet interface view, GE interface view, XGE interface view, MultiGE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, port group view, 25GE interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On a network where a spanning tree protocol is enabled, a switching device periodically sends BPDUs to other devices in the same spanning tree with the interval of the Hello Time. Sending BPDUs periodically ensures that the spanning tree is stable. If the number of sent BPDUs is great in a specified period, excessive system and bandwidth resources will be consumed.

To prevent this problem from occurring, run the **stp transmit-limit** command to set the maximum number of BPDUs that can be sent by an interface in a specified period. In this manner, the BPDU sending speed is controlled, preventing excessive use of system and bandwidth resources by MSTP when the network topology flaps.

Precautions

After the **stp transmit-limit** command is configured, the maximum number of BPDUs sent in a specified period by the interface is determined by the set value.

Example

# Set the maximum BPDUs that GE0/0/1 can send in a specified period to 5.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] stp transmit-limit 5
```

5.12.65 stp transmit-limit (system view)

Function

The **stp transmit-limit** command configures the maximum number of Bridge Protocol Data Units (BPDUs) that each interface of the local device can send per second.

The **undo stp transmit-limit** command restores the maximum number of BPDUs, which can be sent by each interface of the local device per second, to the default value.

By default, each interface can send a maximum of 6 BPDUs per second.

Format

stp transmit-limit *packet-number*

undo stp transmit-limit

Parameters

Parameter	Description	Value
packet-number	Maximum number of BPDUs that each interface of the local device can send per second	The value is an integer ranging from 1 to 255.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On a network running the Spanning Tree Protocol (STP), a switch sends BPDUs to other devices in the same spanning tree at the interval of the Hello time, to maintain the spanning tree stability. If a large number of BPDUs are sent every second, system and bandwidth resources will be greatly consumed.

NOTE

You can configure the Hello time by using the **stp timer hello** command. The Hello time is the length of the Hello timer and specifies the interval at which the switch sends BPDUs.

To prevent excessive usage of system and bandwidth resources, you can run the **stp transmit-limit** command to configure the maximum number of BPDUs that each interface of the local device can send per second. This configuration controls the BPDU sending rate and prevents the Multiple Spanning Tree Protocol (MSTP) from consuming too many system and bandwidth resources when topology flapping occurs.

Precautions

After the **stp transmit-limit** command is executed, *packet-number* controls the maximum number of BPDUs that each interface can send per second.

You can also configure the maximum number of BPDUs that a specific interface can send per second by running the **stp transmit-limit (interface view)** command in the view of this interface. The **stp transmit-limit (interface view)** command configuration in the interface view takes precedence over the **stp transmit-limit** command configuration in the system view. That is, if the **stp transmit-limit (interface view)** command is configured in the view of an interface, the **stp transmit-limit** command configuration in the system view does not take effect for this interface.

Example

# Configure the maximum number of BPDUs that each interface of the local device can send per second to **5**.

```
<HUAWEI> system-view
[HUAWEI] stp transmit-limit 5
```

5.12.66 stp vlan enable

Function

The **stp vlan enable** command enables VBST in a VLAN on the switch.

The **stp vlan disable** command disables VBST in a VLAN on the switch.

The **undo stp vlan disable** command restores the default VBST status in a VLAN on the switch.

By default, VBST is enabled in a VLAN on the switch.

Format

stp vlan { *vlan-id1* [**to** *vlan-id2*] } &<1-10> **enable**

stp vlan { *vlan-id1* [**to** *vlan-id2*] } &<1-10> **disable**

undo stp vlan { *vlan-id1* [**to** *vlan-id2*] } &<1-10> **disable**

Parameters

Parameter	Description	Value
vlan *vlan-id1* [**to** *vlan-id2*]	Specifies one or more VLANs in which VBST is enabled. ● *vlan-id1* specifies the start VLAN ID. ● **to** *vlan-id2* specifies the end VLAN ID. *vlan-id2* must be greater than or equal to *vlan-id1*. *vlan-id2* and *vlan-id1* specify a VLAN range. ● If **to** *vlan-id2* is not specified, VBST is enabled only for the VLAN specified by *vlan-id1*. In the **stp enable** command, you can specify a maximum of 10 VLAN ranges.	The value is an integer that ranges from 1 to 4094.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On a complex Layer 2 network, to prevent or eliminate loops and allow traffic in different VLANs to be forwarded along spanning trees to implement load balancing, deploy VBST on the switch.

Spanning tree calculation occupies system resources. Therefore, run the **stp vlan disable** command to disable VBST in a VLAN where spanning tree calculation does not need to be performed.

Pre-configuration Tasks

When VBST is enabled on a ring network, VBST immediately starts spanning tree calculation. Parameters such as the switch priority and port priority affect spanning tree calculation, and change of these parameters may cause network flapping. To ensure fast and stable spanning tree calculation, perform basic configurations on the switch and ports before enabling VBST.

- Run the **stp mode vbst** command to set the working mode of the switch.
- Run the **stp vlan** { *vlan-id1* [**to** *vlan-id2*] } &<1-10> **priority** *priority* command to set the priority of the switch in the spanning tree.
- Run the **stp vlan** { *vlan-id1* [**to** *vlan-id2*] } &<1-10> **port priority** *priority* command to set the priority of the port in the spanning tree instance.
- Run the **stp vlan** { *vlan-id1* [**to** *vlan-id2*] } &<1-10> **root primary** command to set the switch as the root bridge of the spanning tree instance.
- Run the **stp vlan** { *vlan-id1* [**to** *vlan-id2*] } &<1-10> **root secondary** command to set the switch as the secondary root bridge of the spanning tree.
- Run the **stp vlan** { *vlan-id1* [**to** *vlan-id2*] } &<1-10> **cost***cost* command to set the path cost of the port in the spanning tree instance.
- Run the **instance** *instance-id* **vlan** *vlan-id* command to configure 1:1 mapping between MSTIs and VLANs.

Configurations are needed based on real-world situations.

Precautions

When VBST is enabled globally and in a VLAN, the interface that belongs to the VLAN participates in spanning tree calculation. Whether the interface is in forwarding state depends on the calculation result.

When VBST is disabled in a VLAN, the interface that belongs to the VLAN does not participate in spanning tree calculation and is in forwarding state in the VLAN.

VBST cannot be enabled in the ignored VLAN or control VLAN used by ERPS, RRPP, SEP, or Smart Link.

If VLAN mapping or VLAN stacking is configured on an interface corresponding to the VLAN, VBST negotiation for this VLAN will fail.

Example

# Enable VBST in VLAN 5.

```
<HUAWEI> system-view
[HUAWEI] stp vlan 5 enable
```

# Disable VBST in VLAN 5.

```
<HUAWEI> system-view
```

```
[HUAWEI] stp vlan 5 disable
```

5.12.67 stp vpls-subinterface enable

Function

The **stp vpls-subinterface enable** command enables a main interface to notify its sub-interface bound to a VSI of the received TC BPDUs.

The **undo stp vpls-subinterface enable** command disables a main interface from notifying its sub-interface bound to a VSI of the received TC BPDUs.

By default, a main interface is disabled from notifying its sub-interface bound to a VSI of the received TC BPDUs.

NOTE

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

Format

stp vpls-subinterface enable

undo stp vpls-subinterface enable

Parameters

None.

Views

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

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If an MSTP-enabled interface has a sub-interface configured with L2VPN, you can run the **stp vpls-subinterface enable** command to enable the main interface to notify its sub-interface bound to a VSI of the received TC BPDUs. After the main interface receives TC BPDUs, the main interface can notify the sub-interface bound to the VSI of updating MAC address entries and ARP entries. This function ensures nonstop services. When the **stp vpls-subinterface enable** command is used and the main interface is in Discarding state, the sub-interface bound to the VSI enters the flowdown state. This prevents loops on a VPLS network when CEs are dual-homed to PEs.

This command does not take effect when VBST is running. If this command has been run in STP/RSTP/MSTP mode, switching the STP/RSTP/MSTP mode to VBST mode fails, and the system displays a message indicating switching failure

Precautions

When the forwarding status of an interface moves to Discarding, its VSI-bound sub-interfaces will move to the Discarding state to prevent loops on the VPLS network on which a CE is dual-homed to two PEs.

The **stp vpls-subinterface enable** and **erps vpls-subinterface enable** commands are mutually exclusive on the same interface.

Example

# Enable the 40GE0/0/1 to notify its sub-interface bound to a VSI of the received TC BPDUs.

```
<HUAWEI> system-view
[HUAWEI] interface 40ge 0/0/1
[HUAWEI-40GE0/0/1] stp vpls-subinterface enable
```

5.12.68 vlan-mapping modulo

Function

The **vlan-mapping modulo** command enables VLAN-to-instance mapping assignment based on a default algorithm.

The **undo vlan-mapping modulo** command restores the default mapping.

By default, all VLANs are mapped to CIST, namely, spanning tree instance 0.

Format

vlan-mapping modulo *modulo*

undo vlan-mapping modulo

Parameters

Parameter	Description	Value
modulo	Specifies the value of a module.	The value is an integer ranging from 1 to 64.

Views

MST region view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

MSTP divides a switching network into multiple regions, each of which has multiple spanning trees that are independent of each other. Each spanning tree is called an MSTI and each region is called an MST region.

Two switching devices belong to the same MST region only when they have the following same configurations:

- MST region name
- Mappings between MSTIs and VLANs
- MST region revision level

The **vlan-mapping modulo** command is used to enable VLAN-to-instance mapping assignment based on a default algorithm.

NOTE

In the command, **vlan-mapping modulo** indicates that the formula (VLAN ID-1)%modulo +1 is used. In the formula, (VLAN ID-1)%modulo means the remainder of (VLAN ID-1) divided by the value of modulo. This formula is used to map a VLAN to the corresponding MSTI. The calculation result of the formula is ID of the mapping MSTI. For example, if the modulus is 16, the switch maps VLAN 1 to MSTI 1, VLAN 2 to MSTI 2 VLAN 16 to MSTI 16, VLAN 17 to MSTI 1, and so on.

Precautions

The **instance** *instance-id* **vlan** { *vlan-id* [**to** *vlan-id*] }&<1-10> command is recommended because VLAN-to-instance mapping assignments cannot meet actual mapping requirements.

VBST does not support regions. Therefore, this command does not take effect when the spanning tree protocol is VBST.

Example

# Map all VLANs to spanning tree instances modulo 16.

```
<HUAWEI> system-view
[HUAWEI] stp region-configuration
[HUAWEI-mst-region] vlan-mapping modulo 16
```

5.13 SEP Configuration Commands

5.13.1 Command Support

Commands provided in this section and all the parameters in the commands are supported by all switch models (except the S5731-L and S5731S-L), unless otherwise specified. For details, see specific commands.

5.13.2 block port

Function

The **block port** command configures the mode in which an interface is blocked on the device where the primary edge interface resides.

The **undo block port** command restores the default mode in which an interface is blocked on the device where the primary edge interface resides.

By default, the system selects a blocked interface from the interfaces on both ends of the link that is established last or the link that recovers from a fault last.

Format

block port { **sysname** *sysname* **interface** *interface-type interface-number* | **hop** *hop-id* | **optimal** | **middle** }

undo block port

Parameters

Parameter	Description	Value
sysname *sysname*	Specifies the name of the device where the interface to be blocked resides.	The value is a string of 1 to 20 case-sensitive characters without spaces. When double quotation marks are used around the string, spaces are allowed in the string.
interface *interface-type interface-number*	Specifies the interface to be blocked. *interface-type* indicates the type of the interface to be blocked. After SEP is enabled, **sysname** *sysname* and **interface** { *interface-type interface-number* } specify the interface to be blocked. Before configuring the mode in which an interface is blocked, run the **display sep topology verbose** command to view detailed information about the topology of the current ring and obtain information about all the interfaces in the topology. Then, you can specify the device and interface names.	-

Parameter	Description	Value
hop *hop-id*	Specifies the interface with the specified hop count from the primary edge interface as the blocked interface. *hop-id* specifies the hop count. If *hop-id* is set to 1, the primary edge interface is blocked. If *hop-id* is set to 2, the neighboring interface of the primary edge interface is blocked. The hop count increases by steps of 1 in the downstream direction of the primary edge interface.	The value is an integer that ranges from 1 to 128.
optimal	Specifies the interface with the highest priority as the blocked interface. SEP compares interface priorities as follows: 1. A larger value set using the **sep segment priority** command indicates a higher priority. 2. If interfaces have the same priority value, a smaller bridge MAC address indicates a higher priority. 3. If interfaces have the same priority value and the same bridge MAC address, a smaller interface number indicates a higher priority.	-
middle	Specifies the interface in the middle of the SEP segment as the blocked interface.	-

Views

SEP segment view

Default Level

2: Configuration level

Usage Guidelines

In a SEP segment, some interfaces are blocked to prevent loops. Any interface in a SEP segment may be blocked if no interface is specified for blocking. A complete SEP segment contains only one blocked interface.

You can specify the blocked interface according to network requirements or your reference. The specified interface is not blocked immediately. Normally, the blocked interface is one of the two interfaces that complete neighbor negotiations last. The specified interface preempts to be the blocked interface only after the preemption mechanism takes effect.

The SEP segment must have been created before the **block port** command is used.

To make the **block port** command configuration take effect, complete the following tasks before using the **block port** command.

- Run the **sep segment** command in the system view to create a SEP segment.
- Run the **control-vlan (SEP segment view)** command to configure the control VLAN of the SEP segment.
- Run the **sep segment (interface view)** command to add the interface to the SEP segment and configure the interface as the primary edge interface.

Example

# On the device where the primary edge interface is located, specify the device and interface names to block the specified interface.

```
<HUAWEI> system-view
[HUAWEI] sep segment 1
[HUAWEI-sep-segment1] block port sysname HUAWEI interface gigabitethernet 0/0/1
```

# On the device where the primary edge interface is located, specify the interface with the specified hop count from the primary edge interface as the interface to be blocked.

```
<HUAWEI> system-view
[HUAWEI] sep segment 1
[HUAWEI-sep-segment1] block port hop 3
```

# On the device where the primary edge interface is located, specify the interface with the highest priority as the interface to be blocked.

```
<HUAWEI> system-view
[HUAWEI] sep segment 1
[HUAWEI-sep-segment1] block port optimal
```

# On the device where the primary edge interface is located, specify the interface in the middle of the SEP segment as the interface to be blocked.

```
<HUAWEI> system-view
[HUAWEI] sep segment 1
[HUAWEI-sep-segment1] block port middle
```

5.13.3 control-vlan (SEP segment view)

Function

The **control-vlan** command configures the control VLAN of a SEP segment for SEP packet transmission.

The **undo control-vlan** command deletes the configured control VLAN.

By default, no control VLAN is configured in a SEP segment.

Format

control-vlan *vlan-id*

undo control-vlan

Parameters

Parameter	Description	Value
vlan-id	Specifies the ID of the control VLAN in a SEP segment.	The value is an integer that ranges from 1 to 4094.

Views

SEP segment view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After a SEP segment is created, run the **control-vlan** command to create a control VLAN for the SEP segment.

Compared with a data VLAN, a control VLAN forwards only SEP packets but not service packets in a SEP segment, which improves SEP security.

Precautions

- Devices in the same SEP segment must be configured with the same control VLAN to fast forward SEP packets. Different SEP segments can use the same control VLAN.
- In the absence of neighbors, devices that are not in a SEP segment cannot be added to the control VLAN of the SEP segment. Otherwise, network loops occur.
- The control VLAN must be not created, and is not used by other features. In addition, no interface is added to the control VLAN.
- To check whether the control VLAN is created or view the control VLAN where SEP packets are transmitted, run the **display sep interface** command and specify the **verbose** parameter.
- You must configure the control VLAN of a SEP segment before adding interfaces to the SEP segment.
  - If the SEP segment contains an interface, the control VLAN cannot be deleted. To delete the configured control VLAN, run the **undo sep segment** command in the interface view to remove the interface from the SEP segment, and then run the **undo control-vlan** command.
  - If the SEP segment contains no interface, you can configure the control VLAN multiple times. Only the latest configuration takes effect.
  - After the control VLAN is created, the configuration file automatically displays the command for creating the VLAN.

    Each SEP segment must have a control VLAN. After an interface is added to a SEP segment that has a control VLAN, the interface is automatically added to the control VLAN.

- If the interface type is trunk, in the configuration file, the **port trunk allow-pass vlan** command is displayed in the view of the interface added to the SEP segment.
- If the interface type is hybrid, in the configuration file, the **port hybrid tagged vlan** command is displayed in the view of the interface added to the SEP segment.

Example

# Configure control VLAN 5 for SEP segment 1.

```
<HUAWEI> system-view
[HUAWEI] sep segment 1
[HUAWEI-sep-segment1] control-vlan 5
```

5.13.4 deal smart-link-flush

Function

The **deal smart-link-flush** command enables a device in a SEP segment to process SmartLink Flush packets.

The **undo deal smart-link-flush** command disables a device in a SEP segment from processing SmartLink Flush packets.

By default, a device in a SEP segment is disabled from processing SmartLink Flush packets.

Format

deal smart-link-flush

undo deal smart-link-flush

Parameters

None

Views

SEP segment view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When a host is connected to a SEP network through a SmartLink group, the host sends SmartLink Flush packets to the connected devices in the SEP segment, if the active/standby switchover of member interfaces in the SmartLink group occurs. In this situation, the **deal smart-link-flush** command must be used to enable the devices in the SEP segment to process SmartLink Flush packets.

Prerequisites

Interfaces have been added to the SEP segment.

Precautions

After the **deal smart-link-flush** command is used, the device that receives a SmartLink Flush packet in the SEP segment floods the forwarding database (FDB) to notify the other devices in the SEP segment of topology changes. The other devices then refresh their MAC address entries to ensure reliable traffic transmission.

The **deal smart-link-flush** command must be run on the device that receives SmartLink Flush packets and the interfaces on the device have been added to the SEP segment.

Example

# Enable a device in SEP segment 1 to process SmartLink Flush packets.

```
<HUAWEI> system-view
[HUAWEI] sep segment 1
[HUAWEI-sep-segment1] deal smart-link-flush
```

5.13.5 description (SEP segment view)

Function

The **description** command configures the description of the SEP segment.

The **undo description** command restores the default setting.

By default, the description of a SEP segment is null.

Format

description *text*

undo description

Parameters

Parameter	Description	Value
text	Specifies the description of a SEP segment	The value is a string of 1 to 255 case-sensitive characters with spaces supported.

Views

SEP segment view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On a device running SEP, you can run the **description** command to configure the description of the SEP segment, such as the SEP segment ID. Configuring the description of a SEP segment facilitates the maintenance of the SEP segment.

Precautions

After being configured in the SEP-Segment view, the description command takes effect only on the local device.

Example

# Configure the description **It's segment 10** for SEP segment 10.

```
<HUAWEI> system-view
[HUAWEI] sep segment 10
[HUAWEI-sep-segment10] description It's segment 10
```

5.13.6 display sep error packet

Function

The **display sep error packet** command displays the statistics about error packets received by SEP and the contents of recently received packets.

Format

display sep error packet

Parameters

None.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

If a device on a Layer 2 network runs SEP is attacked by SEP error packets, the **display sep error packet** command can be used to view recently received MSTP error packets.

Example

Display the statistics about error packets received by SEP and the contents of recently received packets.

```
<HUAWEI> display sep error packet
4 error-packets have been received and the last

one is received at 2012/05/02 12:45:31 UTC+08:00 :


01 80 c2 00 00 02 00 e0 fc 8e 0b 34 88 09 01 01
01 14 80 00 00 e0 fc 8e 0b 34 01 21 80 00 09 06
47 00 00 00 02 14 00 00 00 00 00 00 00 00 00 00
00 00 00 00 c7 00 00 00 03 10 ff ff 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00
```

5.13.7 display sep interface

Function

The **display sep interface** command displays information about the interfaces in a SEP segment.

Format

display sep interface [*interface-type interface-number* | **segment** *segment-id*] [**verbose**]

Parameters

Parameter	Description	Value
interface-type interface-number	Displays SEP information on a specified interface. *interface-type* specifies the type of an interface. *interface-number* specifies the number of an interface.	-
segment *segment-id*	Displays information about the interfaces in a specified SEP segment.	The value is an integer that ranges from 1 to 1024.
verbose	Displays detailed SEP information on a specified interface, including traffic statistics.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

To monitor the status of an interface or locate an interface fault, use this command to collect statistics and the status of the interface. Then you can locate the interface fault according to the statistics.

When using the **display sep interface** command:

- If no parameter is specified, this command displays information about all the interfaces in SEP segments.
- If only *interface-type interface-number* is specified, this command displays information about a specified interface in SEP segments.
- If only **segment** *segment-id* is specified, this command displays information about all the interfaces in a specified SEP segment.
- If only **verbose** is specified, this command displays detailed information about all the interfaces in SEP segments.
- If *interface-type interface-number* and **verbose** are specified, this command displays detailed information about a specified interface in SEP segments.
- If **segment** *segment-id* and **verbose** are specified, this command displays detailed information about a specified interface in a specified SEP segment.

NOTE

Before running this command, complete the following tasks:

- Run the **sep segment** command in the system view to create a SEP segment.
- Run the **sep segment (interface view)** command in the Ethernet interface view to add an interface to a SEP segment and set the role of the interface as required.

Example

# Display information about all the interfaces in SEP segments.

```
<HUAWEI> display sep interface
SEP segment 1
----------------------------------------------------------------
Interface        Port Role      Neighbor Status           Port Status
----------------------------------------------------------------
GE0/0/1            *secondary    up                forwarding
GE0/0/2            common         up                forwarding
```

# Display information about a specified interface in SEP segments.

```
<HUAWEI> display sep interface gigabitethernet 0/0/1
SEP segment 1
----------------------------------------------------------------
Interface          Port Role     Neighbor Status     Port Status
----------------------------------------------------------------
GE0/0/1            common        up                forwarding
```

# Display detailed information about a specified interface in a specified SEP segment.

```
<HUAWEI> display sep interface segment 1 verbose
SEP segment 1
Control-vlan          :3
```

```
Preempt Delay Timer    :15
TC-Notify Propagate to :stp
----------------------------------------------------------------
Interface              :GE0/0/1
Port Role              :Config = *primary / Active =  *secondary
Port Priority          :64
Port Status            :forwarding
Neighbor Status        :up
Neighbor Port          :NULL
NBR TLV             rx :0                tx :0
LSP INFO TLV        rx :0                tx :0
LSP ACK TLV         rx :0                tx :0
PREEMPT REQ TLV     rx :0                tx :0
PREEMPT ACK TLV     rx :0                tx :0
TC Notify           rx :0                tx :0
EPA                 rx :0                tx :0
Interface              :GE0/0/2
Port Role              :Config = common / Active =  common
Port Priority          :64
Port Status            :forwarding
Neighbor Status        :up
Neighbor Port          :LSW3 - GE0/0/1 (00e0-ff7c-6400.0000)
NBR TLV             rx :51820            tx :51882
LSP INFO TLV        rx :50380            tx :5776
LSP ACK TLV         rx :5749             tx :50296
PREEMPT REQ TLV     rx :0                tx :1
PREEMPT ACK TLV     rx :4                tx :0
TC Notify           rx :22               tx :3
EPA                 rx :0                tx :0
```

Table 5-94 Description of the **display sep interface** command output

Item	Description
SEP segment	ID of a SEP segment. To specify the parameter, run the **sep segment** command.
Interface	Interface name.
Port Role	Role of an interface in a SEP segment: ● common: common interface ● primary: primary edge interface ● secondary: secondary edge interface ● *primary: no-neighbor primary edge interface ● *secondary: no-neighbor secondary edge interface
Neighbor Status	Status of the neighbor state machine: ● up: Neighbor negotiations succeed and the protocol status of the interface is Up. ● down: Neighbor negotiations fail and no neighbor relationship is established between the local interface and its peer interface. ● init: The local interface receives packets from the peer interface and neighbor negotiations start. ● conflict: The local interface receives packets from multiple peer interfaces and the protocol status of the interface is Conflict.

Item	Description
Port Status	Current status of the interface: - discarding: The interface is blocked and can forward SEP packets but not data packets. - forwarding: The interface is in Forwarding state and can forward both data packets and SEP packets.
Port Priority	Interface priority. It is an integer that ranges from 1 to 128. By default, the interface priority is 64. To specify the parameter, run the **sep segment priority** command.
Control-vlan	ID of a control VLAN. A control VLAN is used to forward SEP packets in the local SEP segment. To specify the parameter, run the **control-vlan** command.
Preempt Delay Timer	Delay in preempting the blocked interface after the faulty link recovers, in seconds. To specify the parameter, run the **preempt** command.
TC-Notify Propagate to	Object to be notified of a topology change. To specify the parameter, run the **tc-notify** command.
Neighbor Port	Neighbor interface. It is in the format of system name +interface name (system MAC address or interface ID). If there is no neighbor, the value is NULL.
NBR TLV	Neighbor information packet: - rx: indicates the number of received neighbor information packets. - tx: indicates the number of sent neighbor information packets.
LSP INFO TLV	LSA packets: - rx: indicates the number of received LSA packets. - tx: indicates the number of sent LSA packets.
LSP ACK TLV	ACK packets in response to LSA packets: - rx: indicates the number of received ACK packets in response to LSA packets. - tx: indicates the number of sent ACK packets in response to LSA packets.
PREEMPT REQ TLV	Preemption packets: - rx: indicates the number of received preemption packets. - tx: indicates the number of sent preemption packets.
PREEMPT ACK TLV	ACK packets in response to preemption packets: - rx: indicates the number of received ACK packets in response to preemption packets. - tx: indicates the number of sent ACK packets in response to preemption packets.

Item	Description
TC Notify	Packets reporting topology changes: ● rx: indicates the number of received packets reporting topology changes. ● tx: indicates the number of sent packets reporting topology changes.
EPA	Packets reporting edge port selection: ● rx: indicates the number of received packets reporting edge port selection. ● tx: indicates the number of sent packets reporting edge port selection.

5.13.8 display sep segment

Function

The **display sep segment** command displays the configurations of SEP segments.

Format

display sep segment {*segment-id* | **all** }

Parameters

Parameter	Description	Value
segment-id	Displays the configuration of a specified SEP segment.	The value is an integer that ranges from 1 to 1024.
all	Displays the configurations of all SEP segments.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After SEP is configured, you can run the **display sep segment** command to view the configuration of a specified SEP segment or all SEP segments on the network.

Example

# Display the configuration of SEP segment 2.

```
<HUAWEI> display sep segment 2
----------------------------------------------------------------
SEP Segment ID          :2
SEP Control-vlan        :3
Protected-instance      :0 to 5 9 12 to 13 16 to 17 20 to 21
Preempt Delay Timer(s) :20/0 (Configured/Remaining)
Block Port Expected     :Eth-Trunk2
Name of Port Member     :Eth-Trunk3
TC-Notify Propagate to :segment 6
```

# Display the configurations of all SEP segments.

```
<HUAWEI> display sep segment all
----------------------------------------------------------------
SEP Segment ID          :1
SEP Control-vlan        :10
Protected-instance      :0 to 48
Preempt Delay Timer(s) :20/0 (Configured/Remaining)
Block Port Expected     :Eth-Trunk2
Name of Port Member     :GE0/0/1
TC-Notify Propagate to :segment 6
----------------------------------------------------------------
SEP Segment ID          :2
SEP Control-vlan        :3
Protected-instance      :0 to 5 9 12 to 13 16 to 17 20 to 21
Preempt Delay Timer(s) :20/0 (Configured/Remaining)
Block Port Expected     :Eth-Trunk2
Name of Port Member     :Eth-Trunk3
TC-Notify Propagate to :segment 6
----------------------------------------------------------------
Total number of segment configured = 2
```

Table 5-95 Description of the **display sep segment** command output

Item	Description
SEP Segment ID	ID of a SEP segment. To specify the parameter, run the **sep segment** command.
SEP Control-vlan	Control VLAN for transmitting SEP packets. To specify the parameter, run the **control-vlan** command.
Protected-instance	ID of a protected instance. To specify the parameter, run the **protected-instance** command.
Preempt Delay Timer(s)	Delay in preemption. ● Configured: configured value of the Preempt Delay Timer (s). ● Remaining: remaining value of the Preempt Delay Timer (s). If the timer does not start, 0 is displayed. If preemption is not configured for a SEP segment, one of the two interfaces that complete neighbor negotiation last remains to be blocked even though a network fault is rectified. Consequently, the interface specified to be blocked is not blocked. To specify the parameter, run the **preempt** command.
Block Port Expected	Specified blocked interface. To specify the parameter, run the **block port** command.

Item	Description
Name of Port Member	Name of a member interface.
TC-Notify Propagate to	Object to which topology changes are reported. To specify the parameter, run the **tc-notify** command.

5.13.9 display sep topology

Function

The **display sep topology** command displays the topologies of SEP segments.

Format

display sep topology [**segment** *segment-id*] [**verbose**]

Parameters

Parameter	Description	Value
segment *segment-id*	Displays the topology of a specified SEP segment.	The value is an integer that ranges from 1 to 1024.
verbose	Displays detailed information about the topology of a SEP segment.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After SEP is configured, you can run the **display sep topology** command to view the topologies of SEP segments, including device names, names of the interfaces added to SEP segments, and roles of the interfaces in a SEP segment.

When running the **display sep topology** command:

- If no parameter is specified, this command displays brief information about the topologies of all the SEP segments on the device.
- If only **segment** *segment-id* is specified, this command displays brief information about the topology of a specified SEP segment.

- If only **verbose** is specified, this command displays detailed information about the topologies of all SEP segments on the device.
- If **segment** *segment-id* and **verbose** are specified, this command displays detailed information about the topology of a specified SEP segment on the device.

NOTE

Before running this command, complete the following tasks:

- Run the **sep segment** command in the system view to create a SEP segment.
- Run the **sep segment (interface view)** command in the Ethernet interface view to add an interface to the SEP segment and set the role of the interface as required.

  Edge interfaces must be configured in the SEP segment; otherwise, the SEP topology is incomplete and the system displays an error message.

Example

# Display the topologies of all SEP segments on the device.

