12 Reliability Commands

12.1 BFD Configuration Commands

12.1.1 Command Support

Only the following switch models support BFD:

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.

12.1.2 authentication-mode (BFD)

Function

The **authentication-mode** command configures BFD session authentication information.

The **undo authentication-mode** command deletes the configured BFD session authentication information.

By default, BFD session authentication information is not configured.

Format

authentication-mode met-sha1 key-id *key-id-value* **cipher** *cipher-text* **nego-packet** [**timeout-interval** *interval-value*]

undo authentication-mode

Parameters

Parameter	Description	Value
met-sha1	Specifies MSHA1 to decrypt and authenticate.	-
key-id *key-id-value*	Specifies the authentication key ID of a BFD session.	The value is an integer that ranges from 1 to 255.
cipher *cipher-text*	Specifies a ciphertext BFD authentication password. You can enter either a simple or ciphertext password, but the password is displayed in ciphertext in the configuration file.	The value is a string of characters. • The value is a string of 1 to 20 characters for simple authentication passwords. • The value is a string of 20 to 148 characters for ciphertext authentication passwords. **NOTE** The characters exclude question marks (?) and spaces. However, if a password string is between a pair of quotation marks, the string can contain spaces.
nego-packet	Authenticates BFD negotiation packets.	-
timeout-interval *interval-value*	Specifies the negotiation timeout period of a BFD session.	The value is an integer ranging from 1 to 10000, in seconds. This parameter has no default value. **NOTE** After a BFD negotiation timeout period is configured, the BFD negotiation timeout timer is started when the BFD session goes Down (the event is not triggered by a link fault detected). If the timer has expired but the BFD session is still Down, the link protocol of the associated interface goes Down.

Views

BFD session view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On a network demanding higher security, run the **authentication-mode** command to configure BFD session authentication information to improve network security. In a specific access scenario, for example, when a multicast BFD session is associated with the protocol status of an interface, you need to configure authentication information for the BFD session on the interface. BFD negotiation can succeed, the BFD-associated protocol status of the interface can be activated, and users can access the device through this interface only when the BFD session authentication information on both ends is consistent.

Prerequisites

BFD has been globally enabled using the **bfd** command in the system view.

A BFD session used to detect the physical link status has been created using the **bfd bind peer-ip default-ip** command in the system view.

Precautions

If you run the **authentication-mode** command to configure BFD session authentication information, BFD renegotiation will be performed. BFD renegotiation can succeed only when the BFD session authentication information on both ends is consistent.

Adding, modifying, or deleting BFD session authentication information may interrupt the service associated with the BFD session.

Example

Configure multicast BFD session authentication information.

```
<HUAWEI> system-view
[HUAWEI] bfd test bind peer-ip default-ip interface GigabitEthernet0/0/1
[HUAWEI-bfd-session-test] authentication-mode met-sha1 key-id 5 cipher YsHsjx_202206 nego-packet timeout-interval 5
```

12.1.3 bfd

Function

The **bfd** command enables the global Bidirectional Forwarding Detection (BFD) function and displays the BFD view.

The **undo bfd** command disables global BFD.

By default, global BFD is disabled.

Format

bfd

undo bfd

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To fast detect link faults, run the **bfd** command in the system view to enable global BFD.

Precautions

BFD must be enabled globally before BFD parameters are configured.

NOTICE

Running the **undo bfd** command in the system view may affect services associated with BFD and deletes all BFD sessions on the device. To restore the BFD function, you have to re-configure BFD sessions.

Example

Enable the global BFD function.

```
<HUAWEI> system-view
[HUAWEI] bfd
[HUAWEI-bfd]
```

12.1.4 bfd bind peer-ip

Function

The **bfd bind peer-ip** command creates a BFD session, specifies the peer IP address, and displays the BFD session view.

The **undo bfd** *session-name* command deletes a specified BFD session and cancels the peer IP address.

By default, BFD binding is not created.

Format

bfd *session-name* **bind peer-ip** *ip-address* [**vpn-instance** *vpn-name*] [**interface** *interface-type interface-number*] [**source-ip** *ip-address*]

undo bfd *session-name*

Parameters

Parameter	Description	Value
session-name	Specifies the name of a BFD session.	The value is a string of 1 to 15 case-sensitive characters without spaces. **NOTE** When double quotation marks are used around the string, spaces are allowed in the string.
peer-ip *ip-address*	Specifies the peer IP address bound to the BFD session.	-
vpn-instance *vpn-name*	Specifies the name of a Virtual Private Network (VPN) instance that is bound to a BFD session.	The value must be an existing VPN instance name.
interface *interface-type interface-number*	Specifies the type and number of the interface bound to the BFD session. ● *interface-type* specifies the type of the interface. ● *interface-number* specifies the number of the interface.	-

Parameter	Description	Value
source-ip *ip-address*	Indicates the source IP address carried in BFD packets. • During BFD session negotiation, if the source IP address is not specified, the system searches the local routing table for an outbound interface from which the peer IP address is reachable. The IP address of this outbound interface is used as the source IP address of the BFD packets sent by the local end. • When a BFD session is detecting links, if this parameter is not specified, the system uses a fixed source IP address in BFD packets. When BFD is used with the Unicast Reverse Path Forwarding (URPF) function, you must manually configure the source IP address in BFD packets because the URPF function checks the source IP address in received packets. **NOTE** For details about URPF, see URPF Configuration in the *S300, S500, S2700, S5700, and S6700 V200R023C00 Configuration Guide - Security*.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To fast detect and monitor links, create BFD sessions.

To create a BFD binding, pay attention to the following points:

- If only the peer IP address is specified, BFD is configured to detect the multi-hop link.
- If the peer IP address and local interface are specified, BFD is configured to detect the single-hop link, that is, a specific route with this interface as the outbound interface and with the peer IP address as the next-hop address.
- If both the peer IP address and the VPN instance are specified, BFD is configured to detect the multi-hop link in the VPN instance.
- The single-hop link in the VPN instance is detected if both the peer IP address, VPN instance, and local interface are specified.

Prerequisites

Global BFD has been enabled by using the **bfd** command in the system view.

Follow-up Procedure

- Run the **discriminator** command to set the local and remote discriminators for the current BFD session.

Precautions

- When creating a single-hop BFD session, bind the single-hop BFD session to the peer IP address and the local address. You only need to bind a multi-hop BFD session to the peer IP address.
- When the BFD configuration items are created, the system checks only the format of the IP address. The BFD session cannot be established if an incorrect peer IP address or source IP address is bound.
- When a multi-hop BFD session is configured, the value of **peer-ip** or **source-ip** cannot be the IP address of a GRE tunnel interface.
- When a multi-hop BFD session is configured and the peer IP address is the same as the 32-bit destination IP address of an LDP or static LSP, the BFD session is associated with the LSP. That is, if the BFD session detects a fault, an LSP switchover is performed.

Example

Create a BFD session named **atob** to detect the single-hop link from VLANIF100 to the peer IP address at 10.10.10.2.

```
<HUAWEI> system-view
[HUAWEI] bfd
[HUAWEI-bfd] quit
[HUAWEI] bfd atob bind peer-ip 10.10.10.2 interface vlanif 100
```


Create a BFD session named **atoc** to detect the multi-hop link to the peer IP address 10.10.20.2.

```
<HUAWEI> system-view
[HUAWEI] bfd
[HUAWEI-bfd] quit
[HUAWEI] bfd atoc bind peer-ip 10.10.20.2
```

12.1.5 bfd bind peer-ip default-ip

Function

The **bfd bind peer-ip default-ip** command creates a BFD binding for detecting the physical status of a link.

The **undo bfd** *session-name* command deletes a specified BFD session and the created BFD binding.

By default, no BFD binding for monitoring physical status of a link is configured.

Format

bfd *session-name* **bind peer-ip default-ip interface** *interface-type interface-number* [**source-ip** *ip-address*] [**auto**]

undo bfd *session-name*

Parameters

Parameter	Description	Value
session-name	Specifies the session name of BFD.	The value is a string of 1 to 15 characters without spaces. **NOTE** When quotation marks are used around the string, spaces are allowed in the string.
peer-ip default-ip	Indicates the default multicast IP address that is bound to a BFD session.	By default, BFD uses the multicast IP address 224.0.0.184. You can set the multicast IP address by running the **default-ip-address** command.

Parameter	Description	Value
interface-type interface-number	Specifies the type and number of the interface bound to a BFD session. • *interface-type* specifies the interface type. • *interface-number* specifies the interface number.	-
source-ip *ip-address*	Indicates the source IP address carried in BFD packets. If the source IP address is not specified, the system searches the local routing table for an outbound interface from which the peer IP address can be reached. The IP address of this outbound interface is used as the source IP address of BFD packets sent by the local end. Generally, this parameter is not required. When BFD is used with the Unicast Reverse Path Forwarding (URPF) function, you must manually configure the source IP address in BFD packets because the URPF function checks the source IP address in received packets. **NOTE** For details about URPF, see URPF Configuration in the *S300, S500, S2700, S5700, and S6700 V200R023C00 Configuration Guide - Security*.	-
auto	Enables automatic negotiation of local and remote discriminators.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If **source-ip** is specified, the URPF-enabled device does not incorrectly discard BFD packets. Ensure that the source IP address is correct. The system only checks whether the source IP address is valid (for example, it cannot be a multicast or broadcast address) without checking correctness.

Precautions

When the **bfd bind peer-ip default-ip** command is used to configure a BFD session, ring protocols cannot be configured on the interface bound to the BFD session. Otherwise, MAC address flapping may occur.

If the IP address of an outbound interface is changed after a BFD session is configured, the source IP address of BFD packets is not updated.

NOTE

If automatic negotiation of local and remote discriminators is not configured, run the **commit** command to commit the configuration to make the configuration take effect.

Unlike common static BFD sessions, static BFD sessions with automatically negotiated discriminators have separate characteristics:

- The **bfd bind peer-ip source-ip auto** command can be run and immediately create a static BFD session with automatically negotiated discriminators, without the **commit** command executed.
- Parameters of a static BFD session with automatically negotiated discriminators take effect immediately after being modified, without the **commit** command executed. The parameters include the minimum interval at which BFD packets are sent and received and the detection multiplier.
- The **commit** command can be run for a static BFD session with automatically negotiated discriminators to support the forward version compatibility.

Example

Create a BFD session named **test**, and then detect the one-hop link that is bound to the local interface GigabitEthernet0/0/1 through the default multicast IP address.

```
<HUAWEI> system-view
[HUAWEI] bfd test bind peer-ip default-ip interface gigabitethernet 0/0/1
[HUAWEI-bfd-session-test]
```


12.1.6 bfd bind peer-ip source-ip auto

Function

The **bfd bind peer-ip source-ip auto** command creates a static BFD session with automatically negotiated discriminators.

The **undo bfd** *session-name* command deletes a specified BFD session.