```
<LSW1> display sep topology
SEP segment 1
SEP detects a segment failure that may be caused by an incomplete topology
-----------------------------------------------------------------------
System Name      Port Name          Port Role       Port Status     Hop
-----------------------------------------------------------------------
LSW1             GE0/0/1            *secondary      forwarding      1
LSW1             GE0/0/2            common          forwarding      2
LSW3             GE0/0/1            common          forwarding      3
LSW3             GE0/0/2            common          forwarding      4
LSW2             GE0/0/1            common          forwarding      5
LSW2             GE0/0/2            *secondary      discarding      6
```

# Display detailed topology information in SEP segment 1.

```
<LSW1> display sep topology segment 1 verbose
SEP segment 1
---------------------------------------------------------------
System Name     :LSW1
Port Name       :GE0/0/1
Port Role       :Config = primary / Active =  primary
PortID          :00e0-9e62-6100.0000
Port Priority   :64
Port Status     :forwarding
Link Status     :up
Neighbor Status :up
Age Time        :60(s)
Sequence Number :0x8000000e
Neighbor Port   :LSW2 - GE0/0/2 (00e0-8830-fe00.0000)
Brother Port    :LSW1 - GE0/0/3 (00e0-9e62-6100.0001)
```

Table 5-96 Description of the **display sep topology** command output

Item	Description
SEP segment	ID of a SEP segment. To specify the parameter, run the **sep segment** command.
System Name	Device name.
Port Name	Name of an interface added to the SEP segment.

Item	Description
Port Role	Role of an interface in the SEP segment: ● common: common interface ● primary: primary edge interface ● secondary: secondary edge interface ● *primary: no-neighbor primary edge interface ● *secondary: no-neighbor secondary edge interface Config: indicates the configured role of an interface in a SEP segment. Active: indicates the running role of an interface in a SEP segment. **NOTE** In normal situations, a SEP segment has a primary edge interface, a secondary edge interface, and common interfaces.
Port Status	Current status of an interface: ● discarding: The interface is blocked and can forward SEP packets but not data packets. ● forwarding: The interface is in Forwarding state and can forward both data packets and SEP packets.
PortID	Interface ID. It is in the format of 6-byte system MAC address +2-byte interface number.
Port Priority	Interface priority. It is an integer that ranges from 1 to 128. By default, the interface priority is 64. To specify the parameter, run the **sep segment priority** command.
Link Status	Link status: ● up: The link is Up. ● down: The link is Down.
Neighbor Status	Status of the neighbor state machine: ● up: Neighbor negotiations succeed and the protocol status of the interface is Up. ● down: Neighbor negotiations fail and no neighbor relationship is established between the local interface and its peer interface. ● init: The local interface receives packets from the peer interface and neighbor negotiations start. ● conflict: The local interface receives packets from multiple peer interfaces and the protocol status of the interface is Conflict.
Age Time	Aging time of the LSA.
Sequence Number	Sequence number of the LSA.

Item	Description
Neighbor Port	Neighbor interface. It is in the format of system name +interface name (system MAC address or interface ID). If there is no neighbor, the value is NULL.
Brother Port	Brother interface. It is in the format of system name +interface name (system MAC address or interface ID). If there is no brother, the value is NULL.

5.13.10 preempt (SEP segment view)

Function

The **preempt** command configures the blocked interface preemption mode on the device where the primary edge interface is located.

The **undo preempt delay** command cancels the configuration of delayed preemption on the primary edge interface.

By default, the SEP preemption mode is not configured.

Format

preempt { **manual** | **delay** *seconds* }

undo preempt delay

Parameters

Parameter	Description	Value
manual	Indicates the manual preemption mode.	-
delay	Indicates the delayed preemption mode.	-
seconds	Specifies the preemption delay. You can configure a preemption delay to prevent network flapping. When link faults are rectified, the specified interface waits until the delay timer expires, and then preempts to be the blocked interface.	The value is an integer that ranges from 15 to 600, in seconds.

Views

SEP segment view

Default Level

2: Configuration level

Usage Guidelines

In a SEP segment, some ports are blocked to prevent loops.

When a link in the SEP segment fails, the blocked interface in Up state changes to the Forwarding state after receiving a fault notification packet. If the preemption mode is not configured, when all link faults are rectified or the last two interfaces enabled with SEP complete neighbor negotiations, interfaces send blocking status packets to each other. The interface with the highest priority is then blocked, and the other interfaces enter the Forwarding state.

NOTE

The blocked interface is determined by the administrative priority and user-defined priority of each interface. The priority value of an interface contains 16 bits. The higher 8 bits are defined by the system, and the lower 8 bits are set by the user. The value of the lower 8 bits ranges from 1 to 128, and the default value is 64. The interface with the highest priority is blocked.

If the preemption mode is configured on the device where the primary edge interface is located, the specified interface transitions to the Blocking state and sends blocking status packets to other ports.

SEP supports the following preemption modes:

- Delayed preemption

  After all interface faults are rectified, the faulty interface does not send any fault notification packet. If the primary edge interface does not receive any fault notification packet within 3 seconds, it starts the delay timer. When the delay timer expires, the devices in the SEP segment initiate blocked interface preemption.

  NOTE

  You must set the preemption delay when delayed preemption is used because there is no default delay time.

  After delay preemption is configured, you can run the **undo preempt delay** command in the SEP segment view to delete the configuration of delay preemption.

- Manual preemption

  In this mode, if the link status databases of the primary and secondary edge interfaces are complete, the primary edge interface sends preemption packets to block the specified interface. Then the specified interface sends blocking status packets to request the original blocked interface to transition to the Forwarding state.

  NOTE

  - Manual preemption is a one-off operation and will not take effect again after the preemption is complete on the SEP segment. To change the blocked interface, run the **preempt** command and specify the **delay** parameter to configure delayed preemption.
  - Manual preemption causes a short link disconnection in the SEP segment.

Blocked interface preemption is triggered when the following conditions are met:

- The primary edge interface in the SEP segment is selected.

To configure interface roles, run the **sep segment** *segment-id* [**edge** [**no-neighbour**] { **primary** | **secondary** }] command in the interface view.

- The method of selecting the interface to block is configured on the device where the primary edge interface is located.

  To configure the method of selecting the interface to block, run the **block port** { **sysname** *sysname* **interface** *interface-type interface-number* | **hop** *hop-id* | **optimal** | **middle** } command in the SEP segment view.
- The topology of the SEP segment must be complete.

Example

# Configure the manual preemption mode on the device where the primary edge port is located.

```
<HUAWEI> system-view
[HUAWEI] sep segment 1
[HUAWEI-sep-segment1] preempt manual
```

# Configure the delayed preemption mode on the device where the primary edge port is located.

```
<HUAWEI> system-view
[HUAWEI] sep segment 1
[HUAWEI-sep-segment1] preempt delay 100
```

5.13.11 protected-instance

Function

The **protected-instance** command configures protected instances in a SEP segment.

The **undo protected-instance** command deletes the protected instances in a SEP segment.

By default, no protected instance is configured in a SEP segment.

Format

protected-instance { **all** | { *instance-id1* [**to** *instance-id2*] } &<1-10> }

undo protected-instance { **all** | { *instance-id1* [**to** *instance-id2*] } &<1-10> }

Parameters

Parameter	Description	Value
all	Indicates all protected instances in a SEP segment.	-

Parameter	Description	Value
instance-id1 [**to** *instance-id2*]	Specifies the IDs of protected instances in a SEP segment. The keyword **to** connecting two instance IDs, indicating an ID range from *instance-id1* to *instance-id2*. The value of *instance-id2* must be greater than the value of *instance-id1*. **&<1-10>** indicates that the parameter before the sign (&) can be repeated 1 to 10 times.	The value is an integer in the range 0 to 4094. Each device supports a maximum of 65 instances.

Views

SEP segment view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In common SEP networking, a physical ring can be configured with only one SEP segment in which only one interface can be blocked. If an interface in a complete SEP segment is blocked, all service data is transmitted only along the path where the primary edge interface is located. The path where the secondary edge interface is located remains idle, wasting bandwidth.

SEP multi-instance is used to improve bandwidth efficiency, allowing each physical interface on a ring network to be added to two SEP segments. A physical ring can be configured with two logical rings, allowing packets carrying different VLAN IDs to pass through. Load balancing is then implemented between the two logical rings. This implementation requires logical rings to be configured with different protected instances and mappings between protected instances and VLANs to be configured. The **protected-instance** command can be used to configure protected instances for a SEP segment.

Prerequisites

The protected instance IDs configured for SEP segments do not overlap. If different SEP segments have duplicate protected instance IDs, replan protected instance IDs.

Follow-up Procedure

Complete the following tasks to configure mappings between protected instances and VLANs:

1. Run the **stp region-configuration** command to enter the MST region view.

2. Run the **instance** *instance-id* **vlan** { *vlan-id1* [**to** *vlan-id2*] } &<1-10> command to configure mappings between protected instances and VLANs.

   The value of *instance-id* specified in this command must be the same as the value of *instance-id* specified in the **protected-instance** command.
3. Run the **active region-configuration** command to activate the configured mappings between protected instances and VLANs.

Precautions

If you run the **protected-instance** command multiple times in the same SEP segment, multiple instances are configured.

After the **protected-instance** command is run to configure different protected instances for SEP segments and mappings between protected instances and VLANs are set, topology changes affect only corresponding VLANs. This ensures reliable data transmission.

Before adding an interface to a SEP segment, ensure that the SEP segment has been configured with protected instances; otherwise, the interface cannot be added to the SEP segment.

Example

# Configure protected instances for SEP segment 1.

```
<HUAWEI> system-view
[HUAWEI] sep segment 1
[HUAWEI-sep-segment1] protected-instance all
```

5.13.12 reset sep error packet statistics

Function

The **reset sep error packet statistics** command clears the statistics of error sep packets.

Format

reset sep error packet statistics

Parameters

None

Views

All views

Default Level

3: Management level

Usage Guidelines

Applicable Scenario

You can use the **reset sep error packet statistics** command to clear the history statistics when you need to observe the statistics of error sep packets in a period from the current time.

Precautions

The **reset sep error packet statistics** command clears the statistics about error sep packets are cleared and cannot be restored. Therefore, confirm the action before you use the command.

Example

# Clear the statistics about error sep packets.

```
<HUAWEI> reset sep error packet statistics
```

5.13.13 reset sep interface statistics

Function

The **reset sep interface statistics** command clears SEP packet statistics on a specified interface in a SEP segment.

Format

reset sep interface *interface-type interface-number* **statistics**

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Clears SEP packet statistics on a specified interface in a SEP segment. *interface-type* specifies the type of the interface in a SEP segment. *interface-number* specifies the number of the interface in a SEP segment.	-

Views

All views

Default Level

3: Management level

Usage Guidelines

Before collecting SEP packet statistics on an interface within a certain period, clear existing traffic statistics on this interface. In such a situation, you can run the **reset sep interface statistics** command.

NOTE

- Before the **reset sep interface statistics** command is run, the SEP segment must be created and the interface must be added to the SEP segment.
- After the **reset sep interface statistics** command is run, SEP packet statistics on the specified interface in the SEP segment are cleared and cannot be restored. Confirm your action before you use this command.

Example

# Clear SEP packet statistics on GE 0/0/1 in the SEP segment.

```
<HUAWEI> reset sep interface gigabitethernet 0/0/1 statistics
```

5.13.14 sep segment

Function

The **sep segment** command creates a SEP segment and displays the SEP segment view. If the specified SEP segment has been created, you can directly enter the SEP segment view.

The **undo sep segment** command deletes the existing SEP segment.

Format

sep segment *segment-id*

undo sep segment *segment-id*

Parameters

Parameter	Description	Value
segment-id	Specifies the ID of a SEP segment.	The value is an integer that ranges from 1 to 1024.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

On a Layer 2 switching network, packets will be transmitted infinitely once a loop occurs, causing a broadcast storm. The broadcast storm occupies all the bandwidth on the network, causing network congestion or even breakdown of the entire network. To prevent loops on a Layer 2 switching network, Huawei develops the Smart Ethernet Protection (SEP) protocol.

SEP is a ring network protocol specially used for the Ethernet link layer. It blocks redundant links to prevent loops. It can run on a network together with STP, RSTP, MSTP, and RRPP and supports display of the network topology. When the devices of other vendors are used on the network, SEP can also prevent loops, but does not need to be configured on these devices.

A SEP segment consists of interconnected Layer 2 switching devices configured with the same SEP segment ID and control VLAN ID. A SEP segment is the basic unit for SEP.

The switches support a maximum of 48 SEP segments.

NOTE

A maximum of two interfaces on a Layer 2 switching device can be added to the same SEP segment.

Before enabling SEP, run the **sep segment** command to create a SEP segment. Then run the **control-vlan (SEP segment view)** command in the SEP segment view to configure a control VLAN.

A SEP segment can be deleted only when it does not contain any interface. If the SEP segment contains interfaces, run the **undo sep segment** *segment-id* command in the corresponding interface views to delete the interfaces from the SEP segment one by one.

Example

# Create SEP segment 1.

```
<HUAWEI> system-view
[HUAWEI] sep segment 1
[HUAWEI-sep-segment1]
```

5.13.15 sep segment (interface view)

Function

The **sep segment** command adds an Ethernet interface to a specified SEP segment and configures the role of the Ethernet interface.

The **undo sep segment** command removes an Ethernet interface from a specified SEP segment and deletes the interface role configuration.

By default, an Ethernet interface is not added to a specified SEP segment and is not configured with a role.

Format

sep segment *segment-id* [**edge** [**no-neighbor**] { **primary** | **secondary** }]

undo sep segment *segment-id*

Parameters

Parameter	Description	Value
segment-id	Specifies the ID of the SEP segment to which an Ethernet interface is added.	The value is an integer that ranges from 1 to 1024.
edge	Specifies the Ethernet interface added to the SEP segment as an edge interface.	-
no-neighbor	Specifies the Ethernet interface as a no-neighbor edge interface.	-
primary	Specifies the Ethernet interface as a primary edge interface.	-
secondary	Specifies the Ethernet interface as a secondary edge interface.	-

Views

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

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A Layer 2 interface can forward SEP packets only after being added to a SEP segment. Each Layer 2 switching device in a SEP segment is a node. Each node can have at most two Layer 2 interfaces added to the same SEP segment.

When using the **sep segment** command:

- If no parameter is specified, this command adds an Ethernet interface to a specified SEP segment and configures the interface as a common interface.

  In a SEP segment, all interfaces except edge interfaces and blocked interfaces are common interfaces.

  A common interface monitors the status of the directly-connected SEP link. When the link status changes, the interface sends a topology change notification message to notify its neighbors. Then the topology change notification message is flooded on the link until it finally reaches the primary edge interface. The primary edge interface determines how to process the link change.

- If **edge** and **primary** are specified, this command adds an Ethernet interface to the specified SEP segment and configures the interface as the primary edge interface.

  A SEP segment has only one primary edge interface, which is determined by the configuration and primary edge interface election. The primary edge interface initiates blocked interface preemption, terminates packets, and sends topology change notification messages to other networks.
- If **edge** and **secondary** are specified, this command adds an Ethernet interface to the specified SEP segment and configures the interface as the secondary edge interface.

  A SEP segment has only one secondary edge interface, which is determined by the configuration and secondary edge interface election. The secondary edge interface terminates packets and sends topology change notification messages to other networks.
- If **edge**, **no-neighbor**, and **primary** are specified, this command adds an Ethernet interface to the specified SEP segment and configures the interface as the no-neighbor primary edge interface.

  An interface at the edge of a SEP segment is a no-neighbor edge interface. There are two types of no-neighbor edge interface: no-neighbor primary edge interface and no-neighbor secondary edge interface. You can configure the role of a no-neighbor edge interface. A no-neighbor edge interface terminates packets and sends topology change notification messages to other networks. It is commonly used to interconnect Huawei devices and non-Huawei devices or interconnect Huawei devices and devices that do not support SEP.
- If **edge**, **no-neighbor**, and **secondary** are specified, this command adds an Ethernet interface to the specified SEP segment and configures the interface as the no-neighbor secondary edge interface.

To view the role of an interface added to a SEP segment, run the **display sep topology** or **display sep interface** command.

Precautions

- You have created a SEP segment and configured a control VLAN and protected instances.
- To add an interface to a SEP segment, configure the interface as a hybrid or trunk interface.
- If **no-neighbor** is not specified, the interface to be added to the SEP segment is not an STP or RRPP interface.
- Two interfaces at the edge of a SEP segment must be configured as edge interfaces. The roles of the interfaces are defined by users.
- All the interfaces on the network are Up so that the SEP segment is complete and the displayed topology information is correct.

Example

# Add GE 0/0/1 to SEP segment 1 and configure the interface as the no-neighbor secondary edge interface.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] port link-type hybrid
```

```
[HUAWEI-GigabitEthernet0/0/1] sep segment 1 edge no-neighbor secondary
```

5.13.16 sep segment priority

Function

The **sep segment priority** command configures the priority of an Ethernet interface in a specified SEP segment.

The **undo sep segment priority** command restores the default priority of an Ethernet interface in a specified SEP segment.

By default, the priority of an Ethernet interface in a specified SEP segment is 64.

Format

sep segment *segment-id* **priority** *priority*

undo sep segment *segment-id* **priority**

Parameters

Parameter	Description	Value
segment-id	Specifies the ID of the SEP segment to which an Ethernet interface is added.	The value is an integer that ranges from 1 to 1024.
priority	Specifies the priority of an Ethernet interface in a specified SEP segment. A larger value indicates a higher priority. When the link fault is rectified, the interface with the highest priority is likely to become the blocked interface.	The value is an integer that ranges from 1 to 128. The default value is 64.

Views

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

Default Level

2: Configuration level

Usage Guidelines

In a SEP segment, some interfaces are blocked to prevent loops. Any interface in a SEP segment may be blocked if no interface is specified for blocking. A complete SEP segment contains only one blocked interface.

If you run the **block port optimal** command to select the blocked interface according to the port priority, the interface priority set using the **sep segment**

priority command determines whether the interface will be blocked when an interface fault is rectified.

The blocked interface is determined by the administrative priority and user-defined priority of each interface. The priority value of an interface contains 16 bits. The higher 8 bits are defined by the system, and the lower 8 bits are set by the user. A higher interface priority indicates a higher probability that the interface is blocked.

SEP compares interface priorities as follows:

1. Compares configured interface priority values. A larger value indicates a higher priority.
2. Compares bridge MAC addresses of interfaces with same priority values. A smaller bridge MAC address indicates a higher priority.
3. Compares interface numbers of interfaces with identical bridge MAC addresses. A smaller interface number indicates a higher priority.

Before using the **sep segment priority** command, ensure that the interface is added to the specified SEP segment using the **sep segment** (interface view) command.

Example

# Set the priority of GE 0/0/1 added to SEP segment 1 to 10.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] port link-type hybrid
[HUAWEI-GigabitEthernet0/0/1] sep segment 1
[HUAWEI-GigabitEthernet0/0/1] sep segment 1 priority 10
```

5.13.17 tc-notify

Function

The **tc-notify** command configures a SEP segment to report topology changes to other SEP segments or networks running other ring network protocols.

The **undo tc-notify** command disables a SEP segment from reporting topology changes to other SEP segments or networks running other ring network protocols.

By default, a SEP segment does not send topology change notifications.

Format

tc-notify { **segment** { *segment-id1* [**to** *segment-id2*] } &<1-10> | **stp** | **rrpp** | **smart-link send-packet vlan** *vlan-id* | **vpls** }

undo tc-notify { **segment** { *segment-id1* [**to** *segment-id2*] } &<1-10> | **stp** | **rrpp** | **smart-link send-packet vlan** | **vpls** }

NOTE

Only S5731-S, S5731-H, S5731S-H, S5732-H, S6720-EI, S6720S-EI, S6730-S, S6730S-H, and S6730-H support **vpls** parameter.

Parameters

Parameter	Description	Value
segment *segment-id1* [**to** *segment-id2*]	Specifies the SEP segments to which topology changes of the local SEP segment need to be reported. Topology changes of the local SEP segment are reported to other SEP segments, but not the local SEP segment. The keyword **to** connecting two instance IDs, indicating an ID range from *instance-id1* to *instance-id2*. The value of *instance-id2* must be greater than the value of *instance-id1*.	The value is an integer that ranges from 1 to 1024.
stp	Indicates that the local SEP segment reports topology changes to STP networks.	-
rrpp	Indicates that the local SEP segment reports topology changes to RRPP networks.	-
smart-link	Indicates that the local SEP segment reports topology changes to an upper-layer network using SmartLink Flush packets. When the local SEP segment is connected to an upper-layer network through a no-neighbor edge interface, this parameter must be specified in the **tc-notify** command.	-
send-packet vlan *vlan-id*	Specifies the ID of a VLAN used to transmit SmartLink Flush packets.	The value is an integer that ranges from 1 to 4094.
vpls	Indicates that the local SEP segment reports topology changes to VPLS networks.	-

Views

SEP segment view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If topology changes in a SEP segment are not reported to the upper-layer Layer 2 network in time, devices on the upper-layer network retain the original MAC address entries, causing traffic interruption. To ensure uninterrupted traffic transmission, run the **tc-notify** command to configure the local SEP segment to report topology changes to other SEP segments or networks running other ring network protocols.

Prerequisites

The **sep segment** command has been used to create SEP segments.

Precautions

When the topology of a SEP segment changes, the SEP segment sends topology change notification messages to other SEP segments or networks running other ring network protocols. If the specified segment or network does not exist, the **tc-notify** command configuration does not take effect.

After receiving topology change notification messages from a SEP segment, devices on the upper layer network send Flush FDB packets on the network. Then, all the devices on the upper-layer network delete the original MAC addresses and learn new MAC addresses to ensure normal traffic transmission.

The **tc-notify** command is used on the device connecting a lower-layer network and an upper-layer network.

Example

# Configure SEP segment 1 to report topology changes to SEP segments 10 to 20.

```
<HUAWEI> system-view
[HUAWEI] sep segment 1
[HUAWEI-sep-segment1] tc-notify segment 10 to 20
```

# Configure SEP segment 1 to report topology changes to STP networks.

```
<HUAWEI> system-view
[HUAWEI] sep segment 1
[HUAWEI-sep-segment1] tc-notify stp
```

# Configure SEP segment 1 to report topology changes to RRPP networks.

```
<HUAWEI> system-view
[HUAWEI] sep segment 1
[HUAWEI-sep-segment1] tc-notify rrpp
```

# Configure SEP segment 1 to report topology changes to upper-layer networks using SmartLink Flush packets.

```
<HUAWEI> system-view
[HUAWEI] sep segment 1
[HUAWEI-sep-segment1] tc-notify smart-link send-packet vlan 3
```

# Configure SEP segment 1 to report topology changes to VPLS networks.

```
<HUAWEI> system-view
[HUAWEI] sep segment 1
[HUAWEI-sep-segment1] tc-notify vpls
```

5.13.18 tc-protection interval

Function

The **tc-protection interval** command sets the interval for suppressing topology change (TC) notification packets.

The **undo tc-protection interval** command restores the default interval for suppressing TC notification packets.

By default, the interval for suppressing TC notification packets is 2s.

Format

tc-protection interval *interval-value*

undo tc-protection interval

Parameters

Parameter	Description	Value
interval-value	Specifies the interval for suppressing TC notification packets. A longer interval ensures stable SEP operating but deteriorates convergence performance.	The value is an integer that ranges from 1 to 10, in seconds.

Views

SEP segment view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Assume that a host is connected to an upstream network through three or more SEP networks. If the topology of the SEP network nearest to the host changes, doubled TC notification packets are flooded on the upper-layer SEP network. Each time TC notification packets pass through a SEP segment, TC notification packets will be doubled. The upstream network will receive multiple duplicate TC notification packets.

Frequent topology change notifications reduce the CPU packet processing capability, and cause devices in the SEP segments to frequently refresh MAC address entries, which consumes bandwidth resources. To address the problem, run the **tc-protection interval** command to suppress TC notification packets.

Prerequisites

The **sep segment** command has been used to create SEP segments.

Precautions

After this command is used, the upstream network only needs to process one TC notification packet but not multiple duplicate TC notification packets. In addition, this function protects devices on the SEP segment against TC attacks.

Example

# Set the interval for suppressing TC notification packets to 3s in SEP segment 1.

```
<HUAWEI> system-view
[HUAWEI] sep segment 1
[HUAWEI-sep-segment1] tc-protection interval 3
```

5.14 RRPP Configuration Commands

5.14.1 Command Support

All models of S300, S500, S2700, S5700, and S6700 series switches (except the S5731-L and S5731S-L) support RRPP.

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

5.14.2 control-vlan

Function

The **control-vlan** command configures the control VLAN in an RRPP domain.

The **undo control-vlan** command deletes the configured control VLAN.

By default, no control VLAN is configured in an RRPP domain.

Format

control-vlan *vlan-id*

undo control-vlan

Parameters

Parameter	Description	Value
vlan-id	Specifies the control VLAN ID in an RRPP domain. The VLAN must be a VLAN that has not been created.	The value is an integer that ranges from 1 to 4093. **NOTE** VLAN 1 is the default VLAN and cannot be configured as the control VLAN.

Views

RRPP domain view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A VLAN that transmits RRPP packets in an RRPP domain is called a control VLAN.

An RRPP domain is configured with two control VLANs, that is, the major control VLAN and sub-control VLAN. You need to specify only the major control VLAN. The VLAN whose ID is one greater than the ID of the major control VLAN becomes the sub-control VLAN.

Precautions

- The control VLAN must be included in the protected VLANs; otherwise, the RRPP ring cannot be configured.
- The control VLAN specified by *vlan-id* must be a VLAN that has not been created, and not been used by other features. The sub-control VLAN specified by *vlan-id* plus one must be a VLAN that has not been created, and not been used by other features.
- The control VLAN is deleted when the RRPP domain is deleted using the **undo rrpp domain** command.

Example

# Set the control VLAN ID in RRPP Domain 1 to 100.

```
<HUAWEI> system-view
[HUAWEI] rrpp domain 1
[HUAWEI-rrpp-domain-region1] control-vlan 100
```

5.14.3 description (RRPP domain view)

Function

The **description** command configures the description of the RRPP domain.

The **undo description** command restores the default setting.

By default, the description of an RRPP domain is null.

Format

description *text*

undo description

Parameters

Parameter	Description	Value
text	Specifies the description of an RRPP domain.	The value is a string of 1 to 255 case-sensitive characters.

Views

RRPP domain view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On a device running RRPP, you can run the **description** command to configure the description of the RRPP domain, such as the RRPP domain ID. Configuring the description of an RRPP domain facilitates the maintenance of the RRPP domain.

Precautions

After being configured in the RRPP domain view, the description command takes effect only on the local device.

Example

# Configure the description **It's RRPP Domain 10** for RRPP domain 10.

```
<HUAWEI> system-view
[HUAWEI] rrpp domain 10
[HUAWEI-rrpp-domain-region10] description It's RRPP Domain 10
```

5.14.4 display rrpp brief

Function

The **display rrpp brief** command displays summary information about all RRPP domains configured on the device.

Format

display rrpp brief [**domain** *domain-id*]

Parameters

Parameter	Description	Value
domain *domain-id*	Displays summary information about a specified RRPP domain. If this parameter is not specified, the command displays summary information about all RRPP domains.	The value is an integer that ranges from 1 to 64.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

You can run the **display rrpp brief** command on the RRPP-enabled device to view summary information about RRPP domains configured on the device. The command output shows whether RRPP is enabled, the configuration of RRPP domains, and information about the configured rings in the RRPP domains.

Example

# Display summary information about RRPP.

```
<HUAWEI> display rrpp brief
Abbreviations for Switch Node Mode :
M - Master , T - Transit , E - Edge , A - Assistant-Edge

RRPP Protocol Status: Disable
RRPP Working Mode: HW
RRPP Linkup Delay Timer: 1 sec (0 sec default)
Number of RRPP Domains: 1

Domain Index   : 1
Control VLAN   : major 30    sub 31
Protected VLAN : Reference Instance 10
Hello Timer    : 1 sec(default is 1 sec)  Fail Timer : 6 sec(default is 6 sec)

 Ring   Ring    Node     Primary/Common            Secondary/Edge       Is
 ID     Level   Mode     Port                      Port                 Enabled
 ------------------------------------------------------------------------------
 1      0       M        GigabitEthernet0/0/2      GigabitEthernet0/0/3       No
```

# Display summary information about RRPP Domain 1.

```
<HUAWEI> display rrpp brief domain 1
Abbreviations for Switch Node Mode :
M - Master , T - Transit , E - Edge , A - Assistant-Edge
```

```
RRPP Protocol Status: Disable
RRPP Working Mode: HW
RRPP Linkup Delay Timer: 1 sec (0 sec default)
Number of RRPP Domains: 1

Domain Index   : 1
Control VLAN   : major 30    sub 31
Protected VLAN : Reference Instance 10
Hello Timer    : 1 sec(default is 1 sec)  Fail Timer : 6 sec(default is 6 sec)

 Ring   Ring    Node     Primary/Common           Secondary/Edge       Is
 ID     Level   Mode     Port                     Port                 Enabled
 ----------------------------------------------------------------------------
 1      0       M        GigabitEthernet0/0/2     GigabitEthernet0/0/3    No
```

Table 5-97 Description of the display rrpp brief command output

Item	Description
Abbreviations for Switch Node Mode	Abbreviations of node modes. The value can be: ● M-Master: indicates the master node. ● T-Transit: indicates the transit node. ● E-Edge: indicates the edge node. ● A-Assistant-Edge: indicates the assistant edge node.
RRPP Protocol Status	Status of RRPP. ● Enable: indicates that RRPP is enabled. ● Disable: indicates that RRPP is disabled. To enable RRPP, run the **rrpp enable** command.
Number of RRPP Domains	Number of RRPP domains configured.
Domain Index	ID of the RRPP domain. To specify the parameter, run the **rrpp domain** command.
RRPP Working Mode	RRPP working mode: ● GB: indicates RRPP defined by the national standard of China. ● HW: indicates RRPP defined by Huawei.
RRPP Linkup Delay Timer	Delay time before the master node becomes Complete. To set the delay time before the master node becomes Complete, run the **rrpp linkup-delay-timer** command.
Control VLAN : major 30 sub 31	Control VLAN IDs of the RRPP domain. **major** indicates the master control VLAN and **sub** indicates the sub-control VLAN. To specify the parameter, run the **control-vlan** command.

Item	Description
Protected VLAN	ID of the instance bound to the protected VLAN in the RRPP domain. To specify the parameter, run the **protected-vlan** command.
Hello Timer	Hello timer in the RRPP domain, in seconds. To set the value of the Hello timer, run the **timer (RRPP domain view)** command.
Fail Timer	Fail timer in the RRPP domain, in seconds. To set the value of the Fail timer, run the **timer (RRPP domain view)** command.
Ring ID	ID of the RRPP ring. To specify the parameter, run the **ring node-mode** command.
Ring Level	Level of the RRPP ring. ● Level 0 indicates the major ring. ● Level 1 indicates the sub-ring. To specify the parameter, run the **ring node-mode** command.
Node Mode	Mode of a node. For modes of a node, see the preceding item **Abbreviations for Switch Node Mode**. To specify the parameter, run the **ring node-mode** command.
Primary/Common Port	Primary interface or common interface on the master node or transit node of an RRPP ring. To specify the parameter, run the **ring node-mode** command.
Secondary/Edge Port	Secondary interface or edge interface on the master node or transit node of an RRPP ring. To specify the parameter, run the **ring node-mode** command.
Is Enabled	Whether a ring is enabled. To enable a ring, run the **ring enable** command.

5.14.5 display rrpp error packet

Function

The **display rrpp error packet** command displays statistics about recently-received RRPP error packets.

Format

display rrpp error packet

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

When a device receives RRPP attack packets on a network, you can run the **display rrpp error packet** command to collect statistics about recently-received RRPP error packets to locate the problem.

Example

# Display statistics about recently-received RRPP error packets.

```
<HUAWEI> display rrpp error packet
4 error-packets have been received and the last

one is received at 2010/01/02 12:45:31 UTC+00:00 :


00 0f e2 07 82 17 00 18 82 99 fc 22 81 00 e0 01
00 48 aa aa 03 00 e0 2b 00 bb 99 0b 00 40 01 05

00 01 00 01 00 00 00 18 82 99 fc 22 00 01 00 03

00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

00 00 00 00 00.
```

5.14.6 display rrpp ring-group

Function

The **display rrpp ring-group** command displays the configuration about an RRPP ring group.

Format

display rrpp ring-group [*ring-group-id*]

Parameters

Parameter	Description	Value
ring-group *ring-group-id*	Specifies the ID of an RRPP ring group. If this parameter is not specified, configurations about all the RRPP ring groups are displayed.	The value is an integer that ranges from 1 to 16.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

You can run the **display rrpp ring-group** command on an RRPP-enabled device to view configurations about RRPP ring groups and learn their running status.

Precautions

If the RRPP-enabled device is an edge node, the ring that sends Edge-Hello packets is displayed.

If the RRPP-enabled device is an assistant edge node, the ring that receives Edge-Hello packets is displayed.

Example

# Display configurations about all ring groups.

```
<HUAWEI> display rrpp ring-group
 Ring Group 1:
 domain 1 ring 1 to 3, 5
 domain 2 ring 1 to 3, 5
 domain 1 ring 1 send Edge-Hello packet

 Ring Group 2:
 domain 1 ring 4, 6 to 7
 domain 2 ring 4, 6 to 7
```

# Check the configuration about Ring Group 2.

```
<HUAWEI> display rrpp ring-group 2
 Ring Group 2:
 domain 1 ring 4, 6 to 7
 domain 2 ring 4, 6 to 7
```

Table 5-98 Description of the display rrpp ring-group command output

Item	Description
Ring Group	ID of the RRPP ring group. To specify the parameter, run the **rrpp ring-group** command.
domain xx ring xx	Sub-rings in the ring group. To specify sub-rings in a ring group, run the **domain** command.
domain xx ring xx send Edge-Hello packet	Sub-ring that sends Edge Hello packets in the RRPP ring group.

5.14.7 display rrpp snooping enable

Function

The **display rrpp snooping enable** command displays information about an interface where RRPP snooping is enabled.

NOTE

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

Format

display rrpp snooping enable { **all** | **interface vlanif** *interface-number* }

display rrpp snooping enable { **all** | **interface** *interface-type interface-number* [*.subinterface-number*] }

Parameters

Parameter	Description	Value
all	Displays information about all interfaces where RRPP snooping is enabled.	-
interface vlanif *interface-number*	Displays information about a VLANIF interface where RRPP snooping is enabled. *interface-number* specifies the number of the VLANIF interface.	-

Parameter	Description	Value
interface *interface-type* *interface-number* [*.subinterface-number*]	Displays information about an interface where RRPP snooping is enabled. *interface-type* specifies the type of the interface, *interface-number* specifies the number of the interface, and *subinterface-number* specifies the number of the sub-interface.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

You can use the **display rrpp snooping enable** command to view information about interfaces where RRPP snooping is enabled.

Example

# Display information about all interfaces where RRPP snooping is enabled.

```
<HUAWEI> display rrpp snooping enable all
 Port                          VsiName          Vlan
-------------------------------------------------------
 Vlanif100                       name1           100
 Vlanif200                       name2           200
```

# Display information about interfaces where RRPP snooping is enabled.

```
<HUAWEI> display rrpp snooping enable interface vlanif 100
 Port                          VsiName          Vlan
-------------------------------------------------------
 Vlanif100                       name1           100
```

Table 5-99 Description of the display rrpp snooping enable command output

Item	Description
Port	Name of the interface where RRPP snooping is enabled. To specify the parameter, run the **rrpp snooping enable** command.
VsiName	Name of the VSI that is bound to the interface. To specify the parameter, run the **rrpp snooping vsi** command.
Vlan	VLAN that is associated with the interface. It refers to the control VLAN of the RRPP ring.

5.14.8 display rrpp snooping vsi

Function

The **display rrpp snooping vsi** command displays the VSI that is associated with RRPP snooping.

NOTE

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

Format

display rrpp snooping vsi { **all** | **interface vlanif** *interface-number* }

display rrpp snooping vsi { **all** | **interface** *interface-type interface-number* [*.subinterface-number*] }

Parameters

Parameter	Description	Value
all	Displays all VSIs that are associated with RRPP snooping.	-
interface vlanif *interface-number*	Displays the VSI associated with RRPP snooping on the specified VLANIF interface. *interface-number* specifies the VLANIF interface number.	-

Parameter	Description	Value
interface *interface-type* *interface-number* [*.subinterface-number*]	Displays the VSI associated with RRPP snooping on the specified interface. *interface-type* specifies the type of the interface, *interface-number* specifies the number of the interface, *subinterface-number* specifies the number of the sub-interface.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

You can run this command on an RRPP snooping-enabled device to view VSIs that are associated with RRPP snooping.

Example

# Display VSIs associated with RRPP snooping on all interfaces.

```
<HUAWEI> display rrpp snooping vsi all
 Port                          VsiName
----------------------------------------------
 Vlanif100                       name1
 Vlanif100                       name2
 Vlanif200                       name1
 Vlanif200                       name2
```

# Display the VSI associated with RRPP snooping on the specified interface.

```
<HUAWEI> display rrpp snooping vsi interface vlanif 100
 Port                          VsiName
----------------------------------------------
 Vlanif100                       name1
 Vlanif100                       name2
```

Table 5-100 Description of the display rrpp snooping vsi command output

Item	Description
Port	Name of the interface that is bound to a VSI. To specify the parameter, run the **rrpp snooping enable** command.
VsiName	Name of the VSI that is associated with the interface. To specify the parameter, run the **rrpp snooping vsi** command.

5.14.9 display rrpp statistics

Function

The **display rrpp statistics** command displays statistics on RRPP packets.

Format

display rrpp statistics domain *domain-id* [**ring** *ring-id*]

Parameters

Parameter	Description	Value
domain *domain-id*	Specifies the ID of an RRPP domain.	The value is an integer that ranges from 1 to 64.
ring *ring-id*	Specifies the ID of an RRPP ring. If *ring-id* is not specified, statistics on packets of all the rings in a specified RRPP domain are displayed.	The value is an integer that ranges from 1 to 64.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

You can run this command to view statistics on RRPP packets on each interface to locate network faults.

Example

# Display the statistics on packets on RRPP Ring 1 in Domain 1.

```
<HUAWEI> display rrpp statistics domain 1 ring 1
RRPP Ring     : 1
Ring Level    : 0
Node Mode     : Master
Is Active     : Yes
Primary port  : GigabitEthernet0/0/1
 Packet         LINK    COMMON    COMPLETE    EDGE    MAJOR    Packet
 Direct  HEALTH  DOWN     FDB      FDB        HELLO   FAULT    Total
 ------------------------------------------------------------------------------
 Send    386     0       0         0           0        0        386
 Rcv     0       0       0         0           0        0        0
Secondary port: GigabitEthernet0/0/2
 Packet         LINK    COMMON    COMPLETE    EDGE    MAJOR    Packet
 Direct  HEALTH  DOWN     FDB      FDB        HELLO   FAULT    Total
 ------------------------------------------------------------------------------
 Send    0       0       0         0           0        0        0
 Rcv     0       0       0         0           0        0        0
```

# Display the statistics on packets on all RRPP rings in Domain 3.

```
<HUAWEI> display rrpp statistics domain 3
RRPP Ring     : 3
Ring Level    : 0
Node Mode     : Transit
Is Active     : Yes
Primary port  : GigabitEthernet0/0/1
 Packet         LINK    COMMON    COMPLETE    EDGE    MAJOR    Packet
 Direct  HEALTH  DOWN     FDB      FDB        HELLO   FAULT    Total
 ------------------------------------------------------------------------------
 Send    0       0       0         0           0        0        0
 Rcv     0       0       0         0           0        0        0
Secondary port: GigabitEthernet0/0/2
 Packet         LINK    COMMON    COMPLETE    EDGE    MAJOR    Packet
 Direct  HEALTH  DOWN     FDB      FDB        HELLO   FAULT    Total
 ------------------------------------------------------------------------------
 Send    0       0       0         0           0        0        0
 Rcv     0       0       0         0           0        0        0
RRPP Ring     : 4
Ring Level    : 1
Node Mode     : Assistant-edge
Is Active     : Yes
Common port   : GigabitEthernet0/0/3
 Packet         LINK    COMMON    COMPLETE    EDGE    MAJOR    Packet
 Direct  HEALTH  DOWN     FDB      FDB        HELLO   FAULT    Total
 ------------------------------------------------------------------------------
 Send    0       0       0         0           0        0        0
 Rcv     0       0       0         0           0        0        0
Edge port     : GigabitEthernet0/0/4
 Packet         LINK    COMMON    COMPLETE    EDGE    MAJOR    Packet
 Direct  HEALTH  DOWN     FDB      FDB        HELLO   FAULT    Total
 ------------------------------------------------------------------------------
 Send    0       0       0         0           0        0        0
 Rcv     0       0       0         0           0        0        0
```

Table 5-101 Description of the display rrpp statistics command output

Item	Description
RRPP Ring	ID of the RRPP ring.

Item	Description
Ring Level	Level of the RRPP ring. ● Level 0 indicates the major ring. ● Level 1 indicates the sub-ring.
Node Mode	Mode of a node on the RRPP ring. ● Master: indicates the master node. ● Transit: indicates the transit node. ● Edge: indicates the edge node. ● Assistant Edge: indicates the assistant edge node that is supported by RRPP defined by Huawei.
Is Active	Whether the RRPP ring is activated. The RRPP ring can be activated only when RRPP and the RRPP ring are enabled. To activate an RRPP ring, run the **rrpp enable** and **ring enable** commands.
Primary port	Primary interface on the RRPP ring.
Secondary port	Secondary interface on the RRPP ring.
Common port	Common interface on the edge node or assistant edge node of the RRPP sub-ring.
Edge port	Edge interface on the edge node or assistant edge node of the RRPP sub-ring.
Packet Direct	Direction of RRPP packets. ● Send: indicates the packets sent from the interface. ● Rcv: indicates the packets received by the interface.
HEALTH	Number of Hello packets sent by the master node to check the loop integrity.
LINK DOWN	Number of LinkDown packets. LinkDown packets are sent by the transit node, edge node, or assistant edge node to notify the master node that the status of the link on the ring becomes Down and the physical ring does not exist. Only statistics on received packets are collected on the master node and statistics on sent packets are collected on other nodes.
COMMON FDB	Number of common FDB packets used to refresh the FDB. Common FDB packets are sent from the master node to request the transit node, edge node, and assistant edge node to update their MAC address forwarding entries and ARP entries. Only statistics on sent packets are collected on the master node and statistics on received packets are collected on other nodes.

Item	Description
COMPLETE FDB	Number of Complete FDB packets used to update the FDB after the ring network recovers. Complete FDB packets are sent from the master node to request the transit node, edge node, and assistant edge node to update their MAC address forwarding entries and ARP entries. These packets are also used to request the transit node to unblock the temporarily blocked interfaces. Only statistics on sent packets are collected on the master node and statistics on received packets are collected on other nodes.
EDGE HELLO	Number of Edge-Hello packets used to check the integrity of the major ring. Edge-Hello packets are sent from the edge node of the sub-ring to the assistant edge node of the same sub-ring. The sub-ring checks the integrity of the major ring in the same domain through the Edge-Hello packets. Only statistics on sent packets are collected on the edge node and statistics on received packets are collected on the assistant edge node.
MAJOR FAULT	Number of Major-Fault packets used to notify faults on the major ring. Major-Fault packets are sent by the assistant edge interface on a sub-ring. If the assistant edge node does not receive the Edge-Hello packet from the edge interface within a specified period, the assistant edge node sends the Major-Fault packet to the edge interface to notify that the packets cannot be transparently transmitted on the major ring. Only statistics on received packets are collected on the edge node and statistics on sent packets are collected on the assistant edge node.
Packet Total	Total number of sent or received packets.

5.14.10 display rrpp verbose

Function

The **display rrpp verbose** command displays detailed configuration about RRPP on the device.

Format

display rrpp verbose [**domain** *domain-id* [**ring** *ring-id*]]

Parameters

Parameter	Description	Value
domain *domain-id*	Specifies the ID of an RRPP domain.	The value is an integer that ranges from 1 to 64.
ring *ring-id*	Specifies the ID of an RRPP ring. If this parameter is not specified, detailed configurations about all the rings in a specified domain is displayed.	The value is an integer that ranges from 1 to 64.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

You can run this command to check detailed configuration about RRPP. The command output helps you analyze the link status of the network and locate network faults.

Example

# Display detailed configuration about the master node on Ring 1 in RRPP Domain 1.

```
<HUAWEI> display rrpp verbose domain 1 ring 1
Domain Index   : 1
Control VLAN   : major 400    sub 401
Protected VLAN : Reference Instance 30
Hello Timer    : 1 sec(default is 1 sec)  Fail Timer : 6 sec(default is 6 sec)
RRPP Ring      : 1
Ring Level     : 0
Node Mode      : Master
Ring State     : Complete
Is Enabled     : Enable                   Is Active : Yes
Primary port   : GigabitEthernet0/0/1               Port status: UP
Secondary port : GigabitEthernet0/0/2               Port status: BLOCKED
```

Table 5-102 Description of the display rrpp verbose command output

Item	Description
Domain Index	ID of the RRPP domain. To specify the parameter, run the **rrpp domain** command.
Control VLAN : major 400 sub 401	Control VLAN IDs of the RRPP domain. **major** indicates the master control VLAN and **sub** indicates the sub-control VLAN. To specify the parameter, run the **control-vlan** command.
Protected VLAN	Instance mapping the protected VLANs of the RRPP domain. To specify the parameter, run the **protected-vlan** command.
Hello Timer	Value of the Hello timer, in seconds. To set the value of the Hello timer, run the **timer (RRPP domain view)** command.
Fail Timer	Value of the Fail timer, in seconds. To set the value of the Fail timer, run the **timer (RRPP domain view)** command.
RRPP Ring	ID of the RRPP ring. To specify the parameter, run the **ring node-mode** command.
Ring Level	Level of the RRPP ring. ● Level 0 indicates the major ring. ● Level 1 indicates the sub-ring. To specify the parameter, run the **ring node-mode** command.
Node Mode	Role of a node on the RRPP ring. The value can be: ● Master: indicates the master node. ● Transit: indicates the transit node. ● Edge: indicates the edge node. ● Assistant Edge: indicates the assistant edge node. To specify the parameter, run the **ring node-mode** command.

Item	Description
Ring State	Status of the RRPP ring. The value can be: ● Complete: indicates that the ring is complete. Only the master node can be in Complete state. ● Failed: indicates that the ring fails. Only the master node can be in Failed state. ● Unknown: indicates that the status of the ring is unknown. The Unknown state occurs when RRPP or the RRPP ring is enabled. ● LinkUp: indicates that the link is Up. Only transit nodes can be in LinkUp state. ● LinkDown: indicates that the link is Down. Only transit nodes can be in LinkDown state. ● Preforwarding: indicates that the link is in Preforwarding state. Only transit nodes can be in Preforwarding state.
Is Enabled	Whether the ring is enabled. To enable a ring, run the **ring enable** command.
Is Active	Whether the RRPP ring is activated. The RRPP ring can be activated only when RRPP and the RRPP ring are enabled. To activate an RRPP ring, run the **rrpp enable** and **ring enable** commands.
Primary port	Primary interface on the RRPP ring. To specify the parameter, run the **ring node-mode** command.
Secondary port	Secondary interface on the RRPP ring. To specify the parameter, run the **ring node-mode** command.
Port status	Status of an interface on the RRPP ring. The value can be: ● UNKNOWN: indicates that the device is not properly installed in a stack. ● UP: indicates that the interface is in Up state and can forward packets. ● DOWN: indicates that the interface is not connected. ● BLOCKED: indicates that the interface is in Up state but cannot forward packets.

5.14.11 domain (RRPP ring group view)

Function

The **domain** command adds sub-rings to an RRPP ring group.

The **undo domain** command deletes the sub-rings from the RRPP ring group.

Format

domain *domain-id* **ring** { *ring-id1* [**to** *ring-id2*] } &<1-10>

undo domain *domain-id* **ring** { *ring-id1* [**to** *ring-id2*] } &<1-10>

Parameters

Parameter	Description	Value
domain-id	Specifies the ID of an RRPP domain.	The value is an integer that ranges from 1 to 64.
ring *ring-id1* **to** *ring-id2*	Specifies the ID of an RRPP sub-ring. ● *ring-id1* specifies the first sub-ring ID. ● **to** *ring-id2* specifies the last sub-ring ID. The value of *ring-id2* must be larger than the value of *ring-id1*. *ring-id1* and *ring-id2* identify a range of instances. If **to** *ring-id2* is not specified, only *ring-id1* is specified.	The value is an integer that ranges from 1 to 64.

Views

RRPP ring group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If multiple RRPP rings exist, you can add sub-rings to the ring group to reduce the number of Edge-Hello packets, improving system performance.

Precautions

A maximum of 15 sub-rings can be added to a ring group.

If the **domain** command is run more than once, all configurations take effect.

- Only an edge node or an assistant edge node on a sub-ring can be added to a ring group. The edge nodes on the sub-rings are configured on the same device. Similarly, the assistant edge nodes are on the same device.
- A sub-ring can belong to only one ring group.
- All the sub-rings in a ring group must be on the same type of nodes, that is, edge nodes or assistant edge nodes.
- To add an activated sub-ring to a ring group, add the sub-ring to the ring group on the assistant edge node, and then perform the same operation on the edge node.

- To delete an activated sub-ring from a ring group, delete the sub-ring from the ring group on the edge node, and then perform the same operation on the assistant edge node.
- All the sub-rings in a ring group must have the same primary ring link; otherwise, the ring group cannot work properly.
- The configuration and activation status of a ring group must be the same on the edge node and assistant edge node.

Example

# Add sub-rings to Ring Group 1.

```
<HUAWEI> system-view
[HUAWEI] rrpp ring-group 1
[HUAWEI-rrpp-ring-group1] domain 1 ring 1 to 3 5
```

5.14.12 protected-vlan

Function

The **protected-vlan** command configures a list of protected VLANs in an RRPP domain.

The **undo protected-vlan** command deletes the list of protected VLANs in an RRPP domain.

Format

protected-vlan reference-instance { **all** | { { *instance-id1* [**to** *instance-id2*] } &<1-10> } }

undo protected-vlan reference-instance { **all** | { { *instance-id1* [**to** *instance-id2*] } &<1-10> } }

Parameters

Parameter	Description	Value
reference-instance	Indicates the instance imported by a specified RRPP domain.	-
all	Indicates that VLANs in all the instances are protected VLANs. **all** can be configured successfully only when instances 0 to 64 are created. This task is performed to create an instance and configure the mapping between the instance and VLANs.	-

Parameter	Description	Value
instance-id1 **to** *instance-id2*	Specifies the ID of a protected instance. ● *instance-id1* specifies the first instance ID. The value is an integer that ranges from 0 to 4094. ● **to** *instance-id2* specifies the last instance ID. *instance-id2* is an integer that ranges from 0 to 4094. The value of *instance-id2* must be larger than the value of *instance-id1*. *instance-id1* and *instance-id2* identify a range of instances. If **to** *instance-id2* is not specified, only *instance-id1* is specified.	The value is an integer that ranges from 0 to 4094.

Views

RRPP domain view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The control VLAN transmits RRPP protocol packets and the data VLAN transmits data packets. The control VLAN and data VLANs must be configured as the protected VLANs so that RRPP takes effect for these VLAN packets. Otherwise, VLAN packets may cause broadcast storms on the ring network. This will cause the network to be unavailable.

Precautions

When you configure the list of protected VLANs, note the following points:

- Protected VLANs must be configured before you configure an RRPP ring.
- You can delete or change existing protected VLANs before configuring an RRPP ring. The protected VLANs cannot be changed after the RRPP ring is configured.
- In the same physical topology, the control VLAN of a domain cannot be configured as a protected VLAN of another domain.
- The control VLAN must be configured as a protected VLAN; otherwise, the RRPP ring cannot be configured.
- The control VLAN can be mapped to other instances before the RRPP ring is created. After the RRPP ring is created, the mapping cannot be changed unless you delete the RRPP ring.
- When an RRPP domain is deleted, the protected VLANs in the RRPP domain are deleted automatically.
- When the mapping between an instance and VLANs changes, the protected VLANs of the RRPP domain also change.
- All the VLANs allowed by an RRPP interface must be configured as protected VLANs.

If the **protected-vlan** command is run more than once, all configurations take effect.

Example

# Configure the VLANs mapping instances 0 as the protected VLANs in Domain 1.

```
<HUAWEI> system-view
[HUAWEI] rrpp domain 1
[HUAWEI-rrpp-domain-region1] control-vlan 100
[HUAWEI-rrpp-domain-region1] protected-vlan reference-instance 0
```

5.14.13 reset rrpp error packet statistics

Function

The **reset rrpp error packet statistics** command clears statistics on RRPP error packets.

Format

reset rrpp error packet statistics

Parameters

None

Views

All views

Default Level

3: Management level

Usage Guidelines

Usage Scenario

If you need to check statistics on RRPP error packets from the current time, you can run this command to clear historical statistics on RRPP error packets.

Configuration Impact

The statistics on all the RRPP error packets are cleared and cannot be restored after you run the command. Exercise caution when you run the command.

Example

# Clear statistics on all the RRPP error packets.

```
<HUAWEI> reset rrpp error packet statistics
```

5.14.14 reset rrpp statistics

Function

The **reset rrpp statistics** command clears statistics on all RRPP packets.

Format

reset rrpp statistics domain *domain-id* [**ring** *ring-id*]

Parameters

Parameter	Description	Value
domain *domain-id*	Specifies the ID of an RRPP domain.	The value is an integer that ranges from 1 to 64.
ring *ring-id*	Specifies the ID of an RRPP ring. If *ring-id* is specified, statistics on RRPP packets on the primary and secondary interfaces of the specified ring in the domain of the switch are cleared. If *ring-id* is not specified, statistics on all the RRPP packets on the RRPP interfaces of all rings are cleared.	The value is an integer that ranges from 1 to 64.

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

This command clears statistics on all the RRPP packets so that you can collect new statistics to analyze the network.

Precautions

The statistics on RRPP packets cannot be restored after you clear them. Exercise caution before you run the command.

Example

# Clear the statistics on RRPP packets on Ring 1 in Domain 1.

```
<HUAWEI> reset rrpp statistics domain 1 ring 1
```

# Clear the statistics on RRPP packets all the rings in Domain 1.

```
<HUAWEI> reset rrpp statistics domain 1
```

5.14.15 ring enable

Function

The **ring enable** command enables an RRPP ring.

The **undo ring enable** command disables an RRPP ring.

By default, an RRPP ring is disabled.

Format

ring *ring-id* **enable**

undo ring *ring-id* **enable**

Parameters

Parameter	Description	Value
ring *ring-id*	Specifies the ID of an RRPP ring.	The value is an integer that ranges from 1 to 64.

Views

RRPP domain view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The RRPP ring cannot be activated using the **ring enable** command. You also need to run the **rrpp enable** command to enable RRPP so that the RRPP ring can be activated.

Example

# Activate ring 1 in Domain 1.

```
<HUAWEI> system-view
[HUAWEI] rrpp domain 1
[HUAWEI-rrpp-domain-region1] control-vlan 100
[HUAWEI-rrpp-domain-region1] protected-vlan reference-instance 0
[HUAWEI-rrpp-domain-region1] ring 1 node-mode transit primary-port gigabitethernet 0/0/5
secondary-port gigabitethernet 0/0/6 level 1
[HUAWEI-rrpp-domain-region1] ring 1 enable
```

# Disable Ring 1 in Domain 1.