By default, no static BFD session with automatically negotiated discriminators is established.

Format

bfd *session-name* **bind peer-ip** *ip-address* [**vpn-instance** *vpn-name*] [**interface** *interface-type interface-number*] **source-ip** *ip-address* **auto**

undo bfd *session-name*

Parameters

Parameter	Description	Value
session-name	Specifies the name of a BFD session.	The value is a string of 1 to 15 case-sensitive characters without spaces. **NOTE** When quotation marks are used around the string, spaces are allowed in the string.
peer-ip *ip-address*	Specifies the peer IP address bound to the BFD session.	-
vpn-instance *vpn-name*	Specifies the name of a Virtual Private Network (VPN) instance that is bound to a BFD session.	The value must be an existing VPN instance name.
interface-type interface-number	Specifies the type and number of the interface bound to the BFD session. ● *interface-type* specifies the type of the interface. ● *interface-number* specifies the number of the interface.	-

Parameter	Description	Value
source-ip *ip-address*	Indicates the source IP address carried in BFD packets, that is, IP address of the outbound interface.	-
auto	Enables automatic negotiation of local and remote discriminators.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The local device where a BFD session with automatically negotiated parameters is configured can negotiate with the remote device where a dynamic BFD session is configured; however, the local device enabled with static BFD can establish a BFD session with the remote device enabled with static BFD only. When configuring a BFD session with automatically negotiated parameters or a static BFD session, you can specify the BFD session name. The name of a dynamic BFD session is generated dynamically. When the network changes, the name of the dynamic BFD session may change.

When the remote end is configured with dynamic BFD and the local end needs to be configured with association between BFD and static route (BFD session name needs to be specified during association configuration), a BFD session with automatically negotiated parameters can be configured on the local end. Then the local end can establish a BFD session with the remote end enabled with dynamic BFD and association between BFD and static route can be implemented.

When creating a static BFD session with automatically negotiated discriminators, pay attention to the following points:

- If only the peer IP address is specified, BFD is configured to detect the multi-hop link.
- If the peer IP address and local interface are specified, BFD is configured to detect the single-hop link, that is, a specific route with this interface as the outbound interface and with the peer IP address as the next-hop address.
- Ensure that the source IP address is correct. The system only checks whether the source IP address is valid (for example, it cannot be a multicast or broadcast address) without checking correctness.

- If both the peer IP address and the VPN instance are specified, BFD is configured to detect the multi-hop link in the VPN instance.
- If the peer IP address, VPN instance, and local interface are specified, BFD is configured to detect the single-hop link in the VPN instance.

Prerequisites

Global BFD has been enabled by using the **bfd** command in the system view.

Precautions

- When creating a BFD session, bind the BFD session to the peer IP address and the local address.
- When the BFD configuration items are created, the system checks only the format of the IP address. The BFD session cannot be established if an incorrect peer IP address or source IP address is bound.

NOTE

Unlike common static BFD sessions, static BFD sessions with automatically negotiated discriminators have separate characteristics:

- The **bfd bind peer-ip source-ip auto** command can be run and immediately create a static BFD session with automatically negotiated discriminators, without the **commit** command executed.
- Parameters of a static BFD session with automatically negotiated discriminators take effect immediately after being modified, without the **commit** command executed. The parameters include the minimum interval at which BFD packets are sent and received and the detection multiplier.
- The **commit** command can be run for a static BFD session with automatically negotiated discriminators to support the forward version compatibility.

Example

Create a static BFD session with automatically negotiated discriminators.

```
<HUAWEI> system-view
[HUAWEI] bfd
[HUAWEI-bfd] quit
[HUAWEI] bfd atob bind peer-ip 10.1.1.2 interface vlanif 100 source-ip 10.1.1.1 auto
```

12.1.7 bfd bind peer-ipv6

Function

The **bfd bind peer-ipv6** command creates a BFD6 session to detect IPv6 links.

The **undo bfd** *bfd-name* command deletes a specified BFD6 session.

By default, no BFD6 session is created for IPv6 links.

Format

bfd *session-name* **bind peer-ipv6** *ipv6-address* [**vpn-instance** *vpn-instance-name*] [**interface** *interface-type interface-number*] [**source-ipv6** *ipv6-address*]

undo bfd *session-name*

Parameters

Parameter	Description	Value
session-name	Specifies the name of a BFD6 session.	The value is a string of 1 to 15 case-sensitive characters without spaces. **NOTE** When double quotation marks are used around the string, spaces are allowed in the string.
peer-ipv6 *ipv6-address*	Specifies the peer IPv6 address bound to a BFD6 session.	-
vpn-instance *vpn-instance-name*	Specifies the name of a VPN instance bound to a BFD6 session.	The value must be an existing VPN instance name.
interface *interface-type interface-number*	Specifies the local Layer 3 outbound interface bound to a BFD6 session. • *interface-type* specifies the interface type. • *interface-number* specifies the interface number.	-

Parameter	Description	Value
source-ipv6 *ipv6-address*	Specifies the source IPv6 address carried in BFD packets. Generally, you do not need to set this parameter. If you do not specify the source IP address, the system automatically sets the source IP address according to the following rules: • During BFD for IPv6 session negotiation, if the source IPv6 address is not specified, the system searches the local routing table for an outbound interface from which the peer IP address is reachable. The IPv6 address of this outbound interface is used as the source IP address of the BFD packets sent by the local end. • If this parameter is not specified when a BFD for IPv6 session is detecting links, the system uses a fixed source IPv6 address in BFD packets. **NOTE** When BFD is used with Unicast Reverse Path Forwarding (URPF), you must manually configure the source IPv6 address in BFD packets because URPF checks the source IPv6 address in received packets.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To fast detect and monitor IPv6 links, you can create BFD for IPv6 sessions.

When creating a BFD for IPv6 binding, pay attention to the following points:

- If only the peer IPv6 address is specified, BFD is configured to detect the multi-hop link.
- A single-hop link is detected if both the peer IPv6 address and the local interface are specified. That is, a BFD6 session detects a specific route with this interface as the outbound interface and with the peer IPv6 address as the next hop address.
- If both the peer IPv6 address and the VPN instance are specified, the created BFD6 session detects the multi-hop links in the VPN instance.

- The single-hop links in a VPN instance are detected if both the peer IPv6 address, VPN instance, and local interface are specified.

NOTE

The **source-ipv6** parameter prevents BFD packets from being discarded incorrectly by URPF. The system checks only the source IPv6 address type (it cannot be a multicast or broadcast address), but does not check the address correctness. Therefore, you must manually check the correctness of the source IPv6 address.

When a multi-hop BFD6 session is configured, the value of **peer-ipv6** or **source-ipv6** cannot be the IPv6 address of a GRE tunnel interface.

Prerequisites

Global BFD has been enabled using the **bfd** command in the system view.

Follow-up Procedure

After creating a BFD for IPv6 session and entering its view, perform the following mandatory operations:

1. Run the **discriminator** command to set the local and remote discriminators for the BFD for IPv6 session.
2. Run the **commit** command to commit the configuration.

Perform the following optional operations according to your needs:

- Run the **description** command to configure description for the BFD for IPv6 session.
- Run the **min-tx-interval** command to set the interval for sending BFD for IPv6 packets.
- Run the **min-rx-interval** command to set the interval for receiving BFD for IPv6 packets.
- Run the **detect-multiplier** command to set the local detection multiplier.
- Run the **process-pst** command to configure the Port State Table (PST) of the BFD session.
- Run the **wtr** command to set the Wait-to-Recovery (WTR) time for the BFD for IPv6 session.

Precaution

- The BFD for IPv6 session detects links bidirectionally, so the **bfd bind peer-ipv6** command must be run on both ends of each link.
- After a BFD for IPv6 session is created:
  - If you change the source IPv6 address of outbound interface during session negotiation, the source IPv6 address in BFD packets is also changed.
  - If you change the source IPv6 address of outbound interface during session detection, the source IPv6 address in BFD packets is not changed.

Example

Create a BFD6 session named **atob** to detect a single-hop link.

```
<HUAWEI> system-view
[HUAWEI] bfd
```



```
[HUAWEI-bfd] quit
[HUAWEI] bfd atob bind peer-ipv6 2001:db8:1::1 interface vlanif 10
[HUAWEI-bfd-session-atob] discriminator local 1
[HUAWEI-bfd-session-atob] discriminator remote 2
[HUAWEI-bfd-session-atob] commit
```

Create a BFD6 session named **atoc** to detect a multi-hop link from which BFD6 packets reach 2001:db8:1::1.

```
<HUAWEI> system-view
[HUAWEI] bfd
[HUAWEI-bfd] quit
[HUAWEI] bfd atoc bind peer-ipv6 2001:db8:1::1
[HUAWEI-bfd-session-atoc] discriminator local 3
[HUAWEI-bfd-session-atoc] discriminator remote 4
[HUAWEI-bfd-session-atoc] commit
```

12.1.8 bfd bind peer-ipv6 source-ipv6 auto

Function

The **bfd bind peer-ipv6 source-ipv6 auto** command creates a static BFD6 session with automatically negotiated discriminators.

The **undo bfd** *bfd-name* command deletes a specified BFD6 session.

By default, no static BFD6 session with automatically negotiated discriminators.

Format

bfd *session-name* **bind peer-ipv6** *ipv6-address* [**vpn-instance** *vpn-instance-name*] [**interface** *interface-type interface-number*] **source-ipv6** *ipv6-address* **auto**

undo bfd *session-name*

Parameters

Parameter	Description	Value
session-name	Specifies the name of a BFD6 session.	The value is a string of 1 to 15 case-sensitive characters without spaces. **NOTE** When double quotation marks are used around the string, spaces are allowed in the string.
peer-ipv6 *ipv6-address*	Specifies the peer IPv6 address bound to a BFD6 session.	-
vpn-instance *vpn-instance-name*	Specifies the name of a VPN instance bound to a BFD6 session.	The value must be an existing VPN instance name.

Parameter	Description	Value
interface *interface-type interface-number*	Specifies the local Layer 3 outbound interface bound to a BFD6 session. • *interface-type* specifies the interface type. • *interface-number* specifies the interface number.	-
source-ipv6 *ipv6-address*	Specifies the source IPv6 address carried in BFD packets.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The local device where a BFD session with automatically negotiated parameters is configured can negotiate with the remote device where a dynamic BFD session is configured; however, the local device enabled with static BFD can establish a BFD session with the remote device enabled with static BFD only. When configuring a BFD session with automatically negotiated parameters or a static BFD session, you can specify the BFD session name. The name of a dynamic BFD session is generated dynamically. When the network changes, the name of the dynamic BFD session may change.

When the remote end is configured with dynamic BFD and the local end needs to be configured with association between BFD and static route (BFD session name needs to be specified during association configuration), a BFD session with automatically negotiated parameters can be configured on the local end. Then the local end can establish a BFD session with the remote end enabled with dynamic BFD and association between BFD and static route can be implemented.