```
<HUAWEI> system-view
[HUAWEI] rrpp domain 1
[HUAWEI-rrpp-domain-region1] undo ring 1 enable
```

5.14.16 ring node-mode

Function

The **ring node-mode** command configures the node mode and specifies the interfaces for nodes.

The **undo ring** command deletes an RRPP ring.

NOTE

Deleting the RRPP ring can delete the mode configured on the node and interfaces on the node.

Format

ring *ring-id* **node-mode** { **master** | **transit** } **primary-port** *interface-type interface-number* **secondary-port** *interface-type interface-number* **level** *level-value*

ring *ring-id* **node-mode** { **assistant-edge** | **edge** } **common-port** *interface-type interface-number* **edge-port** *interface-type interface-number*

undo ring *ring-id*

Parameters

Parameter	Description	Value
ring *ring-id*	Specifies the ID of an RRPP ring to be created or deleted.	The value is an integer that ranges from 1 to 64.
master	Specifies the current device as the master node on the RRPP ring to be created. You need to specify the primary and secondary interfaces on the master node, and the level of the ring.	-
transit	Specifies the current device as a transit node on the RRPP ring to be created. You need to specify the primary and secondary interfaces on the transit node, and the level of the ring.	-

Parameter	Description	Value
primary-port	Specifies the primary interface on the node.	-
interface-type interface-number	Specifies the type and number of an interface. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number.	-
secondary-port	Specifies the secondary interface of the node.	-
level-value	Specifies the level on an RRPP ring.	The value can be 0 or 1. ● 0: indicates a major ring. ● 1: indicates a sub-ring.
assistant-edge	Specifies the current device as the assistant edge node on the RRPP ring to be created.	-
edge	Specifies the current device as the edge node on the RRPP ring to be created.	-
common-port *interface-type interface-number*	Specifies the common interface of the sub-ring and major ring. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number.	-
edge-port *interface-type interface-number*	Specifies the edge interface of the sub-ring. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number.	-

Views

RRPP domain view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

RRPP specifies devices and interfaces on the ring network as nodes and interfaces of different roles on the RRPP ring to implement RRPP functions.

Prerequisites

An RRPP domain has been created using the **rrpp domain** command, and STP has been enabled using the **stp disable** command on the interfaces that want to join the RRPP domain.

Precautions

- The rings in the same RRPP domain must use different ring IDs.
- After the RRPP ring is enabled, to delete the RRPP ring using the **undo ring** *ring-id* command, you must run the **undo ring** *ring-id* **enable** command to disable the RRPP ring first.
- After the **control-vlan** command is used to configure the control VLAN in an RRPP domain, the ID of the sub-control VLAN is the control VLAN ID plus one. If the protected VLAN list specified by **protected-vlan** does not contain the control VLAN or sub-control VLAN, the system displays an error message when you run the **ring node-mode** command.

Example

# Configure the master node of Ring 10 in Domain 1, with GE0/0/5 as the primary interface and GE0/0/6 as the secondary interface.

```
<HUAWEI> system-view
[HUAWEI] rrpp domain 1
[HUAWEI-rrpp-domain-region1] control-vlan 100
[HUAWEI-rrpp-domain-region1] protected-vlan reference-instance 0
[HUAWEI-rrpp-domain-region1] ring 10 node-mode master primary-port gigabitethernet 0/0/5
secondary-port gigabitethernet 0/0/6 level 0
```

# Configure the transit node of Ring 10 in Domain 1, with GE0/0/5 as the primary interface and GE0/0/6 as the secondary interface.

```
<HUAWEI> system-view
[HUAWEI] rrpp domain 1
[HUAWEI-rrpp-domain-region1] control-vlan 100
[HUAWEI-rrpp-domain-region1] protected-vlan reference-instance 0
[HUAWEI-rrpp-domain-region1] ring 10 node-mode transit primary-port gigabitethernet 0/0/5
secondary-port gigabitethernet 0/0/6 level 0
```

# Configure the master node of Ring 20 in Domain 1, with GE0/0/5 as the primary interface and GE0/0/6 as the secondary interface.

```
<HUAWEI> system-view
[HUAWEI] rrpp domain 1
```

```
[HUAWEI-rrpp-domain-region1] control-vlan 100
[HUAWEI-rrpp-domain-region1] protected-vlan reference-instance 0
[HUAWEI-rrpp-domain-region1] ring 20 node-mode master primary-port gigabitethernet 0/0/5
secondary-port gigabitethernet 0/0/6 level 1
```

# Configure the transit node of Ring 20 in Domain 1, with GE0/0/5 as the primary interface and GE0/0/6 as the secondary interface.

```
<HUAWEI> system-view
[HUAWEI] rrpp domain 1
[HUAWEI-rrpp-domain-region1] control-vlan 100
[HUAWEI-rrpp-domain-region1] protected-vlan reference-instance 0
[HUAWEI-rrpp-domain-region1] ring 20 node-mode transit primary-port gigabitethernet 0/0/5
secondary-port gigabitethernet 0/0/6 level 1
```

# Delete Ring 10.

```
<HUAWEI> system-view
[HUAWEI] rrpp domain 1
[HUAWEI-rrpp-domain-region1] undo ring 10 enable
[HUAWEI-rrpp-domain-region1] undo ring 10
```

5.14.17 rrpp domain

Function

The **rrpp domain** command creates an RRPP domain.

The **undo rrpp domain** command deletes an RRPP domain.

By default, the RRPP domain is not created.

Format

rrpp domain *domain-id*

undo rrpp domain *domain-id*

Parameters

Parameter	Description	Value
domain *domain-id*	Specifies the ID of an RRPP domain.	The value is an integer that ranges from 1 to 64.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Other RRPP configurations can be performed only after an RRPP domain is created.

Precautions

Before you delete a domain, ensure that no RRPP ring is configured in the domain. If a ring exists in the domain, the domain cannot be deleted.

Example

# Create RRPP Domain 1.

```
<HUAWEI> system-view
[HUAWEI] rrpp domain 1
[HUAWEI-rrpp-domain-region1]
```

# Delete RRPP Domain 1.

```
<HUAWEI> system-view
[HUAWEI] undo rrpp domain 1
```

5.14.18 rrpp enable

Function

The **rrpp enable** command enables RRPP.

The **undo rrpp enable** or **rrpp disable** command disables RRPP.

By default, RRPP is disabled.

Format

rrpp enable

undo rrpp enable

rrpp disable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The RRPP ring cannot be activated using the **rrpp enable** command. You also need to run the **ring enable** command to enable RRPP so that the RRPP ring can be activated.

NOTE

Running the **undo rrpp enable** or **rrpp disable** command may cause network loops. Therefore, exercise caution when running these commands.

Example

# Enable RRPP.

```
<HUAWEI> system-view
[HUAWEI] rrpp enable
```

# Disable RRPP.

```
<HUAWEI> system-view
[HUAWEI] undo rrpp enable
```

# Disable RRPP.

```
<HUAWEI> system-view
[HUAWEI] rrpp disable
```

5.14.19 rrpp linkup-delay-timer

Function

The **rrpp linkup-delay-timer** command sets the value of a LinkUp timer.

The **undo rrpp linkup-delay-timer** command restores the default value of a LinkUp timer.

By default, the value of a LinkUp timer is 0.

Format

rrpp linkup-delay-timer *linkup-delay-timer-value*

undo rrpp linkup-delay-timer

Parameters

Parameter	Description	Value
linkup-delay-timer-value	Sets the value of the LinkUp timer.	The value is an integer that ranges from 0 to 1000, in seconds.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the link recovers, transmission paths of the traffic are switched frequently if the link status changes frequently on a ring. As a result, link flapping occurs and system performance deteriorates. To address this problem, a LinkUp timer is used to set the period after which the status of the master node changes to Complete.

Precautions

After a LinkUp timer is set, the status of the Blocked interface on the RRPP link is changed only after the period set using the *linkup-delay-timer-value* command. This prevents link flapping.

The value set by the *linkup-delay-timer-value* command must be no larger than the value of the Fail timer minus twice the value of the Hello timer.

The **rrpp linkup-delay-timer** command is valid only for the master node.

Configure the LinkUp timer on the master node on the RRPP ring.

In scenarios where RRPP packets are transparently transmitted, running the **rrpp linkup-delay-timer** command on the master node of the major ring is not recommended. If you do so, temporary loops may occur due to RRPP packet interruption or loss.

Example

# Set the value of the LinkUp timer to 2 seconds.

```
<HUAWEI> system-view
[HUAWEI] rrpp linkup-delay-timer 2
```

5.14.20 rrpp ring-group

Function

The **rrpp ring-group** command creates an RRPP ring group and enters the RRPP ring group view.

The **undo rrpp ring-group** command deletes an RRPP ring group.

By default, the RRPP ring group is not created.

Format

rrpp ring-group *ring-group-id*

undo rrpp ring-group *ring-group-id*

Parameters

Parameter	Description	Value
ring-group *ring-group-id*	Specifies the ID of an RRPP ring group.	The value is an integer that ranges from 1 to 16.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can create an RRPP ring group to reduce the number of Edge-Hello packets, improving system performance.

Precautions

A maximum of 16 ring groups are supported on each node.

When running the **rrpp ring-group** command to add a subring to a ring group, add the subring to the ring group on the assistant edge node and then on the edge node.

To delete a ring group, delete it on the edge node first, and then perform the same operation on the assistant edge node.

Example

# Create Ring Group 1 and enter its view.

```
<HUAWEI> system-view
[HUAWEI] rrpp ring-group 1
[HUAWEI-rrpp-ring-group1]
```

5.14.21 rrpp snooping enable

Function

The **rrpp snooping enable** command enables RRPP snooping on an interface.

The **undo rrpp snooping enable** command disables RRPP snooping on an interface.

By default, RRPP snooping is disabled on an interface.

NOTE

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

Format

rrpp snooping enable

undo rrpp snooping enable

Parameters

None

Views

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

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When an RRPP ring accesses the virtual private LAN service (VPLS) network in which devices are connected using PWs, the device cannot respond to RRPP protocol packets directly. Therefore, the VPLS network cannot sense the status change of the RRPP ring. When the RRPP ring topology changes, each node in the VPLS network forwards downstream data according to the MAC address table generated before the RRPP ring topology changes. As a result, the downstream traffic cannot be forwarded. When RRPP snooping is configured on sub-interfaces or VLANIF interfaces, the VPLS network can transparently transmit RRPP protocol packets, detect the changes on the RRPP rings, and upgrade the forwarding entries to ensure that traffic is switched in time to a congestion-free path.

When an RRPP network and a VPLS network are connected to form a network, you can run the **rrpp snooping enable** command to enable RRPP snooping on interfaces of the devices deployed on the network.

Precautions

Before running the **rrpp snooping enable** command, ensure that the following configurations are completed on the sub-interface or VLANIF interface:

- Binding the sub-interface or VLANIF interface to a VSI using the **l2 binding vsi** *vsi-name* command in the interface view.
- Specifying that the sub-interface or VLANIF interface permits only the packets in the control VLAN of the RRPP domain to pass through.

After you run the **rrpp snooping enable** command, RRPP snooping is automatically associated with the VSI bound to this interface.

When RRPP snooping is enabled on the interface, the status of the RRPP ring can be detected through RRPP control packets. When the RRPP ring status changes, the VSI can receive a notification and update the MAC address table.

RRPP and RRPP snooping cannot be simultaneously configured on the same interface.

Example

# Enable RRPP snooping on an interface.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] rrpp snooping enable
```

5.14.22 rrpp snooping vsi

Function

The **rrpp snooping vsi** command associates RRPP snooping on an interface with a VSI that is not bound to the interface.

The **undo rrpp snooping vsi** command cancels the configuration.

By default, the RRPP snooping-enabled interface is not associated with other VSIs on the device.

NOTE

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

Format

rrpp snooping vsi *vsi-name*

undo rrpp snooping vsi *vsi-name*

Parameters

Parameter	Description	Value
vsi-name	Specifies the name of a VSI instance.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Views

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

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In the scenario of RRPP and VPLS association, when the RRPP ring fails, the RRPP snooping-enabled interface clears the forwarding entries on the associated VSI and the remote VPLS device, and relearns the entries. In this way, downstream traffic can be forwarded through a normal path.

Precautions

Before running the **rrpp snooping vsi** command, you must enable RRPP snooping using the **rrpp snooping enable** command.

The VSI specified in the **rrpp snooping vsi** command is bound to other sub-interfaces or VLANIF interfaces, instead of the interface where RRPP snooping is enabled.

After you run the **rrpp snooping vsi** command, the change of the RRPP ring status is reported to the VSI that is bound to the interface so that the VSI can update its MAC address table.

Example

# Associate RRPP snooping with VSI **abc**.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] rrpp snooping vsi abc
```

5.14.23 rrpp snooping all-vsi

Function

The **rrpp snooping all-vsi** command associates a sub-interface with the VSI that all the other sub-interfaces connected to the same primary interface are bound to.

The **undo rrpp snooping all-vsi** command cancels the association.

By default, a sub-interface is not associated with the VSI that all the other sub-interfaces connected to the same primary interface are bound to.

NOTE

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

Format

rrpp snooping all-vsi

undo rrpp snooping all-vsi

Parameters

None

Views

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

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In the scenario of RRPP and VPLS association, when the RRPP ring fails, the RRPP snooping-enabled sub-interface clears the forwarding entries on the associated VSI and the remote VPLS device, and relearns the entries. In this way, downstream traffic can be forwarded through a normal path.

You can run the **rrpp snooping all-vsi** command on the RRPP snooping-enabled sub-interface to associate the sub-interface with the VSI that all the other sub-interfaces connected to the same primary interface are bound to. The sub-interface clears all the forwarding entries of associated VSIs when the preceding fault occurs.

Prerequisites

RRPP snooping has been enabled using the **rrpp snooping enable** command.

Precautions

- You must run the **l2 binding vsi** *vsi-name* command to bind other interfaces connected to the same primary interface to the VSI before associating the VSI using the **rrpp snooping all-vsi** command on the current sub-interface.
- You can run the **undo rrpp snooping all-vsi** command to cancel all the associations between the current sub-interface and the VSIs bound to other interfaces connected to the same primary interface.
- You do not need to enable RRPP snooping on other sub-interfaces connected to the same primary interface.

Example

# Associate the sub-interface with VSIs that all the other sub-interfaces connected to the same primary interface are bound to.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1.1
[HUAWEI-GigabitEthernet0/0/1.1] rrpp snooping enable
[HUAWEI-GigabitEthernet0/0/1.1] rrpp snooping all-vsi
```

5.14.24 timer (RRPP domain view)

Function

The **timer** command sets the values of the Hello timer and Fail timer.

The **undo timer** command restores the default values of the Hello timer and Fail timer.

By default, the value of the Hello timer is 1 second and that of the Fail timer is 6 seconds.

Format

timer hello-timer *hello-value* **fail-timer** *fail-value*

undo timer

Parameters

Parameter	Description	Value
hello-timer *hello-value*	Specifies the value of the Hello timer.	The value is an integer that ranges from 1 to 10, in seconds. The default value is 1.
fail-timer *fail-value*	Specifies the value of the Fail timer.	The value is an integer that ranges from 3 to 1200, in seconds. The default value is 6. The value of *fail-value* must be three times the value of *hello-value* or larger.

Views

RRPP domain view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can set the values of the Hello timer and Fail timer as required.

Precautions

You need to run the **timer** command only on the master node, edge node, and assistant edge node.

The value of the Fail timer must be three times the value of the Hello timer or larger.

By default, the value of the Hello timer on an edge node is half of the value of the Hello timer on the master node of the major ring.

The values of the Hello timer and Fail timer must be the same on the nodes in an RRPP domain; otherwise, the edge interface on the edge node may be unstable.

You are advised to set the value of the Fail timer to 30 seconds, because the default value may cause temporary loops. For example, when RRPP multi-instance is enabled, multiple RRPP domains are configured on the same ring. If the value of the Fail timer is set to the default value, loops may occur.

Example

# Set the Hello timer and Fail timer in RRPP Domain 1 to 2s and 7s respectively.

```
<HUAWEI> system-view
[HUAWEI] rrpp domain 1
[HUAWEI-rrpp-domain-region1] timer hello-timer 2 fail-timer 7
```

# Restore the default values of the timers in RRPP Domain 1.

```
<HUAWEI> system-view
[HUAWEI] rrpp domain 1
[HUAWEI-rrpp-domain-region1] undo timer
```

5.15 ERPS (G.8032) Configuration Commands

5.15.1 Command Support

Commands provided in this section and all the parameters in the commands are supported by all switch models (except the S5731-L and S5731S-L), unless otherwise specified. For details, see specific commands.

5.15.2 clear (ERPS ring view)

Function

The **clear** command clears the port blocking mode of an ERPS ring.

Format

clear

Parameters

None

Views

ERPS ring view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To clear the FS or MS mode configured by the **erps ring protect-switch** command, run the **clear** command. The **clear** command also provides the following functions:

- Triggers revertive switching before the WTR or WTB timer expires in the case of revertive switching operations.
- Triggers revertive switching in the case of non-revertive operations.

Precautions

The **clear** command is supported in both ERPSv1 and ERPSv2.

Example

# Clear the port blocking mode of ERPS ring 5.

```
<HUAWEI> system-view
[HUAWEI] erps ring 5
[HUAWEI-erps-ring5] clear
```

5.15.3 control-vlan (ERPS ring view)

Function

The **control-vlan** command configures a control VLAN for an ERPS ring to forward RAPS PDUs.

The **undo control-vlan** command deletes the configured control VLAN.

By default, no control VLAN is configured in an ERPS ring.

Format

control-vlan *vlan-id*

undo control-vlan

Parameters

Parameter	Description	Value
vlan-id	Specifies the ID of a control VLAN for an ERPS ring.	The value is an integer that ranges from 1 to 4094.

Views

ERPS ring view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After an ERPS ring is created, run the **control-vlan** command to create the control VLAN. Unlike a data VLAN, a control VLAN is used only to forward ERPS protocol packets but not forward service packets in an ERPS ring, which improves the security of the ERPS protocol.

Precautions

- If you run the **control-vlan** command multiple times, only the latest configuration takes effect.
- After a control VLAN is created, the **vlan batch** { *vlan-id1* [**to** *vlan-id2*] } &<1-10> command used to create common VLANs is displayed in the configuration file.
- After a port is added to an ERPS ring configured with a control VLAN, the port is added to the control VLAN.
  - If the port is a trunk port, the **port trunk allow-pass vlan** *vlan-id* command is displayed in the record of the port that has been added to the ERPS ring in the configuration file.
  - If the port is a hybrid port, the **port hybrid tagged vlan** *vlan-id* command is displayed in the record of the port that has been added to the ERPS ring in the configuration file.
- All the devices in an ERPS ring must use the same control VLAN in an ERPS ring, and different ERPS rings must use different control VLANs.
- The control VLAN must be not created, and is not used by other features. In addition, no interface is added to the control VLAN.
- If ports have been added to an ERPS ring, the control VLAN cannot be modified. To delete the configured control VLAN, run the **undo erps ring** command in the interface view or the **undo port** command in the ERPS ring view to delete ports from the ERPS ring, and run the **undo control-vlan** command to delete the control VLAN.
- Run the **display erps** command to check whether the control VLAN is configured or which VLAN is configured as the control VLAN.

Example

# Configure control VLAN 5 in ERPS ring 1.

```
<HUAWEI> system-view
[HUAWEI] erps ring 1
[HUAWEI-erps-ring1] control-vlan 5
```

5.15.4 description (ERPS ring view)

Function

The **description** command configures the description of an ERPS ring.

The **undo description** command restores the default description of an ERPS ring.

By default, the description of an ERPS ring is the name of the ERPS ring. For example, if the name of an ERPS ring is Ring1, the default description of the ring is Ring 1.

Format

description *text*

undo description

Parameters

Parameter	Description	Value
text	Specifies the description of an ERPS ring.	The value is a string of 1 to 80 case-sensitive characters.

Views

ERPS ring view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can run the **description** command on the ERPS-enabled device to configure the description of an ERPS ring. The description contains information such as the ID of the ERPS ring, which facilitates maintenance.

Precautions

If you run the **description** command multiple times, only the latest configuration takes effect.

After the description is configured in the ERPS ring view, the description only takes effect on the device.

Example

# Configure the description of the ERPS ring 10 as **huawei Ring 1** on the device.

```
<HUAWEI> system-view
[HUAWEI] erps ring 10
[HUAWEI-erps-ring10] description huawei Ring 1
```

5.15.5 display erps

Function

The **display erps** command displays ports that are added to an ERPS ring and information about the ERPS ring.

Format

display erps [**ring** *ring-id*] [**verbose**]

Parameters

Parameter	Description	Value
ring *ring-id*	Displays information about an ERPS ring and the ports that are added to the ERPS ring.	The value is an integer that ranges from 1 to 255.
verbose	Displays detailed information about an ERPS ring and the ports that are added to the ERPS ring.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

You can run the **display erps** command on the ERPS-enabled device to view ports added to the ERPS ring and information about the ERPS ring. The command output facilitates ERPS management and helps you learn the running status of ports.

Prerequisites

To view information about ports that have been added to a specified ERPS ring and the ERPS ring, ensure that the ERPS ring has already been created.

Precautions

If **ring** *ring-id* is not specified, information about all the ERPS rings and ports added to the ERPS rings is displayed.

Example

# Display information about all ERPS rings and ports that are added to the ERPS rings.

```
<HUAWEI> display erps
D  : Discarding
F  : Forwarding
R  : RPL Owner
N  : RPL Neighbour
FS : Forced Switch
MS : Manual Switch
Total number of rings configured = 4
Ring  Control  WTR Timer  Guard Timer  Port 1              Port 2
ID    VLAN     (min)      (csec)
-------------------------------------------------------------------------------
  1     100        1          50  (D)GE0/0/1          (F,R)GE0/0/2
  2     200        2          50  (D)GE0/0/3          (F)GE0/0/4
  3     300        3          50  (F)ETH-TRUNK3       (D)ETH-TRUNK4
  4     400        5          50  (F,R)ETH-TRUNK1      (D)ETH-TRUNK2
--------------------------------------------------------------------------------
```

# Display information about ERPS ring 1 and ports that are added to ERPS ring 1.

```
<HUAWEI> display erps ring 1
D  : Discarding
F  : Forwarding
R  : RPL Owner
N  : RPL Neighbour
FS : Forced Switch
MS : Manual Switch
Ring  Control  WTR Timer  Guard Timer  Port 1              Port 2
ID    VLAN     (min)      (csec)
--------------------------------------------------------------------------------
  1     100        1          50  (D)GE0/0/1         (F,R)GE0/0/2
--------------------------------------------------------------------------------
```

# Display detailed information about all ERPS rings and ports that are added to the ERPS rings.

```
<HUAWEI> display erps verbose
Ring ID                           : 101
Description                       : Ring 101
Control Vlan                      : 1001
Protected Instance                : 4091
Service Vlan                      : 200 to 400
WTR Timer Setting (min)           : 1      Running (s)           : 0
Guard Timer Setting (csec)        : 200    Running (csec)        : 0
Holdoff Timer Setting (deciseconds) : 0      Running (deciseconds) : 0
WTB Timer Running (csec)          : 0
Ring State                        : Idle
RAPS_MEL                          : 7
Revertive Mode                    : Revertive
R-APS Channel Mode                : -
Version                           : 2
Sub-ring                          : No
Forced Switch Port                : -
Manual Switch Port                : -
TC-Notify                         : -
Time since last topology change   : 0 days 0h:31m:49s
--------------------------------------------------------------------------------
Port              Port Role     Port Status     Signal Status
--------------------------------------------------------------------------------
GE0/0/1           Common        Discarding      Non-failed
GE0/0/2           Common        Forwarding      Non-failed

Ring ID                           : 102
Description                       : Ring 102
Control Vlan                      : 1002
Protected Instance                : 4092
Service Vlan                      : 500 to 600
WTR Timer Setting (min)           : 1      Running (s)           : 0
Guard Timer Setting (csec)        : 200    Running (csec)        : 0
Holdoff Timer Setting (deciseconds) : 0      Running (deciseconds) : 0
WTB Timer Running (csec)          : 0
Ring State                        : Idle
RAPS_MEL                          : 7
Revertive Mode                    : Revertive
R-APS Channel Mode                : -
Version                           : 2
Sub-ring                          : No
Forced Switch Port                : -
Manual Switch Port                : -
TC-Notify                         : -
Time since last topology change   : 0 days 4h:12m:20s
--------------------------------------------------------------------------------
Port              Port Role     Port Status     Signal Status
--------------------------------------------------------------------------------
```

```
GE0/0/1            Common        Forwarding      Non-failed
GE0/0/2            RPL Owner     Discarding      Non-failed
```

# Display detailed information about ERPS ring 1 and ports that are added to ERPS ring 1.

```
<HUAWEI> display erps ring 1 verbose
Ring ID                           : 1
Description                       : Ring 102
Control Vlan                      : 1002
Protected Instance                : 4092
Service Vlan                      : 500 to 600
WTR Timer Setting (min)           : 1      Running (s)           : 0
Guard Timer Setting (csec)        : 200    Running (csec)        : 0
Holdoff Timer Setting (deciseconds) : 0      Running (deciseconds) : 0
WTB Timer Running (csec)          : 0
Ring State                        : Idle
RAPS_MEL                          : 7
Revertive Mode                    : Revertive
R-APS Channel Mode                : -
Version                           : 2
Sub-ring                          : No
Forced Switch Port                : -
Manual Switch Port                : -
TC-Notify                         : -
Time since last topology change   : 0 days 4h:13m:40s
--------------------------------------------------------------------------------
Port               Port Role     Port Status     Signal Status
--------------------------------------------------------------------------------
GE0/0/1            Common        Forwarding      Non-failed
GE0/0/2            RPL Owner     Discarding      Non-failed
```

Table 5-103 Description of the display erps command output

Item	Description
D: Discarding	The port is in discarding state.
F: Forwarding	The port is in forwarding state.
R: RPL Owner	The port is the RPL Owner port.
N : RPL Neighbour	The port is the RPL neighbor port.
FS : Forced Switch	The port is blocked by an FS operation.
MS : Manual Switch	The port is blocked by an MS operation.
Total number of rings configured	Number of ERPS rings.
Ring ID	ID of the ERPS ring. To configure an ERPS ring, run the **erps ring** command.
Control VLAN	Control VLAN. To configure a control VLAN, run the **control-vlan** command.
WTR Timer (min)	Value of the WTR timer. To set the value of the WTR timer, run the **wtr-timer** command.
Guard Timer (csec)	Value of the Guard timer. To set the value of the Guard timer, run the **guard-timer** command.

Item	Description
Port 1	A port that is added to the specified ERPS ring.
Port 2	Another port that is added to the specified ERPS ring.
Description	Description of an ERPS ring. To configure the description, run the **description** command.
Protected Instance	ERPS instance. To configure an ERP instance, run the **protected-instance** command.
Service Vlan	Service VLAN associated with ERPS. A service VLAN is mapped to an ERP instance, and is not the control VLAN.
WTR Timer Setting (min) Running (s)	Value of the WTR timer. Setting indicates the configured value and Running indicates the actual value. To set the value of the WTR timer, run the **wtr-timer** command.
Guard Timer Setting (csec) Running (csec)	Value of the Guard timer. Setting indicates the configured value and Running indicates the actual value. To set the value of the Guard timer, run the **guard-timer** command.
Holdoff Timer Setting (deciseconds) Running (deciseconds)	Value of the Holdoff timer. Setting indicates the configured value and Running indicates the actual value. To set the value of the Holdoff timer, run the **holdoff-timer** command.
WTB Timer Running (csec)	Value of the WTB timer.
Ring State	Status of the ERPS ring: ● Idle: indicates that the current blocking point is the RPL Owner port. ● Protection: indicates that a fault has occurred on a link or a device. ● Pending: indicates a transition state during ERPS ring negotiation. For example, the blocking point is being switched back to the RPL Owner port. ● ForcedSwitch: The FS mode is used to block an ERPS port. ● ManualSwitch: The MS mode is used to block an ERPS port.
RAPS_MEL	MEL value. To set the MEL value, run the **raps-mel** command.

Item	Description
Revertive Mode	Revertive or non-revertive switching mode to be used after a faulty ERPS link recovers: ● Revertive: re-blocks the RPL owner port after a faulty ERPS link recovers. ● Non-revertive: retains the RPL owner port status and still blocks the port of the faulty link after a faulty ERPS link recovers. To configure the revertive or non-revertive switching mode, run the **revertive** command.
R-APS Channel Mode	RAPS PDU transmission mode in a sub-ring: ● -: The current ring is not a sub-ring. ● Virtual Channel: VCs are used to transmit RAPS PDUs. ● Non-virtual-channel: NVCs are used to transmit RAPS PDUs. To configure an RAPS PDU transmission mode in a sub-ring, run the **virtual-channel** command.
Version	ERPS version: ● 1: ERPSv1 ● 2: ERPSv2 To configure an ERPS version, run the **version** command.
Sub-ring	ERPS sub-ring ID. To configure an ERPS sub-ring ID, run the **sub-ring** command.
Forced Switch Port	Port that has been blocked by an FS operation. A hyphen (-) indicates that no port has been blocked by an FS operation. To configure an FS mode, run the **erps ring protect-switch** command.
Manual Switch Port	Port that has been blocked by an MS operation. A hyphen (-) indicates that no port has been blocked by an MS operation. To configure a port blocking mode for an ERPS port, run the **erps ring protect-switch** command.
TC-Notify	The ERPS ring is configured to notify other ERPS rings of its topology change. A hyphen (-) indicates that the ERPS ring does not notify other ERPS rings when its topology changes. To configure an ERPS ring to notify other ERPS rings of its topology change, run the **tc-notify erps ring** command.
Time since last topology change	Period since the last ERPS ring topology change.

Item	Description
Port	Port that is added to the ERPS ring.
Port Role	Port role: ● RPL Owner ● Common ● RPL Neighbour
Port Status	Port status: ● Forwarding ● Discarding
Signal Status	Signal status: ● Failed: A fault occurs. ● Non-failed: No fault occurs.

5.15.6 display erps interface

Function

The **display erps interface** command displays ERPS information of a port that has been added to an ERPS ring.

Format

display erps interface *interface-type interface-number* [**ring** *ring-id*]

Parameters

Parameter	Description	Value
interface-type interface-number	Displays ERPS information of a specified port that has been added to an ERPS ring. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number.	-
ring *ring-id*	Specifies the ID of the ERPS ring to which the port has been added.	The value is an integer that ranges from 1 to 255.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

To check the running status of ports that have been added to an ERPS ring, run the **display erps interface** command.

Example

# Display ERPS information about GigabitEthernet0/0/1.

```
<HUAWEI> display erps interface gigabitethernet 0/0/1
Interface State                     : Up
--------------------------------------------------------------------------------
Ring ID                             : 1
Flush Logic
    Remote Node ID                  : 0000-0000-0000
    Remote BPR                      : 0
Track Link Detect Protocol          : 1AG
    MD Name                         : 1
    MA Name                         : 1
    MEP ID                          : 2270
    RMEP ID                         : 2260
    CFM State                       : Failed
```

Table 5-104 Description of the **display erps interface** command output

Item	Description
Interface State	Physical status of the port.
Ring ID	ID of the ERPS ring to which the port has been added.
Flush Logic	Whether the FDB logic is updated.
Remote Node ID	ID of the remote node.
Remote BPR	Blocked port reference of the remote node.
Track Link Detect Protocol	Protocol associated with ERPS on the port. The hyphen (-) indicates that no protocol is associated with ERPS on the port.
MD Name	Name of the maintenance domain for which Ethernet CFM is associated with ERPS.
MA Name	Name of the maintenance association (MA) where Ethernet CFM is associated with ERPS.
MEP ID	ID of the maintenance association end point (MEP) where Ethernet CFM is associated with ERPS.
RMEP ID	ID of the remote maintenance association end point (RMEP) where Ethernet CFM is associated with ERPS.

Item	Description
CFM State	Status of the protocol associated with ERPS on the port.

5.15.7 display erps statistics

Function

The **display erps statistics** command displays statistics about sent and received ring auto protection switching (RAPS) protocol data units (PDUs) on the ports that have been added to ERPS rings.

Format

display erps [**ring** *ring-id*] **statistics**

Parameters

Parameter	Description	Value
ring *ring-id*	Specifies the ID of an ERPS ring. If this parameter is not specified, this command displays statistics about sent and received RAPS PDUs on ports that are added to all ERPS rings.	The value is an integer that ranges from 1 to 255.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

On a Layer 2 network running ERPS, the **display erps statistics** command displays statistics about sent and received RAPS PDUs on the ports that are added to ERPS rings. The command output helps you analyze the network situation, learn the network running status, and maintain devices.

Prerequisites

To query statistics about sent and received RAPS PDUs on the ports that have been added to a specified ERPS ring, ensure that the ERPS ring has been created.

Example

# Display statistics about sent and received RAPS PDUs on the ports that are added to ERPS rings.

```
<HUAWEI> display erps statistics
--------------------------------------------------------------------------------
Ring Port          RX/TX     SF      NR     NRRB      FS      MS    EVENT
--------------------------------------------------------------------------------
   1 Eth-Trunk1      RX         0       0     552       0       0       0
   1 Eth-Trunk1      TX         0      68       0     326       0       6
   1 GE0/0/1        RX         0       6     552       0       0       0
   1 GE0/0/1        TX         4      63       0     326       0       6
  10 GE0/0/2         RX         0       1       0       0       0       0
  10 GE0/0/2         TX         4      74       0       0       0       0
```

# Display statistics about sent and received RAPS PDUs on the ports that are added to ERPS ring 2.

```
<HUAWEI> display erps ring 2 statistics
--------------------------------------------------------------------------------
Ring  Port         RX/TX     SF      NR     NRRB      FS      MS    EVENT
--------------------------------------------------------------------------------
   2  GE0/0/1       RX         0       1       0       0       0       0
   2  GE0/0/1       TX         4      74       0       0       0       0
```

Table 5-105 Description of the display erps statistics command output

Item	Description
Ring	ID of the ERPS ring. To configure an ERPS ring, run the **erps ring** command.
Port	Port that is added to the ERPS ring.
RX/TX	RAPS PDU forwarding: ● RX: RAPS PDUs are received. ● TX: RAPS PDUs are sent.
SF	Statistics about RAPS (SF) messages.
NR	Statistics about RAPS (NR) messages.
NRRB	Statistics about RAPS (NR, RB) messages.
FS	Statistics about RAPS (FS) messages.
MS	Statistics about RAPS (MS) messages.
EVENT	Statistics about RAPS Event messages.

5.15.8 encapsulate-ring-id enable

Function

The **encapsulate-ring-id enable** command enables ERPS ring ID encapsulation in the destination MAC addresses of ERPS protocol packets.

The **undo encapsulate-ring-id enable** command disables ERPS ring ID encapsulation in the destination MAC addresses of ERPS protocol packets.

By default, ERPS ring ID encapsulation in the destination MAC addresses of ERPS protocol packets is disabled.

Format

encapsulate-ring-id enable

undo encapsulate-ring-id enable

Parameters

None

Views

ERPS ring view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A Huawei device cannot communicate with a non-Huawei device that sends ERPS protocol packets whose destination MAC addresses carry ERPS ring IDs. To enable the Huawei device to communicate with such a non-Huawei device, run the **encapsulate-ring-id enable** command to enable ERPS ring ID encapsulation in the destination MAC addresses of ERPS protocol packets sent by the Huawei device.

Precautions

The **encapsulate-ring-id enable** command and its undo form fail to be run in the view of an ERPS ring that has an interface added. To resolve this issue, remove the interface from the ERPS ring by running the **undo erps ring** *ring-id* command in the interface view or **undo port** *interface-type interface-number* command in the ERPS ring view.

Example

# Enable ERPS ring ID encapsulation in the destination MAC addresses of ERPS protocol packets.

```
<HUAWEI> system-view
[HUAWEI] erps ring 1
[HUAWEI-erps-ring1] encapsulate-ring-id enable
```

5.15.9 erps ring

Function

The **erps ring** command creates an ERPS ring and displays the view of the ERPS ring, or directly displays the view of an existing ERPS ring.

The **undo erps ring** command deletes a created ERPS ring.

By default, no ERPS ring is created.

Format

erps ring *ring-id*

undo erps ring *ring-id*

Parameters

Parameter	Description	Value
ring-id	Specifies the ID of an ERPS ring.	The value is an integer that ranges from 1 to 255.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Ethernet Ring Protection Switching (ERPS) is a standard protocol issued by the ITU-T to prevent loops on ring networks. ERPS implements fast convergence of carrier-class reliability standards. It allows all ERPS-capable devices on a ring network to communicate.

To enable ERPS on the device, run the **erps ring** command to create an ERPS ring and enter the ERPS ring view.

To configure parameters such as the control VLAN and the protected instance for an ERPS ring, run the **erps ring** command to enter the ERPS ring view.

Follow-up Procedure

Run the **control-vlan (ERPS ring view)** command to configure a control VLAN for the ERPS ring.

Run the **protected-instance (ERPS ring view)** command to configure an ERP instance for the ERPS ring.

Precautions

To delete an ERPS ring, ensure that no ports are added to the ERPS ring. If any port is added to the ERPS ring, the system displays a message indicating a failure to delete the ERPS ring. To delete an ERPS ring where ports are added, run the **undo erps ring** command in the interface view or the **undo port** command in the ERPS ring view to remove the port, and run the **undo erps ring** command to delete the ERPS ring.

Example

# Create ERPS ring 1.

```
<HUAWEI> system-view
[HUAWEI] erps ring 1
[HUAWEI-erps-ring1]
```

5.15.10 erps ring (interface view)

Function

The **erps ring** command adds a port to an ERPS ring and specifies a role for the port.

The **undo erps ring** command deletes a port from an ERPS ring and cancels the port role.

By default, a port is not added to an ERPS ring, and no port role is specified.

Format

erps ring *ring-id* [**rpl** { **owner** | **neighbour** }]

undo erps ring *ring-id*

Parameters

Parameter	Description	Value
ring-id	Specifies the ID of an ERPS ring.	The value is an integer that ranges from 1 to 255.
rpl { **owner** | **neighbour** }	Specifies the port to be added to an ERPS ring as the RPL owner port or RPL neighbor port.	-

Views

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

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After an ERPS ring is created, run the **erps ring** command in the interface view to add Layer 2 ports to the ERPS ring so that RAPS PDUs can be correctly forwarded. Each device in an ERPS ring is a node, and a maximum of two Layer 2 ports on each node can be added to the same ERPS ring.

ERPS defines three port roles: RPL owner port, RPL neighbor port (only in ERPSv2), and common port.

- RPL owner port

  An RPL owner port is responsible for blocking traffic over the Ring Protection Link (RPL) to prevent loops. An ERPS ring has only one RPL owner port.

  When the node on which the RPL owner port resides receives an RAPS PDU indicating a link or node fault in an ERPS ring, the node unblocks the RPL owner port. Then the RPL owner port can send and receive traffic to ensure nonstop traffic forwarding.

  The link where the RPL owner port resides is the RPL.

- RPL neighbor port

  An RPL neighbor port is directly connected to an RPL owner port.

  Both the RPL owner port and RPL neighbor ports are blocked in normal situations to prevent loops.

  If an ERPS ring fails, both the RPL owner and neighbor ports are unblocked.

  The RPL neighbor port helps reduce the number of FDB entry updates on the device where the RPL neighbor port resides.

- Common port

  Common ports are ring ports other than the RPL owner and neighbor ports.

  A common port monitors the status of the directly connected ERPS link and sends RAPS PDUs to notify the other ports of its link status changes.

Prerequisites

An ERPS ring has been created using the **erps ring** command.

- The control VLAN and ERP instance have been configured using the **control-vlan** and **protected-instance** commands respectively in the ERPS ring view.
- The port is not a Layer 3 port. If the port is a Layer 3 port, run the **portswitch** command to switch the port to the Layer 2 mode.
- Spanning Tree Protocol (STP), Rapid Ring Protection Protocol (RRPP), Smart Ethernet Protection (SEP), or Smart Link is not enabled on the port.
  - If the port has STP enabled, run the **stp disable** command in the interface view to disable STP.
  - If the port has RRPP enabled, run the **undo ring** *ring-id* command in the RRPP domain view to disable RRPP.
  - If the port has SEP enabled, run the **undo sep segment** *segment-id* command in the interface view to disable SEP.
  - If the port has Smart Link enabled, run the **undo port** command in the Smart Link group view to disable Smart Link.

- ERPSv2 has been specified in the ERPS ring using the **version v2** command if the port is specified as an RPL neighbor port.

Precautions

- Before running the **undo erps ring** command to delete a port from an ERPS ring, run the **shutdown (interface view)** command to shut down the port. The port can be enabled again according to the actual situation.
- If ports added to an ERPS ring are all ordinary ports, any port on the device with the largest MAC address will be blocked.
- If an RPL neighbor port is configured for a non-virtual channel of a sub-ring, network convergence may fail to meet requirements because SF packets are discarded on the port in the case of a link fault.

Example

# Add GE0/0/1 to ERPS ring 2.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] erps ring 2
```

5.15.11 erps ring protect-switch

Function

The **erps ring protect-switch** command configures a port blocking mode for an ERPS port.

Format

erps ring *ring-id* **protect-switch** { **force** | **manual** }

Parameters

Parameter	Description	Value
ring-id	Specifies the ID of an ERPS ring.	The value is an integer that ranges from 1 to 255.
force	Forcibly blocks a port immediately after FS is configured, irrespective of whether link failures have occurred.	-
manual	Indicates the MS mode for blocking an ERPS port.	-

Views

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

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Because the Ring Protection Link (RPL) may have high bandwidth, you can block the low-bandwidth link so that user traffic can be transmitted on the RPL. ERPSv2 supports both Forced Switch (FS) and Manual Switch (MS) modes for blocking an ERPS port:

- FS: forcibly blocks a port immediately after FS is configured, irrespective of whether link failures have occurred.
- MS: blocks a port on which MS is configured when the ERPS ring is in Idle or Pending state.

FS takes precedence over MS.

Prerequisites

- The **erps ring** or **port (ERPS ring view)** command has been executed to add the port to an ERPS ring.
- The **version v2** command has been executed to specify ERPSv2.

Configuration Impact

After an ERPS port is blocked in FS or MS mode, the node on which the ERPS port resides sends RAPS (FS) or RAPS (MS) messages to the other nodes in the ERPS ring. As a result, ERPS performs recalculation and finally unblocks the RPL owner port.

Precautions

The ERPS ring specified by *ring-id* must be the one to which the port belongs; otherwise, the command does not take effect.

To change the port blocking mode from MS to FS, run the **erps ring** *ring-id* **protect-switch force** command to set the FS mode. To change the port blocking mode from FS to MS, run the **clear** command in the ERPS ring view to delete the FS mode, and then run the **erps ring** *ring-id* **protect-switch manual** command to set the MS mode.

You can delete the manual port blocking mode only by using the **clear** command in the ERPS ring view.

The **erps ring protect-switch** command is not saved in the configuration file.

Example

# Specify the FS mode to block GigabitEthernet0/0/1 in ERPS ring 5.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] erps ring 5
[HUAWEI-GigabitEthernet0/0/1] erps ring 5 protect-switch force
```

5.15.12 erps track cfm

Function

The **erps track cfm** command associates ERPS with Ethernet CFM to fast detect link failures.

The **undo erps track cfm** command disassociates ERPS from Ethernet CFM.

By default, ERPS is not associated with Ethernet CFM.

Format

erps ring *ring-id* **track cfm md** *md-name* **ma** *ma-name* **mep** *mep-id* **remote-mep** *rmep-id*

undo erps ring *ring-id* [**track cfm**]

Parameters

Parameter	Description	Value
ring *ring-id*	Specifies the ID of an ERPS ring.	The value is an integer that ranges from 1 to 255.
md *md-name*	Specifies the name of a maintenance domain (MD).	The value is a string of 1 to 43 case-sensitive characters. Spaces and question marks (?) are not supported. MD names on a device must be unique. **NOTE** When double quotation marks are used around the string, spaces are allowed in the string.
ma *ma-name*	Specifies the name of a maintenance association (MA).	The value is a string of 1 to 43 case-sensitive characters. Spaces and question marks (?) are not supported. **NOTE** When double quotation marks are used around the string, spaces are allowed in the string.
mep *mep-id*	Specifies the ID of a maintenance association end point (MEP).	The value is an integer that ranges from 1 to 8191.

Parameter	Description	Value
remote-mep *rmep-id*	Specifies the ID of a remote maintenance association end point (RMEP).	The value is an integer that ranges from 1 to 8191.

Views

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

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To fast detect faults, implement fast convergence, and shorten traffic interruptions, run the **erps track cfm** command to associate ERPS with Ethernet CFM on a port added to an ERPS ring.

Prerequisites

- STP, RRPP, or SEP is not enabled on the port.
  - If the port has STP enabled, run the **stp disable** command in the interface view to disable STP.
  - If the port has RRPP enabled, run the **undo ring** *ring-id* command in the RRPP domain view to disable RRPP.
  - If the port has SEP enabled, run the **undo sep segment** *segment-id* command in the interface view to disable SEP.
- The port is not a Layer 3 port. If the port is a Layer 3 port, run the **portswitch** command to switch the port to the Layer 2 mode.
- The ERPS ring specified by **ring** *ring-id* must be the one to which the port belongs.
- Ethernet CFM has not been applied to other ports in the ERPS ring.

Precautions

This command is supported in both ERPSv1 and ERPSv2.

The association between ERPS and CFM takes effect only when the interface has ERPS associated with CFM and has an interface-based MEP created using the **mep mep-id** command.

Example

# Associate ERPS with Ethernet CFM on GigabitEthernet0/0/1.

```
<HUAWEI> system-view
```

```
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] erps ring 5
[HUAWEI-GigabitEthernet0/0/1] erps ring 5 track cfm md md1 ma ma1 mep 1 remote-mep 2
```

5.15.13 erps vpls-subinterface enable

Function

The **erps vpls-subinterface enable** command enables topology change notification of an interface to instruct VSI-bound sub-interfaces or VLANIF interfaces to update MAC address entries promptly after the ERPS ring topology changes.

The **undo erps vpls-subinterface enable** command disables topology change notification of an interface.

By default, the interface does not instruct VSI-bound sub-interfaces or VLANIF interfaces to update MAC address entries promptly after the ERPS ring topology changes.

NOTE

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

Format

erps vpls-subinterface enable

undo erps vpls-subinterface enable

Parameters

None

Views

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

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In normal situations, when an ERPS ring topology changes, the ERPS ring reselects a blocked interface, and accordingly all devices will update MAC address entries. However, if an ERPS-enabled interface has VSI-bound sub-interfaces or VLANIF interfaces, which cannot detect topology changes immediately, the MAC address entries will not be updated on the VPLS network in time. To resolve this problem, run the **erps vpls-subinterface enable** command to enable an interface to instruct VSI-bound sub-interfaces or VLANIF interfaces to update MAC address entries promptly after the ERPS ring topology changes.

Prerequisites

An interface has been added to an ERPS ring using the **erps ring (interface view)** command.

Configuration Impact

After the **erps vpls-subinterface enable** command has been run, when the forwarding status of an interface changes to Discarding, its VSI-bound sub-interfaces or VLANIF interfaces will change to the Flowdown state to prevent loops on the VPLS network on which a CE is dual-homed to PEs.

Precautions

The **erps vpls-subinterface enable** and **stp vpls-subinterface enable** commands are mutually exclusive on the same interface.

If an interface is deleted from all ERPS rings using the **undo erps ring** command, the **erps vpls-subinterface enable** command configuration on the interface is also deleted.

If a user is delivering the ERPS configuration, the **erps vpls-subinterface enable** command fails to be run.

Example

# Enable GE0/0/1 to instruct VSI-bound sub-interfaces or VLANIF interfaces to update MAC address entries promptly after the ERPS ring topology changes.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] erps ring 1
[HUAWEI-GigabitEthernet0/0/1] erps vpls-subinterface enable
```

5.15.14 guard-timer (ERPS ring view)

Function

The **guard-timer** command sets the Guard timer in an ERPS ring.

The **undo guard-timer** command restores the default value of the Guard timer.

By default, the Guard timer is 200 centiseconds in an ERPS ring.

Format

guard-timer *time-value*

undo guard-timer

Parameters

Parameter	Description	Value
time-value	Specifies the value of the Guard timer in an ERPS ring.	The value is an integer that ranges from 1 to 200, in centiseconds.

Views

ERPS ring view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On a Layer 2 network running ERPS, after a faulty link or node recovers, the device sends RAPS PDUs to inform the other nodes of link or node recovery and starts the Guard timer. Before the Guard timer expires, the device does not receive any RAPS PDU. If the device receives out-of-date RAPS PDUs indicating that the link or node fails, the local port may be blocked again. After the Guard timer expires, if the device receives an RAPS PDU indicating that another port fails, the local port enters the Forwarding state.

Precautions

If the value of the Guard timer is too small, network loops may occur. The default value (200 centiseconds) is recommended.

Example

# Set the Guard timer to 180 centiseconds in ERPS ring 10.

```
<HUAWEI> system-view
[HUAWEI] erps ring 10
[HUAWEI-erps-ring10] guard-timer 180
```

5.15.15 holdoff-timer (ERPS ring view)

Function

The **holdoff-timer** command sets the Holdoff timer in an ERPS ring.

The **undo holdoff-timer** command restores the default value of the Holdoff timer.

By default, the Holdoff timer is 0 deciseconds in an ERPS ring.

Format

holdoff-timer *time-value*

undo holdoff-timer

Parameters

Parameter	Description	Value
time-value	Specifies the value of the Holdoff timer in an ERPS ring.	The value is an integer that ranges from 0 to 100, in deciseconds.

Views

ERPS ring view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On Layer 2 networks running ERPS, there may be different requirements for protection switching. For example, on a network where multi-layer services are provided, after a server fails, users may require a period of time to rectify the server fault so that clients do not detect the fault. That is, protection switching is not performed immediately.

You can run the **holdoff-timer** command to set the Holdoff timer. When a fault occurs, the fault is not immediately reported to ERPS. Instead, the Holdoff timer starts. If the fault persists after the timer expires, the fault will be reported to ERPS.

Precautions

If you run the **holdoff-timer** command multiple times, only the latest configuration takes effect.

Example

# Set the Holdoff timer to 10 in ERPS ring 10.

```
<HUAWEI> system-view
[HUAWEI] erps ring 10
[HUAWEI-erps-ring10] holdoff-timer 10
```

5.15.16 port (ERPS ring view)

Function

The **port** command adds a port to an ERPS ring and specifies a role for the port.

The **undo port** command deletes a port from an ERPS ring and cancels the port role.

By default, a port is not added to an ERPS ring, and no port role is specified.

Format

port *interface-type interface-number* [**rpl** { **owner** | **neighbour** }]

undo port *interface-type interface-number*

Parameters

Parameter	Description	Value
interface-type interface-number	Specifies the port to be added to an ERPS ring. *interface-type* specifies the interface type and *interface-number* specifies the interface number.	-
rpl { **owner** | **neighbour** }	Specifies the port to be added to an ERPS ring as the RPL owner port or RPL neighbor port.	-

Views

ERPS ring view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After an ERPS ring is created, run the **port** command to add Layer 2 ports to the ERPS ring so that RAPS PDUs can be correctly forwarded. Each device in an ERPS ring is a node, and a maximum of two Layer 2 ports on each node can be added to the same ERPS ring.

ERPS defines three port roles: RPL owner port, RPL neighbor port (only in ERPSv2), and common port.

- RPL owner port

  An RPL owner port is responsible for blocking traffic over the Ring Protection Link (RPL) to prevent loops. An ERPS ring has only one RPL owner port.

  When the node on which the RPL owner port resides receives an RAPS PDU indicating a link or node fault in an ERPS ring, the node unblocks the RPL owner port. Then the RPL owner port can send and receive traffic to ensure nonstop traffic forwarding.

  The link where the RPL owner port resides is the RPL.

- RPL neighbor port

  An RPL neighbor port is directly connected to an RPL owner port.

  Both the RPL owner port and RPL neighbor ports are blocked in normal situations to prevent loops.

  If an ERPS ring fails, both the RPL owner and neighbor ports are unblocked.

  The RPL neighbor port helps reduce the number of FDB entry updates on the device where the RPL neighbor port resides.

- Common port

  Common ports are ring ports other than the RPL owner and neighbor ports.

  A common port monitors the status of the directly connected ERPS link and sends RAPS PDUs to notify the other ports of its link status changes.

Prerequisites

- The control VLAN and ERP instance have been configured using the **control-vlan** and **protected-instance** commands respectively in the ERPS ring view.
- The port is not a Layer 3 port. If the port is a Layer 3 port, run the **portswitch** command to switch the port to the Layer 2 mode.
- Spanning Tree Protocol (STP), Rapid Ring Protection Protocol (RRPP), Smart Ethernet Protection (SEP), or Smart Link is not enabled on the port.
  - If the port has STP enabled, run the **stp disable** command in the interface view to disable STP.
  - If the port has RRPP enabled, run the **undo ring** *ring-id* command in the RRPP domain view to disable RRPP.
  - If the port has SEP enabled, run the **undo sep segment** *segment-id* command in the interface view to disable SEP.
  - If the port has Smart Link enabled, run the **undo port** command in the Smart Link group view to disable Smart Link.
- ERPSv2 has been specified in the ERPS ring using the **version v2** command if the port is specified as an RPL neighbor port.

Precautions

Before deleting a port from an ERPS ring or changing the port role, use the **shutdown (interface view)** command to disable the port. Then remove the port or change the port role and run the **undo shutdown (interface view)** command to enable the port. Otherwise, traffic forwarding may fail.

If ports added to an ERPS ring are all ordinary ports, any port on the device with the largest MAC address will be blocked.

Example

# Add GE0/0/1 to ERPS ring 10, and set the port to the RPL owner port.

```
<HUAWEI> system-view
[HUAWEI] erps ring 10
[HUAWEI-erps-ring10] port gigabitethernet 0/0/1 rpl owner
```

5.15.17 protected-instance (ERPS ring view)

Function

The **protected-instance** command configures Ethernet ring protection (ERP) instances in an ERPS ring.

The **undo protected-instance** command deletes ERP instances from an ERPS ring.

By default, no ERP instance is configured in an ERPS ring.

Format

protected-instance { **all** | { *instance-id1* [**to** *instance-id2*] &<1-10> } }

undo protected-instance { **all** | { *instance-id1* [**to** *instance-id2*] &<1-10> } }

Parameters

Parameter	Description	Value
instance-id1 **to** *instance-id2*	Specifies the ID of an ERP instance. ● *instance-id1* specifies the first ERP instance ID. ● **to** *vlan-id2* specifies the last ERP instance ID. The value of *instance-id2* must be greater than the value of *instance-id1*. *instance-id1* and *instance-id2* identify a range of ERP instances. If **to** *instance-id2* is not specified, only *instance-id1* is specified.	The value is an integer that ranges from 0 to 4094.
all	Indicates all ERP instances.	-

Views

ERPS ring view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On a device running ERPS, the VLAN where ERPS PDUs and data packets are transmitted must be mapped to an ERP instance. Otherwise, VLAN packets may cause broadcast storms on the ring network. As a result, the network may become unavailable.

Precautions

- If the **stp mode (system view)** command is used to set the STP working mode to VLAN-based Spanning Tree (VBST), the ERP instance specified by the **protected-instance** command must be the created static instance.
- If you run the **protected-instance** command multiple times in the same ERPS ring, multiple ERP instances are configured.
- If ports have been added to the ERPS ring, the ERP instance cannot be modified. To delete the configured ERP instance, run the **undo erps ring** command in the interface view or the **undo port** command in the ERPS ring view to delete ports from the ERPS ring, and run the **undo protected-instance** command to delete the ERP instance.

Follow-up Procedure

Configure the mapping between protected instances and VLANs. The specific procedures are as follows:

1. Run the **stp region-configuration** command to enter the MST region view.

2. Run the **instance** *instance-id* **vlan** { *vlan-id* [**to** *vlan-id*] } &<1-10> command to configure the mapping relationship between the protected instance and the VLAN.

   The parameter *instance-id* in this command must the same as the parameter *instance-id* in the **protected-instance** command.

3. Run the **active region-configuration** command to activate the protected instance and the mapping relationship between the protected instance and the VLAN.

Example

# Configure ERP instance 5 in ERPS ring 1.

```
<HUAWEI> system-view
[HUAWEI] erps ring 1
[HUAWEI-erps-ring1] protected-instance 5
```

5.15.18 raps-mel

Function

The **raps-mel** command sets the value of the MEL field in Ring Auto Protection Switching (RAPS) Protocol Data Units (PDUs).

The **undo raps-mel** command restores the default value of the MEL field.

By default, the value of the MEL field in RAPS PDUs is 7.

Format

raps-mel *level-id*

undo raps-mel

Parameters

Parameter	Description	Value
level-id	Specifies the value of the MEL field in RAPS PDUs.	The value is an integer that ranges from 0 to 7.

Views

ERPS ring view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On a Layer 2 network running ERPS, if another fault detection protocol is enabled, the MEL field in RAPS PDUs is used to determine whether the RAPS PDUs can be forwarded. If the MEL value in an ERPS ring is smaller than the MEL value of the fault detection protocol, the RAPS PDUs have a lower priority and are discarded. If the MEL value in an ERPS ring is larger than the MEL value of the fault detection protocol, the RAPS PDUs can be forwarded. You can run the **raps-mel** command to set the value of the MEL field in RAPS PDUs.

In addition, the MEL value can also be used for interworking with other vendors' devices in an ERPS ring. The same MEL value ensures smooth communication between devices.

Precautions

If you run the **raps-mel** command multiple times, only the latest configuration takes effect.

Example

# Set the value of the MEL field to 5 in ERPS ring 1.

```
<HUAWEI> system-view
[HUAWEI] erps ring 1
[HUAWEI-erps-ring1] raps-mel 5
```

5.15.19 reset erps statistics

Function

The **reset erps statistics** command clears packet statistics in an ERPS ring.

Format

reset erps [**ring** *ring-id*] **statistics**

Parameters

Parameter	Description	Value
ring *ring-id*	Clears packet statistics in a specified ERPS ring.	The value is an integer that ranges from 1 to 255.

Views

All views

Default Level

3: Management level

Usage Guidelines

Usage Scenario

Before collecting traffic statistics on a specific interface in a given period of time, clear the existing statistics on the interface by using the **reset erps** command.

Prerequisites

The ERPS ring has been created, and ports have been added to the specified ERPS ring.

Precautions

The cleared statistics cannot be restored. Exercise caution when you run this command.

Example

# Clear packet statistics in ERPS ring 2.