When creating a static BFD for IPv6 session with automatically negotiated discriminators, pay attention to the following points:

- If only the peer IPv6 address is specified, BFD is configured to detect the multi-hop link.
- A single-hop link is detected if both the peer IPv6 address and the local interface are specified. That is, a BFD6 session detects a specific route with this interface as the outbound interface and with the peer IPv6 address as the next hop address.
- If both the peer IPv6 address and the VPN instance are specified, the created BFD6 session detects the multi-hop links in the VPN instance.

- If the peer IPv6 address, VPN instance, and local interface are specified, the created BFD6 session detects the single-hop links in the VPN instance.

Prerequisites

Global BFD has been enabled using the **bfd** command in the system view.

Follow-up Procedure

After creating a static BFD for IPv6 session with automatically negotiated discriminators and entering its view, perform the following mandatory operations:

- Run the **description** command to configure description for the BFD for IPv6 session.
- Run the **min-tx-interval** command to set the interval for sending BFD packets.
- Run the **min-rx-interval** command to set the interval for receiving BFD packets.
- Run the **detect-multiplier** command to set the local detection multiplier.
- Run the **process-pst** command to configure the Port State Table (PST) of the BFD session.
- Run the **wtr** command to set the Wait-to-Recovery (WTR) time for the BFD for IPv6 session.

Precaution

A static BFD for IPv6 session and a static BFD6 session with automatically negotiated discriminators have the following differences:

- The local and remote discriminators must be specified for a static BFD for IPv6 session.
- The local and remote discriminators are optional for a static BFD6 session with automatically negotiated discriminators.

If the IPv6 address of outbound interface is changed for a BFD for IPv6 session, the source IPv6 address in BFD packets is not changed.

The source address is mandatory for a static BFD6 session with automatically negotiated discriminators.

Example

Create a static BFD6 session named **atob** with the automatically negotiated discriminators to detect a single-hop link.

```
<HUAWEI> system-view
[HUAWEI] bfd
[HUAWEI-bfd] quit
[HUAWEI] bfd atob bind peer-ipv6 2001:db8:1::1 interface gigabitethernet 0/0/1 source-ipv6 2001:db8:1::1 auto
[HUAWEI-bfd-session-atob]
```

Create a static BFD6 session named **atoc** with the automatically negotiated discriminators to detect the multi-hop link from which BFD6 packets reach 2001:db8:1::1.

```
<HUAWEI> system-view
[HUAWEI] bfd
```



```
[HUAWEI-bfd] quit
[HUAWEI] bfd atoc bind peer-ipv6 2001:db8:1::1 source-ipv6 2001:db8:1::1 auto
[HUAWEI-bfd-session-atoc]
```

12.1.9 bfd one-arm-echo

Function

The **bfd one-arm-echo** command configures the BFD echo function.

The **undo bfd** command deletes a specified BFD session and cancels the binding.

By default, the BFD echo function is not configured.

Format

bfd *session-name* **bind peer-ip** *peer-ip* [**vpn-instance** *vpn-instance-name*] **interface** *interface-type interface-number* [**source-ip** *ip-address*] **one-arm-echo**

undo bfd *session-name*

Parameters

Parameter	Description	Value
session-name	Specifies the name of a BFD session supporting the BFD echo function.	The value is a string of 1 to 15 case-insensitive characters without spaces. **NOTE** When quotation marks are used around the string, spaces are allowed in the string.
peer-ip *peer-ip*	Specifies the peer IP address bound to the BFD session.	The value is in dotted decimal notation.
vpn-instance *vpn-instance-name*	Specifies the name of a Virtual Private Network (VPN) instance that is bound to a BFD session.	The value must be an existing VPN instance name.
interface-type interface-number	Specifies the type and number of the interface bound to a BFD session. • *interface-type* specifies the interface type. • *interface-number* specifies the interface number.	-

Parameter	Description	Value
source-ip *ip-address*	Indicates the source IP address carried in BFD packets. This parameter should be configured.	-
one-arm-echo	Indicates a BFD session supporting the BFD echo function.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Among two directly connected devices, one device supports BFD, whereas the other device does not support BFD. To rapidly detect forwarding failures between the two devices, configure a BFD session supporting the BFD echo function on the BFD-supporting device. The BFD-supporting device sends an Echo Request packet to the remote device. The remote device sends the Echo Request packet back along the same path to detect the forwarding link connectivity.

When you configure a BFD session supporting the BFD echo function:

- Specify **source-ip** *ip-address*. Ensure that the source IP address is correct. The system only checks whether the source IP address is valid (for example, it cannot be a multicast or broadcast address) without checking correctness. When URPF is enabled, ensure that **source-ip** *ip-address* can be pinged from the remote device so that the URPF-enabled device does not incorrectly discard BFD packets.
- On a network, some devices discard packets with the same source and destination IP addresses, so you are advised to set the value of **source-ip** *ip-address* to be different from the IP address of the outbound interface.
- If a VPN instance is specified, BFD is configured to detect the one-hop link in the VPN instance.

Prerequisites

Global BFD has been enabled using the **bfd** command in the system view.

Precautions

The difference between a BFD session supporting the BFD echo function and a common BFD session is as follows:

- When configuring a BFD session supporting the BFD echo function, you can only specify **local** *discr-value* in the **discriminator** command.
- You can only run the **min-echo-rx-interval** command to change the interval for receiving BFD packets.

NOTE

- If the IP address of an outbound interface is changed after a BFD session is configured, the source IP address of BFD packets is not updated.
- The BFD echo function is only applicable to single-hop BFD sessions.
- After the **bfd one-arm-echo** command is executed, run the **commit** command to commit the configuration to make the configuration take effect.

Example

Configure a BFD session **test** supporting the BFD echo function.

```
<HUAWEI> system-view
[HUAWEI] bfd test bind peer-ip 10.10.10.1 interface vlanif 100 source-ip 10.10.10.2 one-arm-echo
[HUAWEI-bfd-session-test] discriminator local 100
[HUAWEI-bfd-session-test] commit
```

12.1.10 bfd session-name

Function

The **bfd** command displays the view of a specified BFD session.

The **undo bfd** command deletes a specified BFD session.

Format

bfd *session-name*

undo bfd *session-name*

Parameters

Parameter	Description	Value
session-name	Specifies the name of a BFD session.	The value is a string of 1 to 15 characters without spaces. **NOTE** When quotation marks are used around the string, spaces are allowed in the string.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To configure the created BFD session, run the **bfd** *session-name* command to enter the specified BFD session view.

Prerequisites

A BFD session has been created by using either of the following commands:

- **bfd bind peer-ip**
- **bfd bind peer-ip default-ip**
- **bfd bind peer-ip source-ip auto**
- **bfd one-arm-echo**

Precautions

The **bfd** *session-name* command displays the BFD session view regardless of whether the BFD session status is Up.

After the functional parameters of the BFD session are set, you must run the **commit** command to make (expect static BFD session with automatically negotiated discriminators), the configurations take effect.

If the BFD session is in the Down state, after you run the **bfd** *session-name* command to enter the BFD session view and set functional parameters, the configurations can immediately take effect after being committed using the **commit** command.

Example

Enter the view of the BFD session named **session**.

```
<HUAWEI> system-view
[HUAWEI] bfd session
[HUAWEI-bfd-session-session]
```

12.1.11 bfd session nonexistent-config-check

Function

The **bfd session nonexistent-config-check enable** command enables the device to check whether the associated BFD session is deleted.

The **undo bfd session nonexistent-config-check disable** command enables the device to check whether the associated BFD session is deleted.

The **bfd session nonexistent-config-check disable** command disables the device from checking whether the associated BFD session is deleted.

By default, the device is enabled to check whether the associated BFD session is deleted.

Format

bfd session nonexistent-config-check enable

undo bfd session nonexistent-config-check disable

bfd session nonexistent-config-check disable

Parameters

None

Views

BFD view

Default Level

2: Configuration level

Usage Guidelines

After BFD for IPv4/IPv6 static routes and association between VRRP/VRRP6/E-Trunk and BFD are configured, deleting the BFD session may cause the association function to become ineffective. You can run the **bfd session nonexistent-config-check enable** command to enable the device to check whether the associated BFD session is deleted. When the associated BFD session is being deleted, the system displays a message indicating that the BFD session cannot be deleted. This function prevents the associated BFD session from being deleted incorrectly.

Example

Disable the device from checking whether the associated BFD session is deleted.

```
<HUAWEI> system-view
[HUAWEI] bfd
[HUAWEI-bfd] bfd session nonexistent-config-check disable
```

12.1.12 commit

Function

The **commit** command commits the BFD session configuration.

Format

commit

Parameters

None

Views

BFD session view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To make the modification on a BFD session take effect, you must run the **commit** command.

Precautions

- To establish a BFD session, the interface bound to the BFD session must be Up and there is a reachable route to the peer IP address.
- If conditions for BFD session setup are not met, the system keeps the configuration entries of the BFD session. The BFD session, however, cannot be established when you use the **commit** command.
- The system periodically scans BFD configuration entries that are committed but not used to establish sessions. If conditions are met, a session is established.
- The number of BFD sessions that can be established in the system is limited. When the number of established BFD sessions reaches the upper limit and you use the **commit** command to commit the configurations of a new BFD session, the system generates a log indicating that the BFD session cannot be established and sends traps.
- After creating a BFD session, if you need to modify session parameters, such as **process-pst**, **process-interface-status**, **min-tx-interval**, **min-rx-interval**, **detect-multiplier**, **tos-exp (BFD session view)**, **wtr**, **description**, **authentication-mode (BFD)**, **trigger if-down delay** or **receiving-admindown trigger if-down** you can directly run the corresponding commands without running the **commit** command, and the modification takes effect immediately.
- After running the **bfd bind peer-ip source-ip auto** command to create configurations for a static BFD session with automatically negotiated discriminators, you do not need to run the **commit** command to commit the configurations. BFD sessions can be automatically established, and relevant configurations are labeled with the commit tags. The **commit** command can still be used but does not take effect.

Example

Commit the BFD session configuration.

```
<HUAWEI> system-view
[HUAWEI] bfd test bind peer-ip default-ip interface gigabitethernet 0/0/1
[HUAWEI-bfd-session-test] discriminator local 22
[HUAWEI-bfd-session-test] discriminator remote 33
[HUAWEI-bfd-session-test] commit
```


12.1.13 dampening timer-interval

Function

The **dampening timer-interval** command configures BFD session flapping suppression timers.

The **undo dampening timer-interval** command restores the default configuration.

BFD session flapping suppression timers start by default.

The default initial, secondary, and maximum BFD session flapping suppression timer values are 2000 ms, 5000 ms, and 12000 ms, respectively.