```
<HUAWEI> reset erps ring 2 statistics
```

5.15.20 revertive

Function

The **revertive** command configures revertive switching or non-revertive switching in an ERPS ring. The switching mode determines whether the RPL owner port is blocked again after a link fault is rectified.

The **undo revertive disable** command restores the default configuration.

By default, ERPS rings use revertive switching.

Format

revertive { **enable** | **disable** }

undo revertive disable

Parameters

Parameter	Description	Value
enable	Enables revertive switching in an ERPS ring.	-
disable	Disables revertive switching. That is, non-revertive switching is used in an ERPS ring.	-

Views

ERPS ring view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After link faults in an ERPS ring are rectified, re-blocking the RPL owner port depends on the switching mode:

- In revertive switching, the RPL owner port is re-blocked after the WTR timer expires, and the RPL is blocked.
- In non-revertive switching, the WTR timer is not started, and the original faulty link is still blocked.

Prerequisites

The **version v2** command has been executed to specify ERPSv2.

Example

# Configure non-revertive switching in ERPS ring 5.

```
<HUAWEI> system-view
[HUAWEI] erps ring 5
[HUAWEI-erps-ring5] revertive disable
```

5.15.21 sub-ring

Function

The **sub-ring** command configures an ERPS ring as a sub-ring.

The **undo sub-ring** command restores the default configuration.

By default, all ERPS rings are major rings.

Format

sub-ring

undo sub-ring

Parameters

None

Views

ERPS ring view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

ERPS has two versions: ERPSv1 and ERPSv2. ERPSv2 supports multi-ring topologies such as intersecting ring topologies in addition to single-ring topologies.

To deploy ERPS on a multi-ring network, run the **sub-ring** command to configure some rings as sub-rings.

NOTE

Major rings are closed, and sub-rings are open.

Prerequisites

- The **version v2** command has been executed to specify ERPSv2.
- The ERPS ring does not have any port. If the ERPS ring has a port, run the **undo erps ring** *ring-id* or **undo port** *interface-type interface-number* command to delete the port from the ERPS ring.

Precautions

If a sub-ring uses the VC mode to transmit RAPS PDUs, you must run the **virtual-channel disable** command to restore the RAPS PDU transmission mode to NVC before running the **undo sub-ring** command to restore the sub-ring to a major ring.

Example

# Configure ERPS ring 5 as a sub-ring.

```
<HUAWEI> system-view
[HUAWEI] erps ring 5
[HUAWEI-erps-ring5] sub-ring
```

5.15.22 tc-notify erps ring

Function

The **tc-notify erps ring** command configures an ERPS ring to notify other ERPS rings of its topology change.

The **undo tc-notify erps ring** command disables the topology change notification function.

By default, an ERPS ring does not notify other ERPS rings of its topology change.

Format

tc-notify erps ring { *ring-id1* [**to** *ring-id2*] } &<1-10>

undo tc-notify erps ring { *ring-id1* [**to** *ring-id2*] } &<1-10>

Parameters

Parameter	Description	Value
ring-id1	Specifies the start ring ID of the ERPS ring that will be notified of the topology change.	The value is an integer that ranges from 1 to 255.

Parameter	Description	Value
to *ring-id2*	Specifies the end ring ID of the ERPS ring that will be notified of the topology change. *ring-id1* and *ring-id2* specify a ring range. If **to** *ring-id2* is not specified, an ERPS ring notifies only the ERPS ring specified by *ring-id1* of its topology change. **NOTE** You can specify the ring range for a maximum of 10 times, and the ring ranges can overlap.	The value is an integer that ranges from 1 to 255 and must be greater than or equal to *ring-id1*.

Views

ERPS ring view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the topology of the local ERPS ring changes and other ERPS rings is not notified of the topology change, the MAC address entries remain unchanged on the other ERPS rings and therefore user traffic is interrupted. To ensure nonstop traffic transmission, run the **tc-notify erps ring** command to specify ERPS rings to which topology change notifications are sent.

Prerequisites

The **version v2** command has been executed to specify ERPSv2.

Precautions

- The **tc-notify erps ring** command takes effect only on ERPS sub-rings.
- If an ERPS ring topology changes, the ERPS ring notifies the specified ERPS rings of its topology change. If the ERPS ring that has been specified to receive the topology change notification does not exist, the configuration does not take effect.
- After other ERPS rings receive the topology change notification from an ERPS ring, they send Flush-FDB messages on their separate rings to instruct their nodes to update MAC addresses. This ensures nonstop traffic transmission.
- If the **tc-notify erps ring** command is run more than once, all configurations take effect.

Example

# Configure ERPS ring 5 to notify ERPS rings 1 through 3 of its topology change.

```
<HUAWEI> system-view
[HUAWEI] erps ring 5
[HUAWEI-erps-ring5] tc-notify erps ring 1 to 3
```

5.15.23 tc-notify sep

Function

The **tc-notify sep** command configures the device to notify a SEP segment of topology changes in the ERPS ring so that the SEP segment can update the FDB in a timely manner.

The **undo tc-notify sep** command disables the topology change notification function.

By default, the device does not notify a SEP segment of topology changes in the ERPS ring.

Format

tc-notify sep { **segment** *segment-id* | **all-segment** }

undo tc-notify sep { **segment** *segment-id* | **all-segment** }

Parameters

Parameter	Description	Value
segment *segment-id*	Specifies the ID of a SEP segment.	The value is an integer in the range from 1 to 1024.
all-segment	Indicates all SEP segments.	-

Views

ERPS ring view

Default Level

2: Configuration level

Usage Guidelines

When the topology of the ERPS ring changes and SEP segments are not notified of the topology change, the MAC address entries remain unchanged on the SEP segments and therefore user traffic is interrupted. To ensure nonstop traffic transmission, you can run the **tc-notify sep** command to specify the objects to which ERPS ring topology change notifications are sent.

Example

# Configure the device to notify a SEP segment of topology changes in the ERPS ring.

```
<HUAWEI> system-view
[HUAWEI] sep segment 2
[HUAWEI-sep-segment2] quit
[HUAWEI] erps ring 5
[HUAWEI-erps-ring5] tc-notify sep segment 2
```

5.15.24 tc-protection interval (ERPS ring view)

Function

The **tc-protection interval** command sets the topology change protection interval at which topology change notification messages are sent.

The **undo tc-protection interval** command restores the default topology change protection interval.

By default, the topology change protection interval is 2s.

Format

tc-protection interval *interval-value*

undo tc-protection interval

Parameters

Parameter	Description	Value
interval-value	Specifies the topology change protection interval. A longer interval ensures stable ERPS operation, but may cause slow convergence.	The value is an integer that ranges from 1 to 600, in seconds.

Views

ERPS ring view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If a user terminal connects to an upper-layer network through multiple ERPS rings and the topology of the ERPS ring closest to the user terminal changes, topology change notifications will be multiplied by 2 each time they pass through a ring until they reach the upper-layer network. As a result, the upper-layer network receives many identical topology change notifications.

In addition, if an ERPS ring frequently receives topology change notifications, its nodes will have lower CPU processing capability and repeatedly update Flush-FDB packets, consuming much bandwidth. To prevent this problem, run the **tc-protection interval** command to set the topology change protection interval at which the maximum number of topology change notifications specified in the **tc-protection threshold** command are processed. Then, during the topology change protection interval, the device processes only the specified maximum number of topology change notification messages. If there are excess notifications, the device processes all the excess notifications once after the topology change protection interval elapses. For example, if the topology change protection interval is set to 10 seconds and the maximum number is set to 5, when a device receives topology change notifications, the device processes only the first 5 topology change notifications within 10 seconds and processes the subsequent topology change notifications only after 10s. This prevents the device from frequently deleting MAC address entries and ARP entries.

Prerequisites

The **erps ring** command has been executed to create an ERPS ring.

Precautions

Suppressing topology change notification transmission allows the upper-layer network to receive and process only one notification during the topology change protection interval and protects ERPS nodes against topology change (TC) attacks.

Example

# Set the topology change protection interval to 3s in ERPS ring 1.

```
<HUAWEI> system-view
[HUAWEI] erps ring 1
[HUAWEI-erps-ring1] tc-protection interval 3
```

5.15.25 tc-protection threshold (ERPS ring view)

Function

The **tc-protection threshold** command sets the number of times ERPS parses topology change notifications and updates forwarding entries in the topology change protection interval.

The **undo tc-protection threshold** command restores the default number of times ERPS parses topology change notifications and updates forwarding entries in the topology change protection interval.

By default, ERPS parses topology change notifications and updates forwarding entries three times in the topology change protection interval.

Format

tc-protection threshold *threshold-value*

undo tc-protection threshold

Parameters

Parameter	Description	Value
threshold-value	Specifies the number of times ERPS parses topology change notifications and updates forwarding entries in the topology change protection interval.	The value is an integer that ranges from 1 to 255.

Views

ERPS ring view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After a switching device in an ERPS ring network receives topology change notifications, the device updates MAC address entries and ARP entries. Frequent updates will cause a high CPU usage.

To prevent frequent MAC address and ARP entry updates, run the **tc-protection threshold** command to set the maximum number of topology change notifications that can be processed during the topology change protection interval specified by the **tc-protection interval** command. Then, during the topology change protection interval, the device processes only the specified maximum number of topology change notification messages. If there are excess notifications, the device processes all the excess notifications once after the topology change protection interval elapses. For example, if the topology change protection interval is set to 10 seconds and the maximum number is set to 5, when a device receives topology change notifications, the device processes only the first 5 topology change notifications within 10 seconds and processes the subsequent topology change notifications only after 10s. This prevents the device from frequently deleting MAC address entries and ARP entries.

Prerequisites

The **version v2** command has been run to specify ERPSv2.

Example

# Set the number of times ERPS parses topology change notifications and updates forwarding entries in the topology change protection interval to 5.

```
<HUAWEI> system-view
[HUAWEI] erps ring 5
[HUAWEI-erps-ring5] tc-protection threshold 5
```

5.15.26 version (ERPS ring view)

Function

The **version** command configures an ERPS version.

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

By default, ERPSv1 is used.

Format

version { **v1** | **v2** }

undo version

Parameters

Parameter	Description	Value
v1	Specifies ERPSv1.	-
v2	Specifies ERPSv2.	-

Views

ERPS ring view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

ERPS has two versions: ERPSv1 released by the ITU-T in June and ERPSv2 released in August, 2010. ERPSv2 that is compatible with ERPSv1 provides the following enhanced functions:

- Multi-ring topologies, such as intersecting rings
- RAPS PDU transmission on virtual channels (VCs) and non-virtual-channels (NVCs) in sub-rings
- Forced Switch (FS) and Manual Switch (MS)
- Revertive and non-revertive switching

To configure an ERPS version, run the **version** command.

Precautions

Before specifying ERPSv1 for an ERPSv2-enabled device, delete all ERPS configurations that ERPSv1 does not support. Otherwise, the version cannot be changed.

Example

# Specify ERPSv2 for ERPS ring 5.

```
<HUAWEI> system-view
[HUAWEI] erps ring 5
[HUAWEI-erps-ring5] version v2
```

5.15.27 virtual-channel

Function

The **virtual-channel enable** command configures the virtual channel (VC) mode for RAPS PDU transmission in a sub-ring.

The **virtual-channel disable** command configures the non-virtual-channel (NVC) mode for RAPS PDU transmission in a sub-ring.

The **undo virtual-channel enable** command configures the non-virtual-channel (NVC) mode for RAPS PDU transmission in a sub-ring.

By default, RAPS PDUs are transmitted in NVC mode in a sub-ring.

Format

virtual-channel { **enable** | **disable** }

undo virtual-channel enable

Parameters

Parameter	Description	Value
enable	Enables the VC mode for RAPS PDU transmission in a sub-ring.	-
disable	Disables the VC mode for RAPS PDU transmission in a sub-ring. That is, the NVC mode is used.	-

Views

ERPS ring view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

ERPSv2 supports both single- and multi-ring topologies.

In multi-ring topologies, the VC or NVC mode can be used to transmit RAPS PDUs in a sub-ring:

- VC mode: RAPS PDUs in a sub-ring are transmitted to the major ring by the intersecting node. The RPL owner port of the sub-ring blocks both RAPS PDUs and data traffic.
- NVC mode: RAPS PDUs in a sub-ring are terminated on the intersecting nodes. The RPL owner port of the sub-ring blocks data traffic but not RAPS PDUs.

You can run the **virtual-channel** command to configure the RAPS PDU transmission mode in a sub-ring.

Prerequisites

- The **version v2** command has been executed to specify ERPSv2.
- The **sub-ring** command has been executed to configure an ERPS ring as a sub-ring.

Configuration Impact

If a sub-ring uses the VC mode to transmit RAPS PDUs, you must run the **virtual-channel disable** or **undo virtual-channel enable** command to restore the RAPS PDU transmission mode to NVC before running the **undo sub-ring** command to restore the sub-ring to a major ring.

Example

# Configure the VC mode for RAPS PDU transmission in ERPS sub-ring 5.

```
<HUAWEI> system-view
[HUAWEI] erps ring 5
[HUAWEI-erps-ring5] version v2
[HUAWEI-erps-ring5] sub-ring
[HUAWEI-erps-ring5] virtual-channel enable
```

5.15.28 wtr-timer (ERPS ring view)

Function

The **wtr-timer** command sets the WTR timer in an ERPS ring.

The **undo wtr-timer** command restores the default value of the WTR timer.

By default, the WTR timer is 5 minutes in an ERPS ring.

Format

wtr-timer *time-value*

undo wtr-timer

Parameters

Parameter	Description	Value
time-value	Specifies the value of the WTR timer in an ERPS ring.	The value is an integer that ranges from 1 to 12, in minutes.

Views

ERPS ring view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **wtr-timer** command is applied to RPL owner ports. If an RPL owner port is unblocked due to a link or node fault, the involved port may not go Up immediately after the link or node recovers. To prevent the RPL owner port from alternating between the Up and Down states, the node where the RPL owner port resides starts the WTR timer after receiving an RAPS PDU indicating the link or node recovery:

- If the node receives an RAPS PDU indicating that another port fails before the timer expires, the node disables the WTR timer and enables the RPL owner port.
- If the node does not receive any RAPS PDUs indicating that another port fails before the timer expires, the node blocks the RPL owner port when the WTR timer expires and sends an RAPS PDU indicating that the RPL owner port is blocked. After receiving the RAPS PDU, other nodes set their recovering ports to the Forwarding state in the ring.

Precautions

If you run the **wtr-timer** command multiple times, only the latest configuration takes effect.

Example

# Set the WTR timer to 10 minutes in ERPS ring 10.

```
<HUAWEI> system-view
[HUAWEI] erps ring 10
[HUAWEI-erps-ring10] wtr-timer 10
```

5.16 Loopback Detection Configuration Commands

5.16.1 Command Support

Commands provided in this section and all the parameters in the commands are supported by all switch models (except the S5731-L and S5731S-L), unless otherwise specified. For details, see specific commands.

5.16.2 display loopback-detect

Function

The **display loopback-detect** command displays the loopback detection configuration and status of loopback detection enabled interfaces.

Format

display loopback-detect

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

This command is used to check the loopback detection configuration and status of each interface on which loopback detection is enabled.

Example

# Display the loopback detection configuration and status of loopback detection enabled interfaces.

```
<HUAWEI> display loopback-detect
Loopback-detect sending-packet interval:  5

(A): Auto Loopback-detect
------------------------------------------------------------------
Interface                    RecoverTime  Action     Status
------------------------------------------------------------------
GigabitEthernet0/0/1         30           quitvlan(A) NORMAL
------------------------------------------------------------------
```

Table 5-106 Description of the display loopback-detect command output

Item	Description
Loopback-detect sending-packet interval	Interval between sending loopback detection packets, in seconds. For details, see **loopback-detect packet-interval**.
Interface	Interface on which loopback detection is enabled.
RecoverTime	Interface recovery time, in seconds. For details, see **loopback-detect recovery-time**.

Item	Description
Action	Action performed when a loopback is detected on an interface: ● block: blocks the interface. After the interface is blocked, it is isolated from other interfaces and does not forward received data packets to other interfaces. ● nolearn: disables MAC address learning on the interface. When a loopback is detected on the interface, the interface stops learning MAC addresses. ● shutdown: shuts down the interface. When a loopback is detected on an interface, the interface is shut down. ● trap: only sends a trap. When a loopback is detected on an interface, the interface only sends a trap. ● trap(A): only sends a trap. (A) indicates that automatic loopback detection is performed on an interface. ● quitvlan: quits VLANs. When a loopback is detected on an interface, the interface exits from the VLAN in which a loop occurs. ● quitvlan(A): quits VLANs. (A) indicates that automatic loopback detection is performed on an interface. To specify the parameter, run the **loopback-detect action or loopback-detect auto action** command.
Status	Status of a loopback detection enabled interface: ● NORMAL: No loopback is detected on the interface. ● BLOCK: A loopback is detected on the interface and the interface is blocked. ● NOLEARN: A loopback is detected on the interface and the MAC address learning is disabled on the interface. ● SHUTDOWN: A loopback is detected on the interface and the interface is shut down. ● TRAP: A loopback is detected on the interface and a trap is sent. ● QUITVLAN: A loopback is detected on the interface and the interface exits from the VLAN in which a loop occurs.

5.16.3 display loopback-detect interface

Function

display loopback-detect interface command displays the LBDT configuration and status of LBDT-enabled interfaces.

Format

display loopback-detect interface *interface-type interface-number*

Parameters

Parameter	Description	Value
interface-type interface-number	Specifies the interface type and number.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

This command is used to check the loopback detection configuration and status of each interface on which loopback detection is enabled.

Example

# Display the LBDT configuration and status of interfaces that are enabled with LBDT manually.

```
<HUAWEI> display loopback-detect interface GigabitEthernet 0/0/1
LBDT mode   : Manual
Detect VLAN : Untag
Looped VLAN :
Action      : shutdown
Status      : NORMAL
Recover Time: 15
```

# Display the LBDT configuration and status of interfaces that are enabled with LBDT automatically.

```
<HUAWEI> display loopback-detect interface GigabitEthernet 0/0/1
LBDT mode    : Auto
PVID VLAN    :
  VLAN ID           : 1
  Trap only VLAN ID : -
Mac-flap VLAN:
  Total NUM         : 0
  VLAN ID           : -
```

```
Trap only VLAN NUM: 0
Trap only VLAN ID : -
Quit-vlan VLAN NUM: 0
Quit-vlan VLAN ID : -
```

Table 5-107 Description of the **display loopback-detect interface** command output

Item	Description
LBDT mode	Mode in which LBDT is enabled: ● Manual: LBDT is enabled manually. To enable LBDT on an interface, run the **loopback-detect enable (interface view)** command. ● Auto: LBDT is enabled automatically. To enable automatic LBDT on the device, run the **undo loopback-detect auto disable** command.
Detect VLAN	VLAN where LBDT is configured to detect loops. To configure a VLAN where LBDT is configured to detect loops, run the **loopback-detect packet vlan** command.
Looped VLAN	VLAN where loops are detected.
Action	Action performed when a loopback is detected on an interface: ● block: blocks the interface. After the interface is blocked, it is isolated from other interfaces and does not forward received data packets to other interfaces. ● nolearn: disables MAC address learning on the interface. When a loopback is detected on the interface, the interface stops learning MAC addresses. ● shutdown: shuts down the interface. When a loopback is detected on an interface, the interface is shut down. ● trap: only sends a trap. When a loopback is detected on an interface, the interface only sends a trap. ● quitvlan: quits VLANs. When a loopback is detected on an interface, the interface exits from the VLAN in which a loop occurs. To configure an action performed when a loopback is detected, run the **loopback-detect action** command.

Item	Description
Status	Status of a loopback detection enabled interface: ● NORMAL: No loopback is detected on the interface. ● BLOCK: A loopback is detected on the interface and the interface is blocked. ● NOLEARN: A loopback is detected on the interface and the MAC address learning is disabled on the interface. ● SHUTDOWN: A loopback is detected on the interface and the interface is shut down. ● TRAP: A loopback is detected on the interface and a trap is sent. ● QUITVLAN: A loopback is detected on the interface and the interface exits from the VLAN in which a loop occurs.
Recover Time	Restoration time of an interface, in seconds. To configure the restoration time of an interface, run the **loopback-detect recovery-time** command.
PVID VLAN	VLAN that is specified by the PVID and where automatic LBDT is enabled.
VLAN ID	Default VLAN of the interface. To configure the default VLAN of an interface, run the **port default vlan** command.
Trap only VLAN ID	VLAN that is specified by the PVID and where loops are detected. The value is displayed as - if there is no such a VLAN.
Mac-flap VLAN	VLAN where MAC address flapping detection is enabled automatically.
Total NUM	Total number of VLANs where MAC address flapping detection is enabled automatically to detect MAC address flapping.
VLAN ID	List of VLANs where MAC address flapping detection is enabled automatically to detect MAC address flapping.
Trap only VLAN NUM	Total number of VLANs where MAC address flapping detection is enabled automatically to detect MAC address flapping and the action is **trap**.
Trap only VLAN ID	List of VLANs where MAC address flapping detection is enabled automatically to detect MAC address flapping and the action is **trap**.

Item	Description
Quit-vlan VLAN NUM	Total number of VLANs where MAC address flapping detection is enabled automatically to detect MAC address flapping and the action is **quit-vlan**.
Quit-vlan VLAN ID	List of VLANs where MAC address flapping detection is enabled automatically to detect MAC address flapping and the action is **quit-vlan**.

5.16.4 loopback-detect action

Function

The **loopback-detect action** command configures an action to be taken when a loopback is detected on an interface.

The **undo loopback-detect action** command restores the default action.

By default, an interface is shut down when a loopback is detected on the interface.

Format

loopback-detect action { **block** | **nolearn** | **shutdown** | **trap** | **quitvlan** }

undo loopback-detect action [**block** | **nolearn** | **shutdown** | **trap** | **quitvlan**] (Ethernet interface view, GE interface view, XGE interface view, 40GE interface view, MultiGE interface view, 25GE interface view, 100GE interface view, Eth-Trunk interface view)

undo loopback-detect action (port group view)

Parameters

Parameter	Description	Value
block	Blocks an interface when a loopback is detected.	-
nolearn	Disables MAC address learning on an interface when a loopback is detected on the interface.	-
shutdown	Shuts down an interface when a loopback is detected on the interface.	-

Parameter	Description	Value
trap	Only sends a trap message when a loopback is detected.	-
quitvlan	The interface exits from the VLAN in which a loop occurs when a loopback is detected on an interface.	-

Views

Ethernet interface view, GE interface view, XGE interface view, 25GE interface view, 100GE interface view, 40GE interface view, MultiGE interface view, port group view, Eth-Trunk interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After loopback detection is enabled on an interface, the interface sends loopback detection packets at intervals. When a loopback is detected on the interface, the system performs an action to minimize the impact on the entire network. The **loopback-detect action** command configures the action.

The system performs any of the following actions after detecting a loopback on an interface:

- **block**: blocks the interface. After the interface is blocked, it is isolated from other interfaces and does not forward received data packets to other interfaces.
- **nolearn**: disables MAC address learning on the interface. When a loopback is detected on the interface, the interface stops learning MAC addresses.
- **shutdown**: shuts down the interface.
- **trap**: only sends a trap.
- **quitvlan**: When a loopback is detected on an interface, the interface exits from the VLAN in which a loop occurs.

Prerequisites

Enable loopback detection in the interface view or system view.

Follow-up Procedure

- If the action is set to **block**, **nolearn**, **trap** or **quitvlan**, you can run the **loopback-detect recovery-time** command to set the interface recovery time.

- If the action is set to **shutdown**, the shutdown interface cannot be automatically restored after a loopback is eliminated. You must run the **shutdown** and **undo shutdown** commands or run the **restart** command to enable the interface again. In addition to the preceding methods, the interface that is manually shut down or enters the Error-Down state due to other protocols will be automatically restored after the recovery time. However, the interface that is disabled only by LBDT cannot be restored after the recovery time.

Example

# Configure the system to shut down GigabitEthernet0/0/1 when a loopback occurs.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] loopback-detect action shutdown
```

5.16.5 loopback-detect auto action

Function

The **loopback-detect auto action** command specifies an action when automatic LBDT is triggered to detect loops in the VLAN where MAC address flapping is detected.

The **undo loopback-detect auto action** command restores the default action when automatic LBDT is triggered to detect loops in the VLAN where MAC address flapping is detected.

By default, the action is **trap** when automatic LBDT is triggered to detect loops in the VLAN where MAC address flapping is detected.

Format

loopback-detect auto action { **trap** | **quitvlan** }

undo loopback-detect auto action

Parameters

Parameter	Description	Value
trap	Indicates that the interface only sends a trap when loops are detected.	-
quitvlan	Indicates that the interface is removed from the VLAN where MAC address flapping is detected.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenarios

When the switch is configured with MAC address flapping detection and automatic LBDT, if MAC address flapping is detected in a VLAN, automatic LBDT is triggered to detect loops in the VLAN. Then you can run the **loopback-detect auto action** command to configure an action on the interface to minimize the impact of loops on the entire network.

When automatic LBDT is triggered to automatically detect loops in the VLAN where MAC address flapping is detected, you can configure either of the following actions on the interface:

- **trap**: The interface only sends a trap.
- **quitvlan**: The interface is removed from the VLAN where a loop occurs.

Prerequisites

- MAC address flapping detection has been enabled. For details on how to configure MAC address flapping detection, see Configuring MAC Address Flapping Detection.
- Automatic LBDT has been enabled using the **undo loopback-detect auto disable** command.

Follow-up Procedure

Run the **loopback-detect recovery-time** command to configure the recovery time of the problematic interface.

Precautions

The **quitvlan** action that is configured using this command takes effect only in the scenario where automatic LBDT is triggered to detect a loop between interfaces in the VLAN where MAC address flapping is detected. The **trap** action is used in the scenario where automatic LBDT is triggered to detect a loop on the downstream network or device in the VLAN where MAC address flapping is detected.

Example

# Configure the **quitvlan** action when automatic LBDT is triggered to detect loops in the VLAN where MAC address flapping is detected.

```
<HUAWEI> system-view
[HUAWEI] mac-address flapping detection
[HUAWEI] undo loopback-detect auto disable
[HUAWEI] loopback-detect auto action quitvlan
```

5.16.6 loopback-detect auto disable

Function

The **loopback-detect auto disable** command disables automatic LBDT.

The **undo loopback-detect auto disable** command enables automatic LBDT.

By default, automatic LBDT is enabled.

Format

loopback-detect auto disable

undo loopback-detect auto disable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When an interface changes from Down to Up, a loop may occur. You can enable automatic LBDT. The device then immediately detects loops and reports the corresponding alarm. When the switch is enabled with MAC address flapping detection, if MAC address flapping is detected, LBDT is triggered automatically to detect loops in the VLAN where MAC address flapping occurs.

Precautions

- When the switch is upgraded from an earlier version to V200R009 or later, automatic loop detection is disabled by default.
- The device enabled with automatic LBDT automatically reports an alarm when detecting a loop. After the loop is eliminated, the device automatically reports a clear alarm. The time for reporting a clear alarm is one or two times the recovery time. The recovery time can be configured using the **loopback-detect recovery-time** command. The default value is three detection intervals, that is, 15s.
- When automatic LBDT is enabled, all interfaces where the **loopback-detect enable** command is not configured periodically to send detection packets with the PVID to detect loops, consuming CPU resources. If no loop occurs on a network, run the **loopback-detect auto disable** command to disable automatic LBDT to reduce resource consumption.

Example

# Enable automatic LBDT.

```
<HUAWEI> system-view
[HUAWEI] undo loopback-detect auto disable
```

5.16.7 loopback-detect enable (system view)

Function

The **loopback-detect enable** command enables loopback detection on all interfaces.

The **undo loopback-detect enable** command disables loopback detection on all interfaces.

By default, loopback detection is disabled on all interfaces.

Format

loopback-detect enable

undo loopback-detect enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenarios

When loopback detection needs to be enabled on all or most of interfaces on a device, you can use the **loopback-detect enable** command to simplify configuration.

Precautions

After you run the **loopback-detect enable** command in the system view, the CPU usage increases because all interfaces send broadcast loopback detection packets at intervals.

Loopback detection occupies CPU resources; therefore, disable this function when it is not required.

Follow-up Procedure

If loopback detection is not required on an interface, run the **undo loopback-detect enable** command in the interface view to disable loopback detection.

Example

# Enable loopback detection on all interfaces.

```
<HUAWEI> system-view
[HUAWEI] loopback-detect enable
```

5.16.8 loopback-detect enable (interface view)

Function

The **loopback-detect enable** command enables loopback detection on an interface.

The **undo loopback-detect enable** command disables loopback detection on an interface.

By default, loopback detection is disabled on an interface.

Format

loopback-detect enable

undo loopback-detect enable

Parameters

None

Views

Ethernet interface view, GE interface view, XGE interface view, 40GE interface view, MultiGE interface view, 100GE interface view, 25GE interface view, port group view, Eth-Trunk interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenarios

The **loopback-detect enable** command enables loopback detection on an interface. This function enables the system to detect a loopback on the downstream network quickly and shut down an interface to minimize the impact of the loopback on the entire network.

Precautions

After loopback detection is enabled on an interface, the interface sends loopback detection packets at intervals.