Format

dampening timer-interval maximum *maximum-milliseconds* **initial** *initial-milliseconds* **secondary** *secondary-milliseconds*

undo dampening timer-interval [**maximum** *maximum-milliseconds* **initial** *initial-milliseconds* **secondary** *secondary-milliseconds*]

Parameters

Parameter	Description	Value
maximum *maximum-milliseconds*	Specifies a maximum BFD session flapping suppression timer value.	The value is an integer ranging from 1 to 3600000, in milliseconds. The default value is 12000.
initial *initial-milliseconds*	Specifies an initial BFD session flapping suppression timer value.	The value is an integer ranging from 1 to 3600000, in milliseconds. The default value is 2000.
secondary *secondary-milliseconds*	Specifies a secondary BFD session flapping suppression timer value.	The value is an integer ranging from 1 to 3600000, in milliseconds. The default value is 5000.

Views

BFD session view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If BFD detects link Down, services are switched. A penalty mechanism is provided to delay BFD session negotiation and prevent frequent service switchovers, protecting link resources and reducing link resource consumption.

To configure BFD session flapping suppression timers, run the **dampening timer-interval** command.

Prerequisites

BFD has been globally enabled using the **bfd** command in the system view.

Configuration Impact

After the **dampening timer-interval** command is run:

1. When a BFD session flaps for the first time, the initial BFD session flapping suppression timer starts. If the BFD session flaps again before the initial BFD session flapping suppression timer expires, BFD session renegotiation is triggered after the initial BFD session flapping suppression timer expires.
2. After the initial BFD session flapping suppression timer ends, the secondary BFD session flapping suppression timer starts. If the BFD session flaps before the secondary BFD session flapping suppression timer expires, BFD session renegotiation is triggered after the secondary BFD session flapping suppression timer expires. After that, the timer value is *secondary-milliseconds* x $2^{(n-1)}$, where *n* is the number of times that the secondary BFD session flapping suppression timer starts.
3. After the timer value of *secondary-milliseconds* x $2^{(n-1)}$ is greater than or equal to the value specified by *maximum-milliseconds*, the BFD session uses the value specified by *maximum-milliseconds* as a flapping delay three consecutive times. Then, the BFD session flapping delay is recalculated based on Step 1.

Precautions

The configured maximum BFD session flapping suppression timer value must be greater than the configured initial or secondary BFD session flapping suppression timer value. Otherwise, the configuration fails.

Do not configure both the **dampening timer-interval** and **wtr** commands. Otherwise, the BFD session recovery period becomes long.

Example

Set a maximum, initial, and secondary BFD session flapping suppression timer values to 20000 ms, 1000 ms, and 3000 ms, respectively.

```
<HUAWEI> system-view
[HUAWEI] bfd
[HUAWEI-bfd] dampening timer-interval maximum 20000 initial 1000 secondary 3000
```

12.1.14 default-ip-address

Function

The **default-ip-address** command configures the default multicast IP address used by all BFD sessions.

The **undo default-ip-address** command restores the default multicast IP address.

By default, BFD uses the multicast IP address 224.0.0.184.

Format

default-ip-address *ip-address*

undo default-ip-address

Parameters

Parameter	Description	Value
ip-address	Specifies the default multicast IP address.	The value ranges from 224.0.0.107 to 224.0.0.250.

Views

BFD view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When using BFD to detect the physical status of a link, you may not specify the peer IP address. In certain situations, the peer such as the member link of the Eth-Trunk is not assigned an IP address. In this case, you need to bind a BFD session to a multicast IP address and send BFD control packets to the multicast IP address.

You must change the default multicast IP address in the following situations:

- On the network, other protocols use the multicast IP address.
- If multiple BFD sessions exist on a path, for example, Layer 3 interfaces are connected through Layer 2 switching devices that support BFD, configure different default multicast IP addresses for the devices where different BFD sessions are established. In this manner, BFD packets can be correctly forwarded.

Prerequisites

BFD has been enabled globally using the **bfd** command in the system view.

Precautions

If the **bfd bind peer-ip default-ip** command has been run in the system view, the **default-ip-address** command cannot be used to change the default BFD multicast address.

Example

Set the default multicast IP address to 224.0.0.150.


```
<HUAWEI> system-view
[HUAWEI] bfd
[HUAWEI-bfd] default-ip-address 224.0.0.150
```

12.1.15 description (BFD session view)

Function

The **description** command configures the description of a BFD session.

The **undo description** command deletes the description of a BFD session.

By default, the description of a BFD session is empty.

Format

description *description*

undo description

Parameters

Parameter	Description	Value
description	Specifies the description of a BFD session.	The value is a string of 1 to 51 case-sensitive characters with spaces.

Views

BFD session view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In practice, multiple BFD sessions need to be configured. To differentiate BFD sessions, run the **description** command to configure a description for a BFD session. A meaningful description is recommended.

Configuration Impact

It is difficult to identify a BFD session that is not configured or whose description is deleted.

Precautions

If you run the **description** command in the same BFD session view multiple times, only the latest configuration takes effect.

The **description** command takes effect only for statically configured BFD sessions but does not take effect for dynamic BFD sessions or BFD sessions with automatically negotiated discriminators.

Example

Set the description of the BFD session named **atoc**.

```
<HUAWEI> system-view
[HUAWEI] bfd atoc
[HUAWEI-bfd-session-atoc] description SwitchA_to_SwitchC
```

12.1.16 detect-multiplier

Function

The **detect-multiplier** command sets the local detection multiplier.

The **undo detect-multiplier** command restores the default local detection multiplier.

By default, the local detection multiplier is 3.

Format

detect-multiplier *multiplier*

undo detect-multiplier

Parameters

Parameter	Description	Value
multiplier	Specifies the local detection multiplier of a BFD session.	The value is an integer that ranges from 3 to 50.

Views

BFD session view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The local detection multiplier determines the detection time of a BFD session.

Detection time = Received Detect Multi of the remote system x Max (Local RMRI/ Received DMTI)

where

- Detect Multi: local detection multiplier, which is set by using the **detect-multiplier** command
- Required Min Rx Interval (RMRI): minimum interval for receiving BFD packets, which is set by using the **min-rx-interval** command
- Desired Min Tx Interval (DMTI): minimum interval for sending BFD packets, which is set by using the **min-tx-interval** command

You can increase or reduce the local detection multiplier based on actual networking. On a stable link, there is no need to frequently detect the link status, so you can increase the local detection multiplier.

If no BFD packet is received from the peer device within the detection time, the link is considered as faulty and the BFD session enters the Down state. To reduce the usage of system resources, when the BFD session is detected in Down state, the system adjusts the sending interval to a random value greater than 1000 ms. When the BFD session becomes Up, the configured interval is restored.

Configuration Impact

- On an unstable link, if the local detection multiplier is small, the BFD session may flap. It is recommended that a larger local detection multiplier be used.
- When other protocols are associated with BFD, if a larger local detection multiplier is used, the BFD session takes a long period of time to detect faults on the link and traffic is switched to the backup link after the specified period. Packets may be lost during this period.

Precautions

Both ends of a BFD session can use different local detection multipliers.

Example

Set the local detection multiplier of the BFD session **atoc** to 10.

```
<HUAWEI> system-view
[HUAWEI] bfd atoc
[HUAWEI-bfd-session-atoc] detect-multiplier 10
```

12.1.17 discriminator

Function

The **discriminator** command sets local and remote discriminators for a static BFD session.

Format

discriminator { **local** *discr-value* | **remote** *discr-value* }

Parameters

Parameter	Description	Value
local *discr-value*	Specifies the local discriminator of a BFD session	The value is an integer that ranges from 1 to 8191.
remote *discr-value*	Specifies the remote discriminator of a BFD session	The value is an integer that ranges from 1 to 4294967295.

Views

BFD session view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When creating a static BFD session, run the **discriminator** command to set local and remote discriminators. Otherwise, the static BFD session cannot be set up. The local and remote discriminators differentiate BFD sessions between two systems.

Precautions

- Only static BFD sessions require settings of local and remote discriminators.
- The local discriminator of the local system and the remote discriminator of the remote system must be the same. If the local discriminator of the local system and the remote discriminator of the remote system are different, a static BFD session cannot be set up.
- After the local and remote discriminators of a static BFD session are configured, the local and remote discriminators cannot be modified. To modify the local and remote discriminators of a static BFD session, delete the BFD session and reconfigure the local and remote discriminators.

Example

Set the local discriminator of a BFD session to 80 and the remote discriminator to 800.

```
<HUAWEI> system-view
[HUAWEI] bfd atoc
[HUAWEI-bfd-session-atoc] discriminator local 80
[HUAWEI-bfd-session-atoc] discriminator remote 800
```

12.1.18 display bfd configuration

Function

The **display bfd configuration** command displays the BFD session configuration.

Format

display bfd configuration { **all** | **static** } [**for-lsp** | **for-pw** | **for-te** | **for-vsi-pw**] [**verbose**] (S5731-H, S5731-S, S5731S-S, S6730-S, S6730S-S, S5731S-H, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730S-H and S6730-H)

display bfd configuration { **ldp-lsp peer-ip** *ip-address* **nexthop** *nexthop* [**interface** *interface-type interface-number*] | **static-lsp** *lsp-name* } [**verbose**] (S5731-H, S5731-S, S5731S-S, S6730-S, S6730S-S, S5731S-H, S5732-H, S6720-EI, S6720S-EI, S6730S-H and S6730-H)

display bfd configuration mpls-te interface *interface-type interface-number* [**te-lsp**] [**verbose**](S5731-H, S5731-S, S5731S-S, S6730-S, S6730S-S, S5731S-H, S5732-H, S6720-EI, S6720S-EI, S6730S-H and S6730-H)

display bfd configuration pw interface *interface-type interface-number* [**secondary**] [**verbose**](S5731-H, S5731-S, S5731S-S, S6730-S, S6730S-S, S5731S-H, S5732-H, S6720-EI, S6720S-EI, S6730S-H and S6730-H)

display bfd configuration vsi-pw vsi *vsi-name* **peer** *peer-address* [**vc-id** *vc-id*] [**verbose**](S5731-H, S5731-S, S5731S-S, S6730-S, S6730S-S, S5731S-H, S5732-H, S6720-EI, S6720S-EI, S6730S-H and S6730-H)

display bfd configuration passive-dynamic [**peer-ip** *ip-address* **remote-discriminator** *discriminator*] [**verbose**] (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)

display bfd configuration { **static name** *session-name* | **dynamic** | **static-auto** | **peer-ip** { **default-ip** | *ip-address* [**vpn-instance** *vpn-instance-name*] } | **discriminator** *local-discr-value* } [**verbose**]

display bfd configuration peer-ipv6 *ipv6-address* [**vpn-instance** *vpn-instance-name*] [**verbose**]

display bfd configuration { **all** | **static** } **[for-ip** | **for-ipv6**] [**verbose**]

Parameters

Parameter	Description	Value
all	Displays the configurations of all BFD sessions.	-
static	Displays the configurations of static BFD sessions.	-

Parameter	Description	Value
for-vsi-pw	Displays the configurations of the BFD sessions for detecting VSI PWs.	-
for-ip	Displays the configurations of the BFD sessions for detecting IP links.	-
for-lsp	Displays the configurations of the BFD sessions for detecting LSPs.	-
for-pw	Displays the configurations of the BFD sessions for detecting PWs.	-
for-te	Displays the configurations of the BFD sessions for detecting TE tunnels.	-
vsi-pw	Displays the configurations of the BFD sessions for detecting VSI PWs.	-
vsi *vsi-name*	Displays the configuration of the BFD session with the specified VSI instance name.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
peer *peer-address*	Displays the configuration of the BFD session for detecting a VSI PW with the specified peer IPv4 address.	The value is in dotted decimal notation.
peer-ip *ip-address*	Displays the configuration of the BFD session bound to the specified peer IP address.	-

Parameter	Description	Value
vc-id *vc-id*	Displays the configuration of the BFD session with the specified VC ID.	The value is an integer that ranges from 1 to 4294967295.
passive-dynamic	Displays the configurations of the BFD sessions dynamically created by the end in passive mode.	-
remote-discriminator *discriminator*	Displays the configuration of the BFD session with the local discriminator of the source device initiating the BFD session.	The value is an integer that ranges from 1 to 4294967295.
verbose	Displays detailed BFD configurations.	-
name *session-name*	Displays the configuration of the static BFD session with the specified name.	The value is a string of 1 to 15 characters without spaces. **NOTE** If the string is enclosed within double quotation marks ("), the string can contain spaces.
dynamic	Displays dynamic BFD configurations and the configurations of static BFD sessions with automatically negotiated discriminators.	-
discriminator *local-discr-value*	Displays the configuration of the BFD session with the specified local discriminator.	The value is an integer that ranges from 1 to 16383.
default-ip	Displays statistics about multicast BFD sessions.	-
vpn-instance *vpn-instance-name*	Displays the configuration of the BFD session bound to a specified VPN instance.	The value must be an existing VPN instance name.

Parameter	Description	Value
static-auto	Displays the configuration of the static BFD session with the automatically negotiated discriminators.	-
ldp-lsp	Displays the configurations of the BFD sessions for detecting LDP LSPs.	-
nexthop *nexthop*	Displays the configuration of the BFD session with the specified next hop address.	The value is in dotted decimal notation.
interface-type interface-number	Displays BFD binding information on the specified interface. • *interface-type* specifies the interface type. • *interface-number* specifies the interface number.	-
static-lsp	Displays the configurations of the BFD sessions for detecting static LSPs.	-
lsp-name	Displays the configuration of the BFD session for detecting the static LSP with the specified name.	The value is a string of 1 to 19 case-sensitive characters.
mpls-te	Displays the configurations of the BFD sessions for detecting MPLS TE tunnels.	-
te-lsp	Displays the configuration of the BFD session for detecting the primary LSP bound to a TE tunnel.	-

Parameter	Description	Value
pw	Displays the configurations of the BFD sessions for detecting PWs.	-
secondary	Displays the configuration of the BFD session for detecting the secondary PW.	-
peer-ipv6 *ipv6-address*	Displays the configuration of the BFD6 session bound to a specified IPv6 address.	-
for-ipv6	Displays the configurations of static or all BFD6 sessions.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

When multiple BFD sessions exist, you can view information about certain BFD sessions by specifying the parameters such as the type, name, and peer IP address.

Precautions

If a static BFD session with automatically negotiated discriminators and a dynamic BFD session share the same configurations, you can view that the shared session configurations by BFD session type (static and dynamic).

Example

Display the configurations of all BFD sessions.

```
<HUAWEI> display bfd configuration all
--------------------------------------------------------------------------------
CFG Name       CFG Type      LocalDiscr MIndex    SessNum  Commit   AdminDown
--------------------------------------------------------------------------------
atob           S_IP_PEER     -          512       0        False    False
test           S_IP_PEER     1          513       0        False    False
zzz            S_IP_IF       3          514       0        False    False
--------------------------------------------------------------------------------
    Total Commit/Uncommit CFG Number : 0/3
```


Table 12-1 Description of the display bfd configuration command output

Item	Specification
CFG Name	BFD session name.
CFG Type	BFD session setup type: • S_IP_IF: indicates a single-hop BFD session that is established statically and bound to an interface. • S_IP_PEER: indicates a multi-hop BFD session that is established statically. • S_STA_LSP: indicates a BFD session that is established statically and used for detecting an LSP. • S_LDP_LSP: indicates a BFD session that is established statically and used for detecting an LDP LSP. • S_TE_LSP: indicates a BFD session that is statically established and used for detecting a TE LSP. • S_TE_TNL: indicates a BFD session that is statically established and used for detecting a TE tunnel. • S_PW: indicates a BFD session that is statically established and used for detecting a PW. • S_VSI_PW: indicates a BFD session that is statically established and used for detecting a VSI PW. • Dynamic: indicates a BFD session that is dynamically established. • Entire_Dynamic: indicates a BFD session that is entirely and dynamically established. • S_AUTO_IF: indicates a static single-hop BFD session with automatically negotiated discriminators. • S_AUTO_PEER: indicates a static multi-hop BFD session with automatically negotiated discriminators.
LocalDiscr	Local discriminator of the BFD session. To set the local discriminator of the BFD session, run the **discriminator** command.
MIndex	Configuration entry index of a BFD session.
SessNum	Number of BFD sessions in a configuration entry.
Commit	Flag of enabling a BFD session. After you run the **commit** command to commit configurations in the BFD session view, the flag is displayed as **True**. Otherwise, it is displayed as **False**.

Item	Specification
AdminDown	Flag of the management status of a BFD session. After you run the **shutdown (BFD session view)** command to disable the local session in the BFD session view, the flag is displayed as **True**. Otherwise, it is displayed as **False**.
Total Commit/ Uncommit CFG Number	Total number of BFD sessions that are committed through the **commit** command in the BFD session view and total number of BFD sessions that are not committed.

Display detailed configurations of all BFD sessions.

```
<HUAWEI> display bfd configuration all verbose
--------------------------------------------------------------------------------
 BFD Session Configuration Name : atob
--------------------------------------------------------------------------------
 Local Discriminator    : -              Remote Discriminator   : -
 BFD Bind Type          : Peer IP Address
 Bind Session Type      : Static
 Bind Peer IP Address   : 192.168.1.9
 Bind Interface         : -
 Select Board           : -
 Track Interface        : -
 TOS-EXP                : 7              Local Detect Multi     : 3
 Min Tx Interval (ms)   : 1000           Min Rx Interval (ms)   : 1000
 WTR Interval (ms)      : -              Process PST            : Disable
 Proc Interface Status  : Disable
 Bind Application       : No Application Bind
 Session Description    : -
 Session Create Status  : Failed(65532)
--------------------------------------------------------------------------------

--------------------------------------------------------------------------------
 BFD Session Configuration Name : test
--------------------------------------------------------------------------------
 Local Discriminator    : 1              Remote Discriminator   : 2
 BFD Bind Type          : Peer IP Address
 Bind Session Type      : Static
 Bind Peer IP Address   : 192.168.10.2
 Bind Interface         : -
 Select Board           : -
 Track Interface        : -
 TOS-EXP                : 7              Local Detect Multi     : 3
 Min Tx Interval (ms)   : 1000           Min Rx Interval (ms)   : 1000
 WTR Interval (ms)      : -              Process PST            : Disable
 Proc Interface Status  : Disable
 Bind Application       : No Application Bind
 Session Description    : -
 Session Create Status  : Failed(65532)
--------------------------------------------------------------------------------

--------------------------------------------------------------------------------
 BFD Session Configuration Name : zzz
--------------------------------------------------------------------------------
 Local Discriminator    : 3              Remote Discriminator   : 4
 BFD Bind Type          : Interface(GigabitEthernet0/0/1)
 Bind Session Type      : Static
 Bind Peer IP Address   : 192.168.20.4
 Bind Interface         : GigabitEthernet0/0/1
 TOS-EXP                : 7              Local Detect Multi     : 3
```



```
Min Tx Interval (ms)   : 1000          Min Rx Interval (ms)   : 1000
WTR Interval (ms)      : -             Process PST            : Disable
Auth Key ID            : -             Auth Timer             : -
Meticulous Auth        : False         Auth Type              : None
Proc Interface Status  : Enable
Bind Application       : IFNET
Session Description    : -
Session Create Status  : Failed(65532)
------------------------------------------------------------------------------

  Total Commit/Uncommit CFG Number : 0/3
```

Table 12-2 Description of the display bfd configuration all verbose command output

Item	Specification
BFD Session Configuration Name	BFD session name.
Local Discriminator	Local discriminator of a BFD session. To set the local discriminator of a BFD session, run the **discriminator** command.
Remote Discriminator	Remote discriminator of a BFD session. To set the remote discriminator of a BFD session, run the **discriminator** command.
BFD Bind Type	BFD session binding type: ● Peer IP Address: indicates multi-hop BFD for an IP link. ● Interface: indicates single-hop BFD for an IP link. ● STATIC_LSP: indicates that a static LSP is detected. ● LDP_LSP: indicates that an LDP LSP is detected. ● TE_LSP: indicates that an LSP bound to a TE tunnel is detected. ● TE_TUNNEL: indicates that a TE tunnel is detected. ● PW: indicates that a PW is detected. ● VSI_PW: indicates that a VSI PW is detected.

Item	Specification
Bind Session Type	Mode in which a BFD session is established: ● Static: indicates the BFD sessions that are established through the static configurations. ● Dynamic: indicates the BFD sessions that are triggered dynamically. ● Static_Auto: indicates the statically established BFD sessions with automatically negotiated discriminators. ● Entire_Dynamic: indicates the BFD sessions that are entirely and dynamically triggered.
Bind Peer Ip Address	Peer IP address of a BFD session or multicast IP address bound to a BFD session.
Bind Interface	Local interface bound to a BFD session.
Track Interface	Interface tracked by the BFD session.
TOS-EXP	Priority of a BFD packet. To set the priority of a BFD packet, run the **tos-exp** command.
Local Detect Multi	Local detection multiplier. To set the local detection multiplier, run the **detect-multiplier** command.
Min Tx Interval (ms)	Minimum interval for sending BFD packets. To set the minimum interval for sending BFD packets, run the **min-tx-interval** command.
Min Rx Interval (ms)	Minimum interval for receiving BFD packets. To set the minimum interval for receiving BFD packets, run the **min-rx-interval** command.
WTR Interval (ms)	WTR time. To set the WTR time, run the **wtr** command.
Process PST	Flag for processing the Port Status Table (PST). If the **process-pst** command is configured, this field is displayed as **Enable**. Otherwise, it is displayed as **Disable**.
Auth Key ID	Authentication key ID of a BFD session.
Auth Timer	Negotiation timeout period of a BFD session, in seconds.
Meticulous Auth	Authentication flag ● **True**: strict ● **False**: non-strict

Item	Specification
Auth Type	BFD authentication type: • **NONE**: no authentication • **SIMPLE**: simple password authentication • **MD5**: MD5 authentication • **MMD5**: meticulous MD5 authentication • **SHA1**: SHA1 authentication • **MSHA1**: meticulous SHA1 authentication
Proc interface status	Flag of association between the BFD session status and the interface status. If the **process-interface-status** command is configured, this field is displayed as Enable. Otherwise, it is displayed as **Disable**.
Bind Application	Application bound to the BFD session.
Session Description	Description of the BFD session. To set the description of the BFD session, run the **description** command.
Session Create Status	Status of BFD session creation: • Success • Failed
Total Commit/Uncommit CFG Number	Total number of BFD sessions that are committed through the **commit** command in the BFD session view and total number of BFD sessions that are not committed.