A large number of broadcast packets are sent during loopback detection, occupying CPU resources; therefore, disable loopback detection if it is not required.

On the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S, manual LBDT can be configured on a maximum of 64 Eth-Trunks; on other models, manual LBDT can be configured on a maximum of 32 Eth-Trunks.

Example

# Enable loopback detection for the GE0/0/1 interface.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] loopback-detect enable
```

5.16.9 loopback-detect packet vlan

Function

The **loopback-detect packet vlan** command configures loopback detection in a specified VLAN.

The **undo loopback-detect packet vlan** command cancels the configuration.

By default, loopback detection is disabled in a VLAN.

Format

loopback-detect packet vlan { *vlan-id1* [**to** *vlan-id2*] } &<1-8>

undo loopback-detect packet vlan [{ *vlan-id1* [**to** *vlan-id2*] } &<1-8>]

Parameters

Parameter	Description	Value
vlan-id1 [**to** *vlan-id2*]	Specifies the VLAN IDs of loopback detection packets. ● *vlan-id1* specifies the start VLAN ID. ● **to** *vlan-id2* specifies the end VLAN ID. The value of *vlan-id2* must be greater than the value of *vlan-id1*.	● The value of *vlan-id1* is an integer that ranges from 1 to 4094. ● The value of *vlan-id2* is an integer that ranges from 1 to 4094. ● Each interface can send detection packets with a maximum of 32 VLAN IDs.

Views

Ethernet interface view, GE interface view, XGE interface view, 40GE interface view, MultiGE interface view, 100GE interface view, 25GE interface view, port group view, Eth-Trunk interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

By default, loopback detection is disabled in VLANs. After the **loopback-detect packet vlan** command is executed on an interface, the interface sends multiple copies of tagged loopback detection packets with the specified VLAN tags.

Prerequisites

The specified VLANs exist and the interface has been added to the VLANs in tagged mode.

Before running this command, check whether loopback detection is enabled. If not, run the **loopback-detect enable (interface view)** command to enable loopback detection.

Precautions

If you run the **loopback-detect packet vlan** command multiple times in the same interface view, multiple VLAN IDs are specified.

Each interface can send detection packets with a maximum of 32 VLAN IDs.

Example

# Configure loopback detection in VLAN30 on the GE0/0/1 interface.

```
<HUAWEI> system-view
[HUAWEI] vlan 30
[HUAWEI-vlan30] quit
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] port link-type trunk
[HUAWEI-GigabitEthernet0/0/1] port trunk allow-pass vlan 30
[HUAWEI-GigabitEthernet0/0/1] loopback-detect enable
[HUAWEI-GigabitEthernet0/0/1] loopback-detect packet vlan 30
```

5.16.10 loopback-detect packet-interval

Function

The **loopback-detect packet-interval** command sets the interval between sending loopback detection packets on all interfaces.

The **undo loopback-detect packet-interval** command restores the default interval between sending loopback detection packets on all interfaces.

By default, the interval between sending loopback detection packets is 5 seconds.

Format

loopback-detect packet-interval *packet-interval-time*

undo loopback-detect packet-interval [*packet-interval-time*]

Parameters

Parameter	Description	Value
packet-interval-time	Specifies the interval between sending loopback detection packets.	The value is an integer that ranges from 1 to 300, in seconds.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenarios

After loopback detection is enabled on an interface, the interface sends loopback detection packets at the interval specified by the **loopback-detect packet-interval** command. You can run the **loopback-detect packet-interval** command to adjust the interval between sending loopback detection packets according to service requirements. If a shorter interval is set, the system sends more loopback detection packets in a certain period. This enables the system to detect loopbacks more quickly and accurately, but more system sources are consumed.

Precautions

If you run the **loopback-detect packet-interval** command multiple times, only the latest configuration takes effect.

After a loopback detection-enabled interface recovers from Down to Up, the interface sends loopback detection packets immediately.

Example

# Set the interval between sending loopback detection packets on all interfaces to 10s.

```
<HUAWEI> system-view
[HUAWEI] loopback-detect packet-interval 10
```

5.16.11 loopback-detect recovery-time

Function

The **loopback-detect recovery-time** command sets the interface recovery time after a loopback is detected.

The **undo loopback-detect recovery-time** command restores the interface recovery time after a loopback is detected.

The default recovery time is three times the loopback detection interval.

Format

loopback-detect recovery-time *recovery-time*

undo loopback-detect recovery-time [*recovery-time*] (Ethernet interface view, GE interface view, XGE interface view, 40GE interface view, MultiGE interface view, 25GE interface view, 100GE interface view, Eth-Trunk interface view)

undo loopback-detect recovery-time (port group view)

Parameters

Parameter	Description	Value
recovery-time	Interface recovery time.	The value is an integer that ranges from 1 to 1000, in seconds.

Views

Ethernet interface view, GE interface view, XGE interface view, 40GE interface view, MultiGE interface view, 100GE interface view, 25GE interface view, port group view, Eth-Trunk interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenarios

After loopback detection is enabled on an interface, the device sends loopback detection packets at intervals through the interface, performs the preconfigured action on the interface after a loopback is detected, and starts timing. You can configure the interface recovery time. After the configured interface recovery time, the system will attempt to recover the interface. If the loopback is removed on the interface, the system recovers the interface from the error-down state.

Precautions

If you run the **loopback-detect recovery-time** command multiple times, only the latest configuration takes effect.

After a loop is eliminated, the interface recovery time is the same as the value of *recovery-time* or two times the value of *recovery-time*.

It is recommended that the interface recovery time be three times the packet sending interval. If the packet sending interval has been set to a small value, the interface recovery time should be at least 10 seconds longer than the packet sending interval.

If the action is set to **shutdown**, the shutdown interface cannot be automatically restored after a loopback is eliminated. You must run the **shutdown** and **undo shutdown** commands or run the **restart** command to enable the interface again. In addition to the preceding methods, the interface that is manually shut down or enters the Error-Down state due to other protocols will be automatically restored after the recovery time. However, the interface that is disabled only by LBDT cannot be restored after the recovery time.

NOTE

The default recovery time is three times the loopback detection interval and is not restricted by the value ranging from 1 to 1000. If you configure the command manually, the recovery time can only be set to a value from 1 to 1000.

Example

# Sets the recovery time of the GE0/0/1 interface to 50 seconds.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] loopback-detect recovery-time 50
```

5.16.12 loopback-detect untagged mac-address

Function

The **loopback-detect untagged mac-address** command sets the destination MAC address of untagged loopback detection packets.

The **undo loopback-detect untagged mac-address** command restores the default destination MAC address of untagged loopback detection packets.

By default, the destination MAC address of untagged loopback detection packets is **0180-C200-000A**.

Format

loopback-detect untagged mac-address *mac-address*

undo loopback-detect untagged mac-address [*mac-address*]

Parameters

Parameter	Description	Value
mac-address *mac-address*	Specifies the destination MAC address of untagged loopback detection packets.	The destination MAC address can only be a broadcast MAC address or a multicast MAC address.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **loopback-detect untagged mac-address** command applies to scenarios with self-loops and loops on the downstream network. When the connected interfaces are access interfaces, run the **loopback-detect packet vlan** command to configure the device to detect loops in a specified VLAN. This is because untagged packets are processed only when the transmit interface receives them. If the device is not configured to detect loops in a specified VLAN, run the **loopback-detect untagged mac-address** command.

Prerequisites

Loopback detection has been enabled using the **loopback-detect enable (system view)** command.

Precautions

If you run this command multiple times, only the latest configuration takes effect.

You are not advised to set the destination MAC address of untagged loopback detection packets to a destination MAC address of other protocols but to the broadcast MAC address **FFFF-FFFF-FFFF**.

Example

# Set the destination MAC address of untagged loopback detection packets to **FFFF-FFFF-FFFF**.

```
<HUAWEI> system-view
[HUAWEI] loopback-detect enable
[HUAWEI] loopback-detect untagged mac-address ffff-ffff-ffff
```

5.17 Layer 2 Protocol Tunneling Commands

5.17.1 Command Support

Commands provided in this section and all the parameters in the commands are supported by all switch models (except the S5731-L and S5731S-L), unless otherwise specified. For details, see specific commands.

5.17.2 bpdu

Function

The **bpdu** command configures an interface to send received BPDUs to the CPU or discard BPDUs.

By default, an interface sends received BPDUs to the CPU.

Format

bpdu { **disable** | **enable** }

undo bpdu disable

Parameters

Parameter	Description	Value
disable | **enable**	Indicates the action that an interface performs on BPDUs. ● **disable**: The interface discards BPDUs. ● **enable**: The interface sends BPDUs to the CPU.	-

Views

Ethernet interface view, GE interface view, XGE interface view, 25GE interface view, 40GE interface view, MultiGE interface view, port group view, Eth-Trunk interface view

Default Level

2: Configuration level

Usage Guidelines

After you run the **bpdu enable** command on an interface, the interface forwards a packet to the CPU if the destination MAC address of the packet is the BPDU MAC address. You can use the **display bpdu mac-address** command to view the BPDU MAC address.

NOTE

This command is not supported by the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S2730S-S, S5735-L-I, S5735-L1, S300, S5735-L, S5735S-L1, S5735S-L, S5735S-L-M, S5735-S, S500, S5735-S-I, S5735S-S, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S.

On the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S, an interface directly discards BPDUs by default. If BPDUs of a protocol need to be sent to the CPU for processing, enable the function of this protocol. For example, if STP BPDUs need to be sent to the CPU for processing, enable STP globally and on interfaces.

On the S200, S2730S-S, S5735-L-I, S5735-L1, S300, S5735-L, S5735S-L1, S5735S-L, S5735S-L-M, S500, S5735-S, S5735-S-I, and S5735S-S, an interface directly discards BPDUs except EAPoL packets by default. If BPDUs of a protocol need to be sent to the CPU for processing, enable the function of this protocol. For example, if STP BPDUs need to be sent to the CPU for processing, enable STP globally and on interfaces. EAPoL packets are forwarded by default. To enable a switch to discard EAPoL packets, run the **bpdu packet-type eapol discard** command on the switch.

Example

# Enable Eth-Trunk 1 to send received BPDUs to the CPU.

```
<HUAWEI> system-view
[HUAWEI] interface eth-trunk 1
[HUAWEI-Eth-Trunk1] bpdu enable
```

5.17.3 bpdu dmac

Function

The **bpdu dmac** command configures actions taken on packets with a specified destination MAC address and protocol number.

The **undo bpdu dmac** command restores the default configurations.

By default, no action is taken on packets with a specified destination MAC address and protocol number.

NOTE

S1730S-S1, S200, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S do not support this command.

Format

bpdu dmac *mac-address* **eth-type** *type* **action encapsulate**

undo bpdu dmac *mac-address* **eth-type** *type* **action** [**encapsulate**]

Parameters

Parameter	Description	Value
dmac *mac-address*	Specifies a destination MAC address.	The value is in H-H-H format. An H contains four hexadecimal digits. The value cannot be 0000-0000-0000.
eth-type *type*	Specifies the protocol type of Ethernet packets.	The value is a hexadecimal integer that ranges from 0 to FFFF.
action	Specifies the action taken on received packets.	-
encapsulate	Encapsulates packets.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

To be compatible with devices of other vendors, run this command to configure actions taken on packets with a specified destination MAC address and protocol number. Actions is encapsulating packets.

Example

# Configure the device to forward packets with the destination MAC address 0100-0ccc-cccc and protocol number 0101.

```
<HUAWEI> system-view
[HUAWEI] bpdu dmac 0100-0ccc-cccc eth-type 0101 action encapsulate
```

5.17.4 bpdu mac-address

Function

The **bpdu mac-address** command sets the MAC address of BPDUs.

The **undo bpdu mac-address** command cancels the configuration.

Format

bpdu mac-address *mac-address* [*mac-address-mask*]

undo bpdu mac-address *mac-address* [*mac-address-mask*]

Parameters

Parameter	Description	Value
mac-address [*mac-address-mask*]	Specifies the MAC address and mask of BPDUs.	The first digit of the MAC address must be 0 and the second digit must be an odd number, for example, 03XX-XXXX-XXXX and 0fXX-XXXX-XXXX. The mask of the MAC address must consist of consecutive fs and 0s, for example, ffff-ffff-ff00 and ffff-fff0-0000. **NOTE** ● To enable the device to forward packets destined for 0100-0ccc-cccc by using hardware, run the **undo bpdu mac-address** command to cancel the BPDU MAC address configuration. ● Only addresses of 0100-0ccc-cccc, 0100-0ccc-cccd, and 0118-8255-5555 can be configured as BPDU MAC addresses on the S1720GW-E, S1720GWR-E, S5720I-SI, S5720-LI, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5720S-LI, S5735-S, S500, S5735S-S, S5735-S-I, S5735S-H, S5736-S, and S6720S-S.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A Bridge Protocol Data Unit (BPDU) uses a special reserved multicast MAC address. An interface can send and receive BPDUs regardless of whether the interface is blocked. By default, the switch does not forward BPDUs at Layer 2.

NOTE

Sometimes, bridge protocol packets of the devices from other vendors need to be processed as BPDUs. You can set the MAC address of such packets to the MAC address of BPDUs.

Prerequisites

Before running the **undo bpdu mac-address** *mac-address* [*mac-address-mask*] command to delete a specified BPDU MAC address, delete all BPDU mac-addresses on the network segment. Then, run the **bpdu mac-address mac-address** [*mac-address-mask*] command to add the bpdu mac-address that does not need to be deleted.

Example

# Set the MAC address of BPDUs to 0100-0ccc-cccd.

```
<HUAWEI> system-view
[HUAWEI] bpdu mac-address 0100-0ccc-cccd
```

# Delete the MAC address 0180-c200-0003 as the BPDU MAC address.

```
<HUAWEI> system-view
[HUAWEI] undo bpdu mac-address 0180-c200-0000 ffff-ffff-fff0
[HUAWEI] bpdu mac-address 0180-c200-0000 FFFF-FFFF-FFFE
[HUAWEI] bpdu mac-address 0180-c200-0002 FFFF-FFFF-FFFF
[HUAWEI] bpdu mac-address 0180-c200-0004 FFFF-FFFF-FFFC
[HUAWEI] bpdu mac-address 0180-c200-0008 FFFF-FFFF-FFF8
```

5.17.5 bpdu packet-type eapol discard

Function

The **bpdu packet-type eapol discard** command configures the switch to discard EAPoL packets.

The **undo bpdu packet-type eapol discard** command configures the switch to transparently transmit EAPoL packets.

By default, the switch transparently transmits EAPoL packets.

NOTE

Only the following switch models support this command:

S200, S2730S-S, S5735-L-I, S5735-L1, S300, S5735-L, S5735S-L1, S5735S-L, S5735S-L-M, S500, S5735-S, S5735S-S, S5735-S-I

Format

bpdu packet-type eapol discard

undo bpdu packet-type eapol discard

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Assume that the 802.1X authentication point is deployed at the aggregation or upper layer and the access device functions only as a Layer 2 transparent transmission access device. In such networking, to enable the access device to transparently transmit EAPoL packets to the upper-layer authentication point device, run the **undo bpdu packet-type eapol discard** command on the access device. If the access device does not need to transparently transmit EAPoL packets to the upper-layer authentication point device, run the **bpdu packet-type eapol discard** command on the access device.

Precautions

The **l2protocol-tunnel enable** command takes precedence over the **bpdu packet-type eapol discard** command. If the **bpdu packet-type eapol discard** command is run on a device to discard EAPoL packets and then the **l2protocol-tunnel enable** command is run on an interface to enable the interface to transparently transmit Layer 2 protocol packets, this interface can transparently transmit EAPoL packets.

Example

# Enable the device to discard EAPoL packets.

```
<HUAWEI> system-view
[HUAWEI] bpdu packet-type eapol discard
```

5.17.6 bpdu-tunnel stp bridge role provider

Function

The **bpdu-tunnel stp bridge role provider** command configures the switch as a provider on the network.

The **undo bpdu-tunnel stp bridge role provider** command configures the switch as a customer on the network.

By default, the switch is a customer on the network.

NOTE

Only the S6720S-S, S5735S-H, S5736-S, S5720I-SI, S5735-S, S5735S-S, and S5735-S-I support this command.

Format

bpdu-tunnel stp bridge role provider

undo bpdu-tunnel stp bridge role provider

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

If the switch is configured as a customer, the well-known destination MAC address of the transmitted BPDU packets is 01-80-C2-00-00-00.

If the switch is configured as a provider, the well-known destination MAC address of the transmitted BPDU packets is 01-80-C2-00-00-08. The provider directly forwards the BPDU packets created by the customer, instead of sending the packets to the CPU.

If the **bpdu-tunnel stp bridge role provider** and **l2protocol-tunnel** commands are configured simultaneously, the **l2protocol-tunnel** command preferentially takes effect.

Example

# Configure the switch as a provider on the network.

```
<HUAWEI> system-view
[HUAWEI] bpdu-tunnel stp bridge role provider
```

5.17.7 display bpdu mac-address

Function

The **display bpdu mac-address** command displays the MAC addresses of BPDUs.

Format

display bpdu mac-address

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

A Bridge Protocol Data Unit (BPDU) uses a special reserved multicast MAC address. An interface can send and receive BPDUs regardless of whether the interface is blocked. By default, the switch does not forward BPDUs at Layer 2.

Sometimes, bridge protocol packets of the devices from other vendors need to be processed as BPDUs. You can set the MAC address of such packets to the MAC address of BPDUs.

This command displays the MAC addresses of BPDUs.

Example

# Display the MAC addresses of BPDUs.

```
<HUAWEI> display bpdu mac-address
 Remaining configurable number: 126
 ------------------------------------------------------------------------------
 (001) 0100-0ccc-cccc                 (002) 0100-0ccc-cccd
```

Table 5-108 Description of the display bpdu mac-address command output

Item	Description
Remaining configurable number	Number of remaining MAC addresses that you can specify for BPDUs.

5.17.8 display bpdu-tunnel global config

Function

The **display bpdu-tunnel global config** command displays the role of a device on the network and the multicast MAC address of STP BPDUs.

NOTE

Only the S6720S-S, S5735S-H, S5736-S, S5720I-SI, S5735-S, S5735S-S, and S5735-S-I support this command.

Format

display bpdu-tunnel global config

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

To check the role of a device on the network and the multicast MAC address of STP BPDUs, you can use the **display bpdu-tunnel global config** command.

Example

# Display the role of a device on the network and multicast MAC address of STP BPDUs.

```
<HUAWEI> display bpdu-tunnel global config
BridgeRole      customer
GroupMac        0100-5e00-0011
```

Table 5-109 Description of the display bpdu-tunnel global config command output

Item	Description
BridgeRole	Device role on a network. The roles are classified into two types: ● Customer: The well-known destination MAC address of the BPDUs generated by the customer is 01-80-C2-00-00-00. This is the default type. ● Provider: The well-known destination MAC address of the BPDUs generated by the provider is 01-80-C2-00-00-08. To specify the parameter, run the **bpdu-tunnel stp bridge role provider** command.
GroupMac	Multicast MAC address of STP BPDUs. To specify the parameter, run the **l2protocol-tunnel group-mac** command.

5.17.9 display l2protocol-tunnel group-mac

Function

The **display l2protocol-tunnel group-mac** command displays transparent transmission information about all standard Layer 2 protocols or a specified Layer 2 protocol.

Format

display l2protocol-tunnel group-mac { **all** | *protocol-type* | **user-defined-protocol** *protocol-name* }

Parameters

Parameter	Description	Value
all	Displays transparent transmission information about all standard Layer 2 protocols and user-defined Layer 2 protocols.	-

Parameter	Description	Value
protocol-type	Displays transparent transmission information about a specified Layer 2 protocol.	The protocol type can be: ● Spanning Tree Protocol (STP) ● Link Aggregation Control Protocol (LACP) ● Ethernet Operation, Administration, and Maintenance 802.3ah (EOAM3ah) ● Link Layer Discovery Protocol (LLDP) ● GARP VLAN Registration Protocol (GVRP) ● GARP Multicast Registration Protocol (GMRP) ● HUAWEI Group Management Protocol (HGMP) ● VLAN Trunking Protocol (VTP) ● Unidirectional Link Detection (UDLD) ● Port Aggregation Protocol (PAGP) ● Cisco Discovery Protocol (CDP) ● Per VLAN Spanning Tree Plus (PVST+) ● Shared Spanning Tree Protocol (SSTP) ● Dynamic Trunking Protocol (DTP) ● Device Link Detection Protocol (DLDP) ● Ethernet Synchronization Message Channel (ESMC)

Parameter	Description	Value
user-defined-protocol *protocol-name*	Displays transparent transmission information about a user-defined protocol. *protocol-name* specifies the name of a user-defined protocol.	The name is in the format of character strings. It is case-insensitive without spaces. The value ranges from 1 to 31. When double quotation marks are used around the string, spaces are allowed in the string.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After configuring Layer 2 protocol tunneling, you can run this command to check transparent transmission information about all standard Layer 2 protocols or a specified Layer 2 protocol.

Example

# Display transparent transmission information about the STP protocol.

```
<HUAWEI> display l2protocol-tunnel group-mac stp
Protocol  EncapeType  ProtocolType   Protocol-MAC    Group-MAC       Pri
-----------------------------------------------------------------------------------------
stp       llc          dsap 0x42    0180-c200-0000   0100-0ccd-cdd0  0
                      ssap 0x42
```

Table 5-110 Description of the display l2protocol-tunnel group-mac command output

Item	Description
Protocol	Name of a Layer 2 protocol whose packets are transparently transmitted.
EncapeType	Encapsulation types of protocols. At present, the encapsulation types of protocol packets can be Ethernet II, SNAP and LLC.
ProtocolType	Type of a Layer 2 protocol whose packets are transparently transmitted.

Item	Description
Protocol-MAC	Multicast destination MAC address of transparently transmitted Layer 2 protocol packets.
Group-MAC	Group MAC address of transparently transmitted Layer 2 protocol packets. It is a multicast MAC address that replaces the original multicast destination MAC address of transparently transmitted Layer 2 protocol packets.
Pri	Priority of transparently transmitted Layer 2 protocol packets.

5.17.10 display l2protocol-tunnel statistics

Function

The **display l2protocol-tunnel statistics** command displays statistics about Layer 2 protocol packets that are transparently transmitted on a specified interface.

Format

display l2protocol-tunnel statistics *interface-type interface-number* [{ *protocol-type* } &<1-16> | **user-defined-protocol** *protocol-name*]

Parameters

Parameter	Description	Value
interface-type interface-number	Displays statistics about Layer 2 protocol packets that are transparently transmitted on a specified interface. ● *interface-type* specifies the type of an interface. ● *interface-number* specifies the number of an interface. When specifying an interface in the command, ensure that Layer 2 protocol tunneling is enabled on the interface.	-

Parameter	Description	Value
protocol-type	Displays statistics about a specified protocol.	The protocol type can be: ● Spanning Tree Protocol (STP) ● Link Aggregation Control Protocol (LACP) ● Ethernet Operation, Administration, and Maintenance 802.3ah (EOAM3ah) ● Link Layer Discovery Protocol (LLDP) ● GARP VLAN Registration Protocol (GVRP) ● GARP Multicast Registration Protocol (GMRP) ● HUAWEI Group Management Protocol (HGMP) ● VLAN Trunking Protocol (VTP) ● Unidirectional Link Detection (UDLD) ● Port Aggregation Protocol (PAGP) ● Cisco Discovery Protocol (CDP) ● Per VLAN Spanning Tree Plus (PVST+) ● Shared Spanning Tree Protocol (SSTP) ● Dynamic Trunking Protocol (DTP) ● Device Link Detection Protocol (DLDP) ● Ethernet Synchronization Message Channel (ESMC) You can select one or more Layer 2 protocols.

Parameter	Description	Value
user-defined-protocol *protocol-name*	Displays statistics about transparently transmitted packets of a user-defined protocol. *protocol-name* specifies the name of a user-defined protocol.	The value is a string of 1 to 31 characters without spaces. When double quotation marks are used around the string, spaces are allowed in the string.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After configuring Layer 2 protocol tunneling, you can run this command to view statistics about transparently transmitted packets of a specified Layer 2 protocol. The command output includes:

- Number of Layer 2 protocol packets received by the inbound interface
- Number of Layer 2 protocol packets sent from the outbound interface
- Number of Layer 2 protocol packets discarded when the threshold is exceeded

According to the output information, you can collect traffic statistics and locate faults on the interface.

When an interface transparently transmits packets of multiple Layer 2 protocols, it is recommended that you specify the optional parameters or a regular expression in the command to filter the output information. Otherwise, too much information will be displayed, causing the following problems:

- The displayed information is repeatedly refreshed, causing desired information unable to be located.
- The system does not respond because of prolonged information traversing and searching.

When using this command, pay attention to the following points:

- If no optional parameter is specified, statistics about all Layer 2 protocol packets transparently transmitted on the specified interface are displayed.
- If *protocol-type* is specified, statistics about packets of the specified Layer 2 protocol that are transparently transmitted on the specified interface are displayed.
- If **user-defined-protocol** is specified, statistics about packets of the specified user-defined Layer 2 protocol that are transparently transmitted on the specified interface are displayed.

Example

# Display statistics about transparently transmitted STP and HGMP protocol packets.

```
<HUAWEI> display l2protocol-tunnel statistics GigabitEthernet 0/0/1 stp hgmp
-------------------------------------------------------------------------------
Port             Protocol        Drop      Input      Output     Drop
                             Threshold  Packets    Packets    Packets
-------------------------------------------------------------------------------
GE0/0/1           stp            100       12345      67890      1235
```

Table 5-111 Description of the display l2protocol-tunnel statistics command output

Item	Description
Port	Name of an interface on which Layer 2 protocol tunneling is enabled.
Protocol	Name of a Layer 2 protocol whose packets are transparently transmitted.
Drop Threshold	Drop threshold of transparently transmitted Layer 2 protocol packets. The drop threshold is set by using the **l2protocol-tunnel drop-threshold** command. The unit is packet per second (pps). When the rate of incoming Layer 2 protocol packets on an interface exceeds the threshold, the interface discards excess packets.
Input Packets	Number of incoming Layer 2 protocol packets on the interface enabled with Layer 2 protocol tunneling.
Output Packets	Number of outgoing Layer 2 protocol packets on the interface enabled with Layer 2 protocol tunneling.
Drop Packets	Number of Layer 2 protocol packets discarded on the interface after the traffic rate exceeds the drop threshold.

5.17.11 display l2protocol-tunnel statistics group-mac

Function

The **display l2protocol-tunnel statistics group-mac** command displays statistics about transparently transmitted Layer 2 PDUs whose multicast destination MAC addresses are replaced with a specified destination MAC address (group MAC address) on an interface.

Format

display l2protocol-tunnel statistics group-mac *interface-type interface-number*

Parameters

Parameter	Description	Value
interface-type interface-number	Specifies the interface on which the statistics about transparently transmitted Layer 2 PDUs whose multicast destination MAC addresses are replaced with a specified group MAC address are to be displayed. ● *interface-type* specifies the type of the interface. ● *interface-number* specifies the number of the interface.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After configuring Layer 2 protocol tunneling based on an interface, VLAN, or QinQ on a device, you can run the **display l2protocol-tunnel statistics group-mac** command to check statistics about transparently transmitted Layer 2 PDUs whose multicast destination MAC addresses are replaced with a specified group MAC address on an interface. The command output includes:

- Number of Layer 2 PDUs received by the interface
- Number of Layer 2 PDUs dropped by the interface due to queue resource exhaustion
- Number of Layer 2 PDUs dropped by the interface due to queue execution timeout

The command output helps you locate interface faults.

Example

# Display statistics about transparently transmitted Layer 2 PDUs whose multicast destination MAC addresses are replaced with a specified group MAC address on GE 0/0/1.

```
<HUAWEI> display l2protocol-tunnel statistics group-mac GigabitEthernet 0/0/1
------------------------------------------------------------------------------------------
 Port                 Group-Mac          Input           QueueFull         TimeOut
                                       Packets         DropPackets       DropPackets
 ------------------------------------------------------------------------------------------
 GE0/0/1                0100-0ccd-cdd0     8942            0               8651
                      0100-0ccd-cd2d     232            0               161
                      0100-0ccd-cd29     242            0               181
                      0100-0ccd-cd26     228            0               166
                      0100-0ccd-cd22     277            0               206
                      0100-0ccd-cd19     254            0               184
                      0100-0ccd-cd0c     278            0               203
```

Table 5-112 Description of the **display l2protocol-tunnel statistics group-mac** command output

Item	Description
Port	Interface name
Group-Mac	Multicast MAC address
Input Packets	Number of Layer 2 PDUs received by the interface
QueueFull DropPackets	Number of Layer 2 PDUs dropped by the interface due to queue resource exhaustion
TimeOut DropPackets	Number of Layer 2 PDUs dropped by the interface due to queue execution timeout

5.17.12 l2protocol-tunnel

Function

The **l2protocol-tunnel enable** command enables Layer 2 protocol tunneling on an interface.

The **undo l2protocol-tunnel enable** command disables Layer 2 protocol tunneling on an interface.