12.1.19 display bfd interface

Function

The **display bfd interface** command displays information about a BFD-enabled interface.

Format

display bfd interface [*interface-type interface-number*]

Parameters

Parameter	Description	Value
interface-type interface-number	Specifies the type and number of the interface bound to the BFD session. • *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

Usage Scenario

The **display bfd interface** command displays information about a BFD-enabled interface, including the BFD session bound to the interface and the BFD session status.

Example

Display information about a BFD-enabled interface.

```
<HUAWEI> display bfd interface
------------------------------------------------------------------------------
Interface Name          MIndex       Sess-Count      BFD-State
------------------------------------------------------------------------------
Vlanif100               256          1               up
------------------------------------------------------------------------------
    Total Interface Number : 1
```

Table 12-3 Description of the display bfd interface command output

Item	Description
Interface Name	Name of the BFD-enabled interface.
MIndex	Index of the interface entry.
Sess-Count	Number of BFD sessions bound to the interface.

Item	Description
BFD-State	BFD status of an interface. The value can be up or down. **NOTE** If a BFD session is bound to the interface and configured with the **process-interface-status** command, the BFD session's status is displayed (The interface is up when the BFD session is in the AdminDown or Receive AdminDown state). Otherwise, the interface's physical status is displayed. If multiple BFD sessions are bound to the interface, only one BFD session can be configured with the **process-interface-status** command.
Total Interface Number	Number of the BFD-enabled interface.

12.1.20 display bfd session

Function

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

Format

display bfd session { **dynamic** | **discriminator** *discr-value* | **peer-ip** { **default-ip** | *ip-address* [**vpn-instance** *vpn-instance-name*] } | **static-auto** } [**verbose**]

display bfd session { **all** | **static** } [**for-lsp** | **for-pw** | **for-te** | **for-vsi-pw**] [**verbose**](S5731-H, S5731-S, S5731S-S, S6730-S, S6730S-S, S5731S-H, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730S-H and S6730-H)

display bfd session { **ldp-lsp peer-ip** *ip-address* **nexthop** *ip-address* [**interface** *interface-type interface-number*] | **static-lsp** *lsp-name* } [**verbose**] (S5731-H, S5731-S, S5731S-S, S6730-S, S6730S-S, S5731S-H, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730S-H and S6730-H)

display bfd session mpls-te interface *interface-type interface-number* [**te-lsp**] [**verbose**] (S5731-H, S5731-S, S5731S-S, S6730-S, S6730S-S, S5731S-H, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730S-H and S6730-H)

display bfd session pw interface *interface-type interface-number* [**secondary**] [**verbose**] (S5731-H, S5731-S, S5731S-S, S6730-S, S6730S-S, S5731S-H, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730S-H and S6730-H)

display bfd session passive-dynamic [**peer-ip** *ip-address* **remote-discriminator** *remote-discr-value*] [**verbose**] (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)

display bfd session { **vsi-pw vsi** *vsi-name* **peer** *peer-address* [**vc-id** *vc-id*] } [**verbose**] (S5731-H, S5731-S, S5731S-S, S6730-S, S6730S-S, S5731S-H, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730S-H and S6730-H)

display bfd session peer-ipv6 *ipv6-address* [**vpn-instance** *vpn-instance-name*] [**verbose**]

display bfd session { **all** | **static** } **[for-ip** | **for-ipv6**] [**verbose**]

Parameters

Parameter	Description	Value
all	Displays information about all BFD sessions.	-
static	Displays information about all static BFD sessions.	-
for-ip	Displays information about the BFD sessions for detecting IP links.	-
for-lsp	Displays information about the BFD sessions for detecting LSPs.	-
for-pw	Displays information about the BFD sessions for detecting PWs.	-
for-te	Displays information about the BFD sessions for detecting TE tunnels.	-
for-vsi-pw	Displays information about the BFD sessions for detecting VSI PWs.	-
vsi-pw	Displays information about the BFD session for detecting a VSI PW.	-
vsi-name	Displays information about the BFD session with the specified VSI instance name.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
peer *peer-address*	Displays information about the BFD session for detecting a VSI PW with the specified peer IPv4 address.	The value is in dotted decimal notation.

Parameter	Description	Value
nexthop *ip-address*	Displays information about the BFD session with the specified next hop address.	The value is in dotted decimal notation.
interface *interface-type interface-number*	Displays information about the BFD session with the specified outbound interface.	-
vc-id *vc-id*	Displays information about the BFD session with the specified VC ID.	The value is a decimal integer ranging from 1 to 4294967295.
verbose	Displays detailed information about BFD sessions.	-
dynamic	Displays information about all dynamic BFD sessions and static BFD sessions negotiated with discriminators.	-
passive-dynamic	Displays information about all dynamic BFD sessions created on the end in passive mode.	-
discriminator *discr-value*	Displays information about the BFD session with a specified discriminator. You can specify only a local discriminator.	The value is an integer that ranges from 1 to 16383.
remote-discriminator *remote-discr-value*	Displays information about the BFD session with a specified discriminator. You can specify only a remote discriminator.	The value is an integer that ranges from 1 to 4294967295.
peer-ip *ip-address*	Displays information about the BFD session bound to the specified peer IP address.	The value is in dotted decimal notation.
default-ip	Displays statistics about multicast BFD sessions.	-

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Displays information about the BFD session bound to the specified VPN instance.	The value must be an existing VPN instance name.
static-auto	Displays the information about the static BFD sessions with the automatically negotiated discriminators.	-
ldp-lsp	Displays information about the BFD sessions for detecting LDP LSPs.	-
static-lsp	Displays information about the BFD sessions for detecting static LSPs.	-
lsp-name	Displays information about the BFD session for detecting the static LSP with the specified name.	The value is a string of 1 to 19 case-sensitive characters without spaces.
mpls-te	Displays information about the BFD sessions for detecting MPLS TE tunnels.	-
te-lsp	Displays information about the BFD session for detecting the primary LSP bound to a TE.	-
pw	Displays information about the BFD sessions for detecting PWs.	-
secondary	Displays information about the BFD session for detecting the secondary PW.	-
peer-ipv6 *ipv6-address*	Displays information about the BFD6 session bound to a specified IPv6 address.	-
for-ipv6	Displays information about static or all BFD6 sessions.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

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

Prerequisites

BFD has been enabled globally.

Precautions

- When a BFD session changes from Down to Up, if the WTR time of the session is not 0, BFD sends a notification that the session becomes Up only after the WTR time expires.
- If a static BFD session with automatically negotiated discriminators and a dynamic BFD session are bound to the same peer IP address, the **display bfd session** command displays the same entry for the static BFD session or dynamic BFD session.

Example

Display the summary of all BFD sessions.

```
<HUAWEI> display bfd session all
--------------------------------------------------------------------------------
Local Remote     PeerIpAddr      State     Type        InterfaceName
--------------------------------------------------------------------------------
10    11         10.10.10.2      Up        S_IP_IF     Vlanif31
8192  0          10.10.10.2      Down      S_AUTO_IF   Vlanif31
--------------------------------------------------------------------------------
    Total UP/DOWN Session Number : 1/1
```

Table 12-4 Description of the display bfd session command output

Item	Description
Local	Local discriminator of the BFD session. To set the local discriminator, run the **discriminator** command.
Remote	Remote discriminator of the BFD session. To set the remote discriminator, run the **discriminator** command.
PeerIpAddr	Peer IP address bound to the BFD session.

Item	Description
InterfaceName	Outbound interface bound to the BFD session. In multi-hop BFD, this field is displayed as - because no interface is bound to a BFD session.
State	BFD session status: ● Init: The BFD session is in the initialized state. ● Up: indicates that the BFD session is in Up state. ● Down: indicates that the BFD session is in Down state. ● AdmDown: indicates that a BFD session is AdminDown when the **shutdown (BFD session view)** command is run.

Item	Description
Type	BFD session type: • S_TE_LSP: indicates a BFD session that is established statically and bound to a TE LSP. • S_TE_TNL: indicates a BFD session that is established statically and bound to a TE tunnel. • S_IP_PEER: indicates a BFD session that is established statically and bound to an IP link. • S_IP_IF: indicates a BFD session that is established statically and bound to an interface. • S_LDP_LSP: indicates a BFD session that is established statically and bound to a dynamic LSP. • S_PW(M): indicates a BFD session that is established statically and bound to the primary PW. • S_PW(S): indicates a BFD session that is established statically and bound to the secondary PW. • S_STA_LSP: indicates a BFD session that is established statically and bound to a static LSP. • S_VSI_PW: indicates a BFD session that is established statically and bound to a VSI PW. • D_IP_PEER: indicates a BFD session that is created dynamically and bound to an IP link. • D_IP_IF: indicates a BFD session that is established dynamically and bound to an interface. • D_LDP_LSP: indicates a BFD session that is established dynamically and bound to a dynamic LSP. • D_TE_LSP: indicates a BFD session that is established dynamically and bound to a TE LSP. • D_PW(S): indicates a BFD session that is established dynamically and bound to the secondary PW. • D_PW(M): indicates a BFD session that is established dynamically and bound to the primary PW. • E_Dynamic: indicates a BFD session that is established entirely and dynamically. After you enable the function of dynamically establishing a BFD session on the destination of an LSP, this session type is created. • S_AUTO_IF: indicates a static single-hop BFD session with automatically negotiated discriminators. • S_AUTO_PEER: indicates a static multi-hop BFD session with automatically negotiated discriminators.
Total UP/ DOWN Session Number	Number of BFD sessions in Up or Down state.