The **l2protocol-tunnel disable** command disables Layer 2 protocol tunneling on an interface.

By default, Layer 2 protocol tunneling is disabled on an interface.

Format

l2protocol-tunnel { **all** | { *protocol-type* } &<1-16> | **user-defined-protocol** *protocol-name* } **enable**

l2protocol-tunnel { **all** | { *protocol-type* } &<1-16> | **user-defined-protocol** *protocol-name* } **disable**

undo l2protocol-tunnel { { *protocol-type* } &<1-16> | **user-defined-protocol** *protocol-name* } **enable**

Parameters

Parameter	Description	Value
all	Enables or disables transparent transmission of packets of all standard Layer 2 protocols and user-defined Layer 2 protocols.	-

Parameter	Description	Value
protocol-type	Enables or disables transparent transmission of packets of a specified Layer 2 protocol.	The protocol type can be: ● Spanning Tree Protocol (STP) ● Link Aggregation Control Protocol (LACP) ● Ethernet Operation, Administration, and Maintenance 802.3ah (EOAM3ah) ● Link Layer Discovery Protocol (LLDP) ● GARP VLAN Registration Protocol (GVRP) ● GARP Multicast Registration Protocol (GMRP) ● HUAWEI Group Management Protocol (HGMP) ● VLAN Trunking Protocol (VTP) ● Unidirectional Link Detection (UDLD) ● Port Aggregation Protocol (PAGP) ● Cisco Discovery Protocol (CDP) ● Per VLAN Spanning Tree Plus (PVST+) ● Shared Spanning Tree Protocol (SSTP) ● Dynamic Trunking Protocol (DTP) ● Device Link Detection Protocol (DLDP) ● Ethernet Synchronization Message Channel (ESMC)

Parameter	Description	Value
		NOTE ● You can select one or more preceding protocols. ● By default, the packets with the destination MAC address of 0100-0CCC-CCCD are not BPDUs. PVST+ BPDUs are transparently transmitted by default, and other protocol packets are not transparently transmitted by default. ● If PVST BPDUs need to be transparently transmitted, use PVST+. SSTP can be used to transparently transmit the packets with the destination MAC address of 0100-CCCC-CCCD, regardless of the packet protocol.
user-defined-protocol *protocol-name*	Enables or disables transparent transmission of packets of a specified user-defined Layer 2 protocol. *protocol-name* specifies the name of a user-defined protocol.	The value is a string of 1 to 31 characters without spaces. When double quotation marks are used around the string, spaces are allowed in the string.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Layer 2 protocol tunneling is often configured on an interface connecting the PE and CE. After Layer 2 protocol tunneling is enabled, Layer 2 protocol packets received from the user network need to be sent to the CPU and the destination MAC address in the packets needs to be replaced. On the ISP network, Layer 2 protocol packets are directly forwarded.

Generally, the **l2protocol-tunnel** command is run on user-side interfaces of PEs.

Prerequisites

- The **l2protocol-tunnel vlan** command **enable**s an interface to transparently transmit Layer 2 protocol packets from the specified VLANs. The **l2protocol-tunnel** command **enable**s an interface to transparently transmit all Layer 2 protocol packets.
- The **l2protocol-tunnel vlan** and **l2protocol-tunnel** commands cannot specify the same protocol type on the same interface; otherwise, the configurations conflict.
- Before specifying a user-defined protocol in the **l2protocol-tunnel enable** command, run the **l2protocol-tunnel user-defined-protocol** command to define characteristic information about the Layer 2 protocol.
- STP packets have a default group MAC address for replacing the original destination MAC address. For packets of other Layer 2 protocols, you need to configure a global group MAC address to replace the destination MAC address. For details, see **l2protocol-tunnel group-mac**.
- To improve system performance, do not add service-irrelevant interfaces to the VLAN on which Layer 2 protocol tunneling is enabled.
- When an interface is enabled to transparently transmit the packets of a certain protocol, these packets do not participate in protocol processing. For example, after an interface is enabled to transparently transmit STP packets, the interface does not participate in STP calculation. Therefore, you are advised not to enable a protocol and the transparent transmission of this protocol on the same interface.
- You can configure the **l2protocol-tunnel enable** command on Layer 3 main interfaces and sub-interfaces only when the interfaces are on the S5731-H, S5731S-H, S5732-H, S6730S-H, and S6730-H and these interfaces are bound to VSIs.

Example

# Configure GE0/0/1 to transparently transmit STP BPDUs.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] stp disable
[HUAWEI-GigabitEthernet0/0/1] l2protocol-tunnel stp enable
```

5.17.13 l2protocol-tunnel drop-threshold

Function

The **l2protocol-tunnel drop-threshold** command sets the drop threshold of Layer 2 protocol packets that are transparently transmitted on an interface.

The **undo l2protocol-tunnel drop-threshold** command cancels the setting of the drop threshold.

By default, the drop threshold of Layer 2 protocol packets that are transparently transmitted on an interface is 0 pps. The rate of Layer 2 protocol packets is not limited on the interface.

Format

l2protocol-tunnel drop-threshold *rate* [{ *protocol-type* } &<1-16> | **user-defined-protocol** *protocol-name*]

undo l2protocol-tunnel drop-threshold [{ *protocol-type* } &<1-16> | **user-defined-protocol** *protocol-name*]

undo l2protocol-tunnel drop-threshold *rate* { *protocol-type* | **user-defined-protocol** *protocol-name* }

Parameters

Parameter	Description	Value
rate	Specifies the drop threshold of Layer 2 protocol packets that are transparently transmitted on an interface.	The value is an integer that ranges from 1 to 4096, in pps.

Parameter	Description	Value
protocol-type	Specifies the type of a Layer 2 protocol. The interface discards excess packets of this type of protocol when the rate of these packets exceeds the drop threshold. **NOTE** You can specify multiple protocols in the command.	The protocol type can be: ● Spanning Tree Protocol (STP) ● Link Aggregation Control Protocol (LACP) ● Ethernet Operation, Administration, and Maintenance 802.3ah (EOAM3ah) ● Link Layer Discovery Protocol (LLDP) ● GARP VLAN Registration Protocol (GVRP) ● GARP Multicast Registration Protocol (GMRP) ● HUAWEI Group Management Protocol (HGMP) ● VLAN Trunking Protocol (VTP) ● Unidirectional Link Detection (UDLD) ● Port Aggregation Protocol (PAGP) ● Cisco Discovery Protocol (CDP) ● Per VLAN Spanning Tree Plus (PVST+) ● Shared Spanning Tree Protocol (SSTP) ● Dynamic Trunking Protocol (DTP) ● Device Link Detection Protocol (DLDP) ● Ethernet Synchronization Message Channel (ESMC) You can select one or more Layer 2 protocols.

Parameter	Description	Value
user-defined-protocol *protocol-name*	Sets the drop threshold of packets of a user-defined Layer 2 protocol. *protocol-name* specifies the name of a user-defined protocol.	The value is a string of 1 to 31 characters without spaces. When double quotation marks are used around the string, spaces are allowed in the string.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

After enabling Layer 2 protocol tunneling on an interface, you can run the **l2protocol-tunnel drop-threshold** command on this interface to set the drop threshold of protocol packets.

After Layer 2 protocol tunneling is enabled and the drop threshold of Layer 2 protocol packets is set on an interface, the interface drops excess Layer 2 protocol packets when the drop threshold is exceeded. If the trap function is enabled, the device sends a trap message to the NMS to notify the network administrator.

When using the **l2protocol-tunnel drop-threshold** command, pay attention to the following points:

- If no Layer 2 protocol is specified, the drop threshold applies to all Layer 2 protocol packets that need to be transparently transmitted.
- If a Layer 2 protocol is specified, the interface discards excess packets of the protocol when the rate of these packets exceeds the drop threshold.
- If you run this command without specifying a protocol, and then run the command with a specified protocol, the drop threshold that you set the second time takes effect.

Example

# Set the drop threshold of STP packets that are transparently transmitted on GE0/0/1 to 10 pps.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] l2protocol-tunnel stp enable
[HUAWEI-GigabitEthernet0/0/1] l2protocol-tunnel drop-threshold 10 stp
```

5.17.14 l2protocol-tunnel group-mac

Function

The **l2protocol-tunnel group-mac** command enables the switch to replace the multicast destination MAC address of Layer 2 protocol packets with a specified multicast MAC address.

The **undo l2protocol-tunnel** command disables the group MAC function for Layer 2 protocol tunneling. After you run this command, the switch deletes a configured multicast destination MAC address of Layer 2 protocol packets except STP packets that uses the default multicast destination address or restores the default multicast destination MAC address of STP packets.

By default, the multicast destination MAC address of STP packets is replaced by 0100-0ccd-cdd0. For other Layer 2 protocol packets, there is not a default multicast MAC address for replacing their multicast destination MAC addresses.

Format

l2protocol-tunnel *protocol-type* **group-mac** { *group-mac* | **default-group-mac** }

undo l2protocol-tunnel *protocol-type*

Parameters

Parameter	Description	Value
protocol-type	Specifies the type of a Layer 2 protocol.	The protocol type can be: ● Spanning Tree Protocol (STP) ● Link Aggregation Control Protocol (LACP) ● Ethernet Operation, Administration, and Maintenance 802.3ah (EOAM3ah) ● Link Layer Discovery Protocol (LLDP) ● GARP VLAN Registration Protocol (GVRP) ● GARP Multicast Registration Protocol (GMRP) ● HUAWEI Group Management Protocol (HGMP) ● VLAN Trunking Protocol (VTP) ● Unidirectional Link Detection (UDLD) ● Port Aggregation Protocol (PAGP) ● Cisco Discovery Protocol (CDP) ● Per VLAN Spanning Tree Plus (PVST+) ● Shared Spanning Tree Protocol (SSTP) ● Dynamic Trunking Protocol (DTP) ● Device Link Detection Protocol (DLDP) ● Ethernet Synchronization Message Channel (ESMC)

Parameter	Description	Value
group-mac	Specifies the multicast MAC address that replaces the destination MAC address of Layer 2 protocol packets.	The value is in H-H-H format. An H is a hexadecimal number of 1 to 4 digits. The value ranges from 0100-0000-0000 to 01ff-ffff-ffff.
default-group-mac	Specifies the default MAC address of a multicast group, which is 0100-0ccd-cdd0.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Layer 2 protocols running between user networks, such as MSTP, HGMP, and LACP, must traverse a backbone network to perform Layer 2 protocol calculation.

Generally, the destination MAC addresses in Layer 2 protocol packets of the same Layer 2 protocol are the same. For example, the MSTP PDUs are BPDUs with the destination MAC address 0180-C200-0000. Therefore, when a Layer 2 protocol packet reaches an edge device on a backbone network, the edge device cannot identify whether the Layer 2 protocol packet comes from a user network or the backbone network and sends the Layer 2 protocol packet to the CPU to calculate a spanning tree. As a result, the user network devices calculate a spanning tree with backbone network edge devices but not with user network devices.

To resolve this problem, run the **l2protocol-tunnel group-mac** command on backbone network edge devices to replace the multicast destination MAC addresses in Layer 2 protocol packets with a specified multicast MAC address (group MAC address). This configuration allows Layer 2 protocol packets to be tunneled so that user network devices can calculate a spanning tree.

After this command is run, run the **display l2protocol-tunnel statistics group-mac** command to check statistics about the group-mac packets transparently transmitted by a specified interface.

Precautions

Layer 2 protocols with the same protocol type (For example, the LACP and DLDP protocol types are both 0x8809.) Do not configure the same group-mac. Otherwise, Layer 2 protocol transparent transmission may fail.

When configuring Layer 2 protocol tunneling, do not use the following multicast MAC addresses to replace the destination MAC address of Layer 2 protocol packets:

- Reserved multicast MAC addresses: 0180-C200-0000 to 0180-C200-002F
- Special multicast MAC addresses: 0100-0CCC-CCCC and 0100-0CCC-CCCD
- Destination MAC address of Smart Link packets: 010F-E200-0004
- Multicast MAC addresses that have been used on the network.
- Destination MAC address of VRRP packets: 0100-5E00-0012

NOTE

Do not replace the destination MAC addresses of SSTP, STP, GVRP, and GMRP packets with the same multicast MAC address.

Example

# Configure a device to replace the destination MAC address of STP packets with 0100-0100-0100 before tunneling the STP BPDUs.

```
<HUAWEI> system-view
[HUAWEI] l2protocol-tunnel stp group-mac 0100-0100-0100
```

5.17.15 l2protocol-tunnel protocol-type match disable

Function

The **l2protocol-tunnel protocol-type match disable** command disables a device from matching Layer 2 protocol tunneling packets to be sent to the CPU against the protocol type.

The **undo l2protocol-tunnel protocol-type match disable** command cancels the configuration.

By default, a device matches Layer 2 protocol tunneling packets to be sent to the CPU against the protocol type.

Format

l2protocol-tunnel protocol-type match disable

undo l2protocol-tunnel protocol-type match disable

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To disable a device from matching Layer 2 protocol tunneling packets to be sent to the CPU against the protocol type, run the **l2protocol-tunnel protocol-type match disable** command. After this command is run, the device can transparently transmit Layer 2 protocol packets with more than three tags.

Precautions

After the device is disabled from matching Layer 2 protocol tunneling packets to be sent to the CPU against the protocol type, the device checks only these packets' destination MAC addresses, not their protocol types. Packets with the same destination MAC address but different protocol types are all transparently transmitted. The user-defined Layer 2 protocol type configured using the **l2protocol-tunnel user-defined-protocol** *protocol-name* **protocol-mac** *protocol-mac* **encap-type ethernetii protocol-type** *protocol-type* command does not take effect.

Example

# Disable a device from matching Layer 2 protocol tunneling packets to be sent to the CPU against the protocol type.

```
<HUAWEI> system-view
[HUAWEI] l2protocol-tunnel protocol-type match disable
Info: The specified BPDU tunnel configuration of all interface will be updated. Please wait.
```

5.17.16 l2protocol-tunnel user-defined-protocol

Function

The **l2protocol-tunnel user-defined-protocol** command defines characteristic information about a user-defined Layer 2 protocol, including the protocol name, Ethernet encapsulation format, destination MAC address, and MAC address that replaces the destination MAC address of Layer 2 protocol packets.

The **undo l2protocol-tunnel user-defined-protocol** command deletes characteristic information about a user-defined Layer 2 protocol.

By default, no characteristic information about a user-defined Layer 2 protocol exists on the device.

Format

l2protocol-tunnel user-defined-protocol *protocol-name* **protocol-mac** *protocol-mac* [**encap-type** { { **ethernetii** | **snap** } **protocol-type** *protocol-type-value* | **llc dsap** *dsap-value* **ssap** *ssap-value* }] **group-mac** { *group-mac* | **default-group-mac** }

undo l2protocol-tunnel user-defined-protocol *protocol-name*

Parameters

Parameter	Description	Value
protocol-name	Specifies the name of a user-defined Layer 2 protocol.	The value is a string of 1 to 31 characters without spaces. **NOTE** When double quotation marks are used around the string, spaces are allowed in the string.
protocol-mac *protocol-mac*	Specifies the multicast destination MAC address of the user-defined protocol packets.	The value is in the format of H-H-H. An H is a hexadecimal number of 1 to 4 digits.
encap-type	Indicates the encapsulation format of transparently transmitted Layer 2 protocol packets. ● **ethernetii**: indicates Ethernet_II, the encapsulation format for Layer 2 protocol packets that are transparently transmitted. ● **snap**: indicates Sub-Network Access Protocol (SNAP), the encapsulation format for Layer 2 protocol packets that are transparently transmitted. ● **llc**: indicates Logical Link Control (LLC), the encapsulation format for Layer 2 protocol packets that are transparently transmitted.	-
dsap *dsap-value*	Specifies the destination service access point.	The value ranges from 0x00 to 0xff, in hexadecimal format.
ssap *ssap-value*	Specifies the source service access point.	The value ranges from 0x00 to 0xff, in hexadecimal format.

Parameter	Description	Value
protocol-type *protocol-type-value*	Indicates the Ethernet encapsulation format.	The value is a hexadecimal integer. ● The value ranges from 600 to FFFF for Ethernet II encapsulation type. ● The value ranges from 0 to FFFF for SNAP encapsulation type.
group-mac *group-mac*	Specifies the multicast MAC address that replaces the destination MAC address of Layer 2 protocol packets.	The value is in the format of H-H-H. An H is a hexadecimal number of 1 to 4 digits. The value ranges from 0100-0000-0000 to 01ff-ffff-ffff.
default-group-mac	Replaces the destination MAC address of Layer 2 protocol packets with the default multicast MAC address 0100-0ccd-cdd0.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

When Layer 2 protocol packets with a specified multicast destination MAC address need to be transparently transmitted on an ISP network, you can define characteristic information about the Layer 2 protocol on devices on the ISP network.

When configuring Layer 2 protocol tunneling, do not use the following multicast MAC addresses to replace the destination MAC address of Layer 2 protocol packets:

- Reserved multicast MAC addresses: 0180-C200-0000 to 0180-C200-002F
- Special multicast MAC addresses: 0100-0CCC-CCCC and 0100-0CCC-CCCD
- Destination MAC address of Smart Link packets: 010F-E200-0004
- Common multicast MAC addresses that have been used on the device

Before running the **l2protocol-tunnel** or **l2protocol-tunnel vlan** command to enable transparent transmission of user-defined Layer 2 protocol packets, run the **l2protocol-tunnel user-defined-protocol** command to define characteristic information about the Layer 2 protocol.

Example

# Define a Layer 2 protocol named **huawei**. Set the destination MAC address of its packets to 0180-c200-0022 and use multicast MAC address 0100-0100-0100 to replace the destination MAC address of its packets.

```
<HUAWEI> system-view
[HUAWEI] l2protocol-tunnel user-defined-protocol huawei protocol-mac 0180-c200-0022 group-mac
0100-0100-0100
```

5.17.17 l2protocol-tunnel vlan

Function

The **l2protocol-tunnel vlan** command enables VLAN-based Layer 2 protocol tunneling on an interface.

The **undo l2protocol-tunnel vlan** command disables VLAN-based Layer 2 protocol tunneling on an interface.

By default, VLAN-based Layer 2 protocol tunneling is disabled on an interface.

Format

l2protocol-tunnel { **all** | { *protocol-type* } &<1-15> | **user-defined-protocol** *protocol-name* } **vlan** { *low-id* [**to** *high-id*] } &<1-10>

undo l2protocol-tunnel { **all** | { *protocol-type* } &<1-15> | **user-defined-protocol** *protocol-name* } **vlan** { *low-id* [**to** *high-id*] } &<1-10>

Parameters

Parameter	Description	Value
all	Enables or disables transparent transmission of packets of all standard Layer 2 protocols and user-defined Layer 2 protocols.	-

Parameter	Description	Value
protocol-type	Enables or disables transparent transmission of packets of a specified Layer 2 protocol.	The protocol type can be: ● Spanning Tree Protocol (STP) ● Link Aggregation Control Protocol (LACP) ● Ethernet Operation, Administration, and Maintenance 802.3ah (EOAM3ah) ● Link Layer Discovery Protocol (LLDP) ● GARP VLAN Registration Protocol (GVRP) ● GARP Multicast Registration Protocol (GMRP) ● HUAWEI Group Management Protocol (HGMP) ● VLAN Trunking Protocol (VTP) ● Unidirectional Link Detection (UDLD) ● Port Aggregation Protocol (PAGP) ● Cisco Discovery Protocol (CDP) ● Per VLAN Spanning Tree Plus (PVST+) ● Shared Spanning Tree Protocol (SSTP) ● Dynamic Trunking Protocol (DTP) ● Device Link Detection Protocol (DLDP) ● Ethernet Synchronization Message Channel (ESMC) You can select one or more Layer 2 protocols.

Parameter	Description	Value
user-defined-protocol *protocol-name*	Enables or disables transparent transmission of packets of a user-defined Layer 2 protocol. *protocol-name* specifies the name of a user-defined protocol.	The value is a string of 1 to 31 characters without spaces. When double quotation marks are used around the string, spaces are allowed in the string.
low-id	Specifies the start VLAN ID.	The value is an integer that ranges from 1 to 4094. The value must be smaller than the end VLAN ID.
high-id	Specifies the end VLAN ID.	The value is an integer that ranges from 1 to 4094. The value must be greater than the start VLAN ID.

Views

Ethernet interface view, GE interface view, XGE interface view, 100GE interface view, 40GE interface view, MultiGE interface view, port group view, 25GE interface view, Eth-Trunk interface view

Default Level

2: Configuration level

Usage Guidelines

After a user-side interface of a PE on an ISP network is enabled to transparently transmit Layer 2 protocol packets, the interface directly forwards Layer 2 protocol packets sent from a user network instead of sending the packets to the CPU. In this way, Layer 2 protocol packets are transparently transmitted through the ISP network.

The **l2protocol-tunnel vlan** command is usually used on user-side interfaces of PEs.

The **l2protocol-tunnel vlan** command enables an interface to transparently transmit Layer 2 protocol packets from the specified VLANs. The **l2protocol-tunnel** command enables an interface to transparently transmit all Layer 2 protocol packets.

The **l2protocol-tunnel vlan** and **l2protocol-tunnel** commands cannot specify the same protocol type on the same interface. Otherwise, the configurations conflict.

Before specifying a user-defined protocol in the **l2protocol-tunnel vlan** command, run the **l2protocol-tunnel user-defined-protocol** command to define characteristic information about the Layer 2 protocol.

STP packets have a default MAC address for replacing the original destination MAC address. For packets of other Layer 2 protocols, you need to configure a global group MAC address to replace the destination MAC address. For details, see **l2protocol-tunnel group-mac**.

In addition, the VLAN specified in the command must be the static VLAN, but not the VLAN dynamically created by GVRP or VCMP.

If the **l2protocol-tunnel vlan** command is run more than once, all configurations take effect.

Example

# Enable GE0/0/1 to transparently transmit LACP packets with VLAN tags ranging from 100 to 200.

```
<HUAWEI> system-view
[HUAWEI] vlan batch 100 to 200
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] port link-type trunk
[HUAWEI-GigabitEthernet0/0/1] port trunk allow-pass vlan 100 to 200
[HUAWEI-GigabitEthernet0/0/1] l2protocol-tunnel lacp vlan 100 to 200
```

5.17.18 reset l2protocol-tunnel statistics

Function

The **reset l2protocol-tunnel statistics** command clears statistics about Layer 2 protocol packets that are transparently transmitted on an interface.

Format

reset l2protocol-tunnel statistics *interface-type interface-number* [{ *protocol-type* } &<1-16> | **user-defined-protocol** *protocol-name*]

Parameters

Parameter	Description	Value
interface-type interface-number	Clears statistics about Layer 2 protocol packets that are transparently transmitted on a specified interface. ● *interface-type* specifies the type of an interface. ● *interface-number* specifies the number of an interface. The specified interface must be enabled with Layer 2 protocol tunneling.	-

Parameter	Description	Value
protocol-type	Clears statistics about transparently transmitted packets of a specified protocol.	The protocol type can be: ● Spanning Tree Protocol (STP) ● Link Aggregation Control Protocol (LACP) ● Ethernet Operation, Administration, and Maintenance 802.3ah (EOAM3ah) ● Link Layer Discovery Protocol (LLDP) ● GARP VLAN Registration Protocol (GVRP) ● GARP Multicast Registration Protocol (GMRP) ● HUAWEI Group Management Protocol (HGMP) ● VLAN Trunking Protocol (VTP) ● Unidirectional Link Detection (UDLD) ● Port Aggregation Protocol (PAGP) ● Cisco Discovery Protocol (CDP) ● Per VLAN Spanning Tree Plus (PVST+) ● Shared Spanning Tree Protocol (SSTP) ● Dynamic Trunking Protocol (DTP) ● Device Link Detection Protocol (DLDP) ● Ethernet Synchronization Message Channel (ESMC) You can select one or more Layer 2 protocols.

Parameter	Description	Value
user-defined-protocol *protocol-name*	Clears statistics about transparently transmitted packets of a user-defined protocol. *protocol-name* specifies the name of a user-defined protocol.	The value is a string of 1 to 31 case-sensitive characters without spaces. When double quotation marks are used around the string, spaces are allowed in the string.

Views

User view

Default Level

3: Management level

Usage Guidelines

To collect statistics about Layer 2 protocol packets transparently transmitted on an interface in a specified period, you must reset original statistics on the interface.

When using the **reset l2protocol-tunnel statistics** command, pay attention to the following points:

- If you specify an interface but do not specify any protocol, statistics about all Layer 2 protocol packets on the interface are reset.
- If you specify an interface and a protocol, statistics about packets of the specified protocol are reset.

NOTE

Statistics about Layer 2 protocol packets cannot be restored after being deleted. Confirm your action before you use this command.

Example

# Reset statistics about all Layer 2 protocol packets on GE0/0/1.

```
<HUAWEI> reset l2protocol-tunnel statistics gigabitethernet 0/0/1
```

# Reset statistics about STP packets on GE0/0/2.

```
<HUAWEI> reset l2protocol-tunnel statistics gigabitethernet 0/0/2 stp
```

5.17.19 reset l2protocol-tunnel statistics group-mac

Function

The **reset l2protocol-tunnel statistics group-mac** command clears statistics about transparently transmitted Layer 2 PDUs whose multicast destination MAC addresses are replaced with destination MAC addresses (group MAC address) on an interface.

Format

reset l2protocol-tunnel statistics group-mac [*interface-type interface-number*]

Parameters

Parameter	Description	Value
interface-type interface-number	Specifies the interface on which the statistics about transparently transmitted Layer 2 PDUs whose multicast destination MAC addresses are replaced with a specified group MAC address are to be cleared. ● *interface-type* specifies the type of the interface. ● *interface-number* specifies the number of the interface.	-

Views

User view

Default Level

3: Management level

Usage Guidelines

After Layer 2 protocol tunneling is configured on a device, if you need to collect statistics within a specified period about transparently transmitted Layer 2 PDUs whose multicast destination MAC addresses are replaced with a specified group MAC address on an interface, first run the **reset l2protocol-tunnel statistics group-mac** command to clear existing statistics on the interface, and then enable the interface to collect statistics within that period.

Example

# Clear statistics about transparently transmitted Layer 2 PDUs whose multicast destination MAC addresses are replaced with a specified group MAC address on GE 0/0/1.

```
<HUAWEI> reset l2protocol-tunnel statistics group-mac Gigabitethernet 0/0/1
```

5.17.20 stp bpdu vlan

Function

The **stp bpdu vlan** command configures the STP packets sent from an interface to contain the specified VLAN ID.

The **undo stp bpdu vlan** command cancels the configuration.

By default, the STP packets sent from an interface do not contain VLAN IDs.

Format

stp bpdu vlan *vlan-id*

undo stp bpdu vlan

Parameters

Parameter	Description	Value
vlan-id	Specifies the VLAN ID contained in the STP packets sent from an interface.	The value is an integer that ranges from 1 to 4094.

Views

Ethernet interface view, GE interface view, XGE interface view, 100GE interface view, 40GE interface view, MultiGE interface view, port group view, 25GE interface view, Eth-Trunk interface view

Default Level

2: Configuration level

Usage Guidelines

When multiple user networks connect to the interfaces of the same PE, the PE interface needs to distinguish STP packets from different user networks. In this case, you need to configure the STP packets sent from each CE interface to contain the specified VLAN ID. In addition, the STP packets sent to the CE interface must also contain the specified VLAN ID.

On the CE interface, run the **stp bpdu vlan** *vlan-id* command to configure the STP packets sent to the PE to contain the specified VLAN ID. On the PE interface connected to the CE, run the **l2protocol-tunnel vlan** command to enable the STP packets with the specified VLAN ID to traverse the ISP network.

Before running the **stp bpdu vlan** command on a CE interface, ensure that the CE interface has been added to the specified VLAN.

The **stp bpdu vlan** command is usually configured on the network interface of the CE.

Example

# Configure the STP packets sent from GE0/0/1 to contain VLAN ID 100.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] port link-type trunk
```

```
[HUAWEI-GigabitEthernet0/0/1] port trunk allow-pass vlan 100
[HUAWEI-GigabitEthernet0/0/1] stp bpdu vlan 100
```

5.17.21 stp snooping enable

Function

The **stp snooping enable** command enables STP snooping.

The **undo stp snooping enable** command disables STP snooping.

By default, STP snooping is disabled on interfaces.

Format

stp snooping enable

undo stp snooping enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

After you run the **l2protocol-tunnel** command to enable transparent transmission of Layer 2 protocol packets on untagged interfaces or the **l2protocol-tunnel vlan** command to enable transparent transmission of Layer 2 protocol packets on tagged interfaces, the untagged or tagged interfaces directly forward Layer 2 protocol packets sent from user networks over the ISP network but not send them to the CPU for processing. When a device enabled with Layer 2 protocol tunneling receives TC packets, the device clears the MAC entries and ARP entries and updates the forwarding table after the **stp snooping enable** command is executed.

Example

# Enable STP snooping.

```
<HUAWEI> system-view
[HUAWEI] stp snooping enable
```