Display detailed information about all BFD sessions.

```
<HUAWEI> display bfd session all verbose
--------------------------------------------------------------------------------
Session MIndex : 16384     (One Hop) State : Up        Name : test
--------------------------------------------------------------------------------
 Local Discriminator    : 111             Remote Discriminator   : 222
 Session Detect Mode    : Asynchronous Mode Without Echo Function
 BFD Bind Type          : Interface(Vlanif500)
 Bind Session Type      : Static
 Bind Peer IP Address   : 224.0.0.184
 NextHop Ip Address     : 224.0.0.184
 Bind Interface         : Vlanif500
 FSM Board Id           : 6               TOS-EXP               : 6
 Min Tx Interval (ms)   : 10              Min Rx Interval (ms)  : 10
 Actual Tx Interval (ms): 10              Actual Rx Interval (ms): 10
 Local Detect Multi     : 3               Detect Interval (ms)  : 30
 Echo Passive           : Disable         Acl Number            : -
 Destination Port       : 3784            TTL                   : 255
 Proc Interface Status  : Disable         Process PST           : Disable
 WTR Interval (ms)      : -
 Active Multi           : 3               DSCP                  : -
 Auth Key ID            : 1               Auth Timer            : 0
 Meticulous Auth        : True            Auth Type             : MSHA1
 Xmit Auth Seq          : 0x5cb3cbed      Rcv Auth Seq          : 0x28909183
 Error Packet Info      : Correct Pkt
 Last Local Diagnostic  : No Diagnostic
 Bind Application       : No Application Bind
 Session TX TmrID       : -               Session Detect TmrID  : -
 Session Init TmrID     : -               Session WTR TmrID     : -
 Session Echo Tx TmrID  : -
 PDT Index              : FSM-B030000 | RCV-0 | IF-B030000 | TOKEN-0
 Session Description    : -
 Trigger If-down Delay Time (s)     : -
 Receiving-admindown Trigger If-down : Disable
--------------------------------------------------------------------------------

   Total UP/DOWN Session Number : 1/0
```

Table 12-5 Description of the display bfd session all verbose command output

Item	Description
Session MIndex	Index of BFD session entries.
State	Status of a BFD session.
Name	Name of a BFD session.
Local Discriminator	Local discriminator of the BFD session. To set the local discriminator of the BFD session, run the **discriminator** command.
Remote Discriminator	Remote discriminator of the BFD session. To set the remote discriminator of the BFD session, run the **discriminator** command.

Item	Description
Session Detect Mode	BFD detection modes: • Asynchronous Mode Without Echo Function: indicates the asynchronous mode without the echo function. • Demand Mode Without Echo Function: indicates the demand mode without the echo function.
BFD Bind Type	BFD session binding type: • STATIC_LSP: indicates that a static LSP is detected. • LDP_LSP: indicates that an LDP LSP is detected. • TE_TUNNEL: indicates that a TE tunnel is detected. • TE_LSP: indicates that an LSP bound to a TE is detected. • PW: indicates that a PW is detected. • Peer IP Address: indicates that a multi-hop IP link is detected. • When one-hop BFD is used to detect an IP link, this field is displayed as **Interface** and the name of the bound local interface. • VSI_PW: indicates that a VSI PW is detected. • Static_Auto: indicates the BFD session with automatically negotiated discriminators.
Bind Session Type	Indicates the ways of establishing BFD sessions: • Static: indicates that a BFD session is established manually. • Dynamic: indicates that a BFD session is established dynamically. • Static_Auto: indicates that a BFD session is established with automatically negotiated discriminators. • Entire_Dynamic: indicates that a BFD session is triggered entirely and dynamically. After you enable the function of dynamically establishing a BFD session on the destination of an LSP, this session type is created.
Bind Peer Ip Address	Peer IP address bound to the BFD session.
NextHop Ip Address	IP address of the next hop.
Bind Interface	Outbound interface bound to the BFD session.

Item	Description
Bind Source Ip Address	Source IP address of the local interface bound to the BFD session. This field can be displayed only when the source IP address is specified for the BFD session that is created by running the **bfd bind peer-ip** or **bfd bind peer-ip default-ip** command.
FSM Board Id	Number of the processing board where the state machine works.
TOS-EXP	Priority of a BFD packet. To set the priority of a BFD packet, run the **tos-exp** command.
Min Tx Interval (ms)	Configured minimum interval for sending BFD packets. To set the minimum interval for sending BFD packets, run the **min-tx-interval** command.
Min Rx Interval (ms)	Configured minimum interval for receiving BFD packets. To set the minimum interval for receiving BFD packets, run the **min-rx-interval** command.
Actual Tx Interval (ms)	Actual minimum interval for sending BFD packets.
Actual Rx Interval (ms)	Actual minimum interval for receiving BFD packets.
Local Detect Multi	Local detection multiplier. To set the local detection multiplier, run the **detect-multiplier** command.
Detect Interval (ms)	BFD detection time.
Echo Passive	Whether the BFD passive Echo function is enabled: • Enable • Disable
Acl Number	ACL rule number
Destination Port	Number of the destination port of the BFD session packet. The single-hop BFD control packet uses destination port 3784 and the multi-hop BFD control packet uses 3784 or 4784.
TTL	TTL value of the BFD packet.
WTR Interval (ms)	WTR time of the BFD session. To set the WTR time of the BFD session, run the **wtr** command.

Item	Description
Process PST	Flag for processing the Port Status Table (PST). If the **process-pst** command is configured, this field is displayed as **Enable**. Otherwise, it is displayed as **Disable**.
Proc interface status	Flag of association between the BFD session status and the interface status. If the **process-interface-status** command is configured, this field is displayed as **Enable**. Otherwise, it is displayed as **Disable**.
Active Multi	Detection multiplier that is effective.
DSCP	DSCP value in the BFD session. The value ranges from 1 to 63. The value - indicates that the DSCP value does not take effect in the BFD session.
Auth Key ID	Authentication key ID of a BFD session
Auth Timer	Negotiation timeout period of a BFD session, in seconds
Meticulous Auth	Authentication flag ● **True**: strict ● **False**: non-strict
Auth Type	BFD authentication type: ● **NONE**: no authentication ● **SIMPLE**: simple password authentication ● **MD5**: MD5 authentication ● **MMD5**: meticulous MD5 authentication ● **SHA1**: SHA1 authentication ● **MSHA1**: meticulous SHA1 authentication
Xmit Auth Seq	Local sequence number of a BFD authentication session
Rcv Auth Seq	Remote sequence number of a BFD authentication session

Item	Description
Error Packet Info	Packet error information: • **Correct Pkt**: The packet is correct. • **Incorrect authentication type**: The authentication type is incorrect. • **Incorrect authentication length**: The authentication length is incorrect. • **Incorrect sequence number**: The sequence number is incorrect. • **Authentication failed**: The authentication fails. • **Incorrect authentication keyid**: The authentication key ID is incorrect. • **Local does not configure authentication**: Authentication is not configured at the local end. • **Remote does not configure authentication**: Authentication is not configured at the remote end.
Last Local Diagnostic	Local diagnostic cause for the last BFD session in Down state.
Bind Application	Application bound to the BFD session.
Session TX TmrID	Timer used for a BFD session to send packets.
Session Detect TmrID	BFD session detection timer.
Session Init TmrID	Timer for state machine initialization of a BFD session.
Session WTR TmrID	WTR timer of a BFD session.
Session Echo Tx TmrID	Timer used for a BFD session to send Echo packets.
PDT Index	Product information.
Session Description	Description of the BFD session. To set the description of the BFD session, run the **description** command.
Trigger If-down Delay Time (s)	Delay for a device to instruct the interface protocol to go down after the device detects a BFD down event, in seconds.
Receiving-admindown Trigger If-down	Whether the local device is enabled to instruct the interface protocol to go down upon receipt of an AdminDown packet.
Total UP/DOWN Session Number	Number of BFD sessions in Up or Down state.

12.1.21 display bfd statistics

Function

The **display bfd statistics** command displays global BFD statistics.

Format

display bfd statistics

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

The **display bfd statistics** command displays global BFD statistics.

Precautions

Before using the **display bfd statistics** command to view BFD statistics within a specified period, run the **reset bfd statistics** command to clear existing statistics.

Example

Display global BFD statistics.

```
<HUAWEI> display bfd statistics
Current Display Board Number : Main; Current Product Register Type : S5730-36C-HI
IP Multihop Destination Port : 3784
Total Up/Down Session Number : 1/1
Current Session Number :
     Static session     : 2              Dynamic session        : 0
     E_Dynamic session  : 0                STATIC_AUTO session    : 0
     LDP_LSP session    : 0              STATIC_LSP session     : 0
     TE_TUNNEL session  : 0                TE_LSP session         : 0
     PW session         : 0              IP session             : 2
     VSI PW session     : 0              LDP_TUNNEL session     : 0
     BGP_TUNNEL session : 0
------------------------------------------------------------------------------
PAF/LCS Name                    Maxnum        Minnum        Create
------------------------------------------------------------------------------
BFD_CFG_NUM                       256           1             2
BFD_IF_NUM                      256           1             1
BFD_SESSION_NUM                   256           1             2
BFD_IO_SESSION_NUM                256           1             -
BFD_PER_TUNNEL_CFG_NUM            8             1             -
------------------------------------------------------------------------------
IO Board Current Created Session Statistics Information :(slot/number)
```



```
-------------------------------------------------------------------------------
            0/2
-------------------------------------------------------------------------------
Current Total Used Discriminator Num              : 2
-------------------------------------------------------------------------------
IO Board Reserved Sessions Number Information :(slot/number)
-------------------------------------------------------------------------------
            0/0
-------------------------------------------------------------------------------
BFD HA Information :
-------------------------------------------------------------------------------
Core Current HA Status                    : Slave Not Ready
Shell Current HA Status                   : Slave Not Ready
-------------------------------------------------------------------------------
BFD for LSP Information :
-------------------------------------------------------------------------------
Ability of auto creating BFD session on egress     : Disable
Period of LSP Ping                        : 60
System Session Delay Up Timer                     : OFF
-------------------------------------------------------------------------------
```

Table 12-6 Description of the display bfd statistics command output

Item	Description
Current Display Board Number	Number of the board where information is displayed.
Current Product Register Type	Type of the current product.
IP Multihop Destination Port	UDP port number.
Total Up/Down Session Number	Total number of BFD sessions in Up or Down state.
Current Session Number	Number of current BFD sessions.
Static session	Number of static BFD sessions.
Dynamic session	Number of dynamic BFD sessions.
E_Dynamic session	Number of entirely dynamic sessions.
STATIC_AUTO session	Number of BFD sessions with automatically negotiated discriminators.
LDP_LSP session	Number of BFD sessions for detecting an LDP LSP.
STATIC_LSP session	Number of BFD sessions for detecting a static LSP.
TE_TUNNEL session	Number of BFD sessions for detecting a TE tunnel.
TE_LSP session	Number of BFD sessions for detecting a TE LSP.
PW session	Number of BFD sessions for detecting a PW.
IP session	Number of BFD sessions for detecting an IP address.

Item	Description
LDP_TUNNEL session	Number of current BFD sessions for LDP tunnel
BGP_TUNNEL session	Number of current BFD sessions for BGP tunnel
PAF/LCS Name	Project name of the license file.
BFD_CFG_NUM	Maximum number of BFD sessions that can be globally configured.
BFD_IF_NUM	Maximum number of BFD sessions that can be bound to an interface.
BFD_SESSION_NUM	Maximum number of BFD sessions that can be globally established.
BFD_IO_SESSION_NUM	Maximum number of BFD sessions that can be established globally.
BFD_PER_TUNNEL_CFG_NUM	Maximum number of BFD sessions that can be configured on a tunnel.
IO Board Current Created Session Statistics Information : (slot/number)	Number of BFD sessions that are established.
Current Total Used Discriminator Num	Total number of currently configured discriminators.
IO Board Reserved Sessions Number Information : (slot/number)	Number of BFD sessions that are reserved.
BFD HA Information	-
Core Current HA Status	HA status in the core: ● Normal: indicates that the HA status is normal. ● Batch Backup Going: indicates that backup is being performed. ● Slave Not Ready: indicates that the slave board is not ready. ● Smooth Going: indicates that smooth processing is being performed.

Item	Description
Shell Current HA Status	HA status in the shell: • Normal: indicates that the HA status is normal. • Batch Backup Going: indicates that backup is being performed. • Slave Not Ready: indicates that the slave board is not ready. • Smooth Going: indicates that smooth processing is being performed.
Ability of auto creating BFD session on egress	Whether the capability to establish an entirely dynamic BFD session is enabled.
Period of LSP Ping	Interval for sending LSP ping packets of dynamic BFD sessions for detecting an LSP/PW.
System Session Delay Up Timer	Status of the delay Up timer: • OFF: indicates that the system works properly. • Xs: indicates that the system recovers after X seconds and a BFD session can be Up.

12.1.22 display bfd statistics session

Function

The **display bfd statistics session** command displays BFD session statistics.

Format

display bfd statistics session { **all** | **static** } [**for-lsp** | **for-pw** | **for-te** | **for-vsi-pw**](S5731-H, S5731-S, S5731S-S, S6730-S, S6730S-S, S5731S-H, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730S-H and S6730-H)

display bfd statistics session { **ldp-lsp peer-ip** *ip-address* **nexthop** *nexthop-address* [**interface** *interface-type interface-number*] | **static-lsp** *lsp-name* | **mpls-te interface** *interface-type interface-number* [**te-lsp**] | **pw interface** *interface-type interface-number* [**secondary**] } (S5731-H, S5731-S, S5731S-S, S6730-S, S6730S-S, S5731S-H, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730S-H and S6730-H)

display bfd statistics session { **vsi-pw vsi** *vsi-name* **peer** *peer-address* [**vc-id** *vc-id*] } (S5731-H, S5731-S, S5731S-S, S6730-S, S6730S-S, S5731S-H, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730S-H and S6730-H)

display bfd statistics session { **dynamic** | **discriminator** *discr-value* | **peer-ip default-ip** | **peer-ip** *ip-address* [**vpn-instance** *vpn-instance-name*] | **static-auto** }

display bfd statistics session peer-ipv6 *ipv6-address* [**vpn-instance** *vpn-instance-name*]

display bfd statistics session { **all** | **static** } [**for-ip** | **for-ipv6**]

Parameters

Parameter	Description	Value
all	Displays statistics about all BFD sessions.	-
static	Displays statistics about static BFD sessions.	-
dynamic	Displays statistics about dynamic BFD sessions and static BFD sessions with automatically negotiated discriminators.	-
discriminator *discr-value*	Displays statistics about the BFD sessions with a local discriminator.	The value is an integer that ranges from 1 to 16383.
peer-ip default-ip	Displays statistics about multicast BFD sessions.	-
peer-ip *ip-address*	Displays statistics about the BFD session bound to the specified peer IP address.	-
static-auto	Displays statistics about the static BFD session with the automatically negotiated discriminators.	-
vpn-instance *vpn-instance-name*	Displays statistics about the BFD sessions bound to a specified VPN instance.	The value must be an existing VPN instance name.
for-ip	Displays statistics about the BFD sessions for detecting IP links.	-
for-pw	Displays statistics about the BFD sessions for detecting PWs.	-
for-lsp	Displays statistics about the BFD sessions for detecting LSPs.	-

Parameter	Description	Value
for-te	Displays statistics about the BFD sessions for detecting a TE tunnel.	-
for-vsi-pw	Displays statistics about the BFD sessions for detecting VSI PWs.	-
vsi *vsi-name*	Displays statistics about the BFD session with the specified VSI PW instance name.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
peer *peer-address*	Displays statistics about the BFD session for detecting a VSI PW with the specified peer IPv4 address.	The value is expressed in dotted decimal notation.
vc-id *vc-id*	Displays statistics about the BFD session with the specified VC ID.	The value is an integer that ranges from 1 to 4294967295.
ldp-lsp	Displays statistics about the BFD sessions for detecting LDP LSPs.	-
nexthop *nexthop-address*	Displays statistics about the BFD session with the specified next hop address.	The value is expressed in dotted decimal notation.
interface-type interface-number	Displays statistics about the BFD session with the specified outbound interface. • *interface-type* specifies the interface type. • *interface-number* specifies the interface number.	-
static-lsp	Displays statistics about the BFD sessions for detecting static LSPs.	-

Parameter	Description	Value
lsp-name	Displays statistics about the BFD session for detecting the static LSP with the specified name.	The value is a string of 1 to 19 case-sensitive characters without spaces.
mpls-te	Displays statistics about the BFD sessions for detecting MPLS TE tunnels.	-
te-lsp	Displays statistics about the BFD session for detecting the primary LSP bound to a TE.	-
pw	Displays statistics about the BFD sessions for detecting PWs.	-
secondary	Displays statistics about the BFD session for detecting the secondary PW.	-
peer-ipv6 *ipv6-address*	Displays statistics about the BFD6 session bound to a specified IPv6 address.	-
for-ipv6	Displays statistics about static or all BFD6 sessions.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

The **display bfd statistics session** command displays BFD session statistics.

Precautions

- If static BFD with automatically negotiated discriminators and dynamic BFD share a session, you can specify **all**, **static-auto**, or **dynamic** for query.

- Before using the **display bfd statistics session** command to view BFD session statistics, run the **reset bfd statistics** command to clear existing statistics.

Example

Display statistics on all BFD sessions.

```
<HUAWEI> display bfd statistics session all
--------------------------------------------------------------------------------
Session MIndex : 16397        (Multi Hop)State : Up          Name : dyn_8196
--------------------------------------------------------------------------------
 Session Type                    : Dynamic
 Bind Type                       : IP
 Local/Remote Discriminator      : 8100/8101
 Received Packets                : 1710577
 Send Packets                    : 1710593
 Received Bad Packets            : 0
 Send Bad Packets                : 0
 Down Count                      : 0
 ShortBreak Count                : 0
 Send Lsp Ping Count             : 0
 Dynamic Session Delete Count    : 0
 Create Time                     : 2011-10-23 14:28:34
 Last Down Time                  : 0000-00-00 00:00:00
 Total Time From Last DOWN       : ---D:--H:--M:--S
 Last Up Time                    : 2011-11-14 11:06:52+08:00
 Last Up Lasting Time            : 002D:16H:49M:17S
 Total Time From Create          : 000D:04H:45M:35S
 Auth Time (ms)                  : 0
 Auth Seq Known (ms)             : 0
 Trigger If-down Delay Time (ms) : 0
--------------------------------------------------------------------------------

  Total Session Number : 1
```

Table 12-7 Description of the display bfd statistics session command output

Item	Description
Session MIndex	Index of BFD session entries.
State	Status of a BFD session.
Name	Name of a BFD session.
Session Type	Mode in which a BFD session is established: • Static: indicates that a BFD session is established statically. • Dynamic: indicates that a BFD session is established dynamically. • Static_Auto: indicates that a BFD session is established with automatically negotiated discriminators. • Entire_Dynamic: indicates the BFD sessions that are triggered entirely dynamically. After dynamic BFD session setup is enabled on the sink point of an LSP, a BFD session of this type is created.
Bind Type	BFD session binding type.

Item	Description
Local/Remote Discriminator	Local and remote discriminator of a BFD session. To set the local and remote discriminators of a BFD session, run the **discriminator** command.
Received Packets	Number of BFD packets received at the local end. This field can be deleted using the **reset bfd statistics** command.
Send Packets	Number of BFD packets sent by the local end. This field can be deleted using the **reset bfd statistics** command.
Received Bad Packets	Number of received error packets.
Send Bad Packets	Number of sent error packets.
Down Count	Number of times that a BFD session became Down.
ShortBreak Count	Number of times that a BFD session was transiently disconnected.
Send Lsp Ping Count	Number of LSP ping packets sent by the local end.
Dynamic Session Delete Count	Number of dynamic BFD sessions deleted.
Create Time	Time when a BFD session was created.
Last Down Time	Last time when a BFD session became Down.
Total Time From Last DOWN Down Status Lasting Time	Period from last time when a BFD session became Down to the current time. If a BFD session is Up, "Total Time From Last DOWN" is displayed. If a BFD session is Down, "Down Status Lasting Time" is displayed.
Last Up Time	Last time the BFD session becomes Up.
Last Up Lasting Time	Period from the last time when a BFD session is Up to the current time.
Total Time From Create	Period from the time when a BFD session was created to the current time.
Total Session Number	Number of BFD sessions.
Auth Time (ms)	Remaining time of the authentication timeout timer, in milliseconds
Auth Seq Known (ms)	Remaining time of the sequence number learning timer, in milliseconds

Item	Description
Trigger If-down Delay Time (ms)	Remaining time of the delay timer after which BFD instructs the interface to go down, in milliseconds
Total Session Number	Total number of BFD sessions

12.1.23 display bfd ttl

Function

The **display bfd ttl** command displays the globally configured TTL.

Format

display bfd ttl

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

The **display bfd ttl** command displays the globally configured TTL.

Example

Display information about all globally configured TTLs.

```
<HUAWEI> display bfd ttl
--------------------------------------------------------------------------------
Peer IP                                  Mask        Type          Value
--------------------------------------------------------------------------------
10.10.10.0                               24          single-hop    255
```

Table 12-8 Description of the display bfd ttl command output

Item	Specification
Peer IP	IP segment address.

Item	Specification
Mask	Mask length.
Type	Type of the BFD session. The value can be single-hop or multi-hop.
Value	Initial value of the global TTL value.

12.1.24 min-echo-rx-interval

Function

The **min-echo-rx-interval** command configures the minimum interval for receiving BFD packets of a BFD session supporting the BFD echo function.

The **undo min-echo-rx-interval** command restores the default minimum interval.

By default, the minimum interval is 1000 ms.

Format

min-echo-rx-interval *interval*

undo min-echo-rx-interval

Parameters

Parameter	Description	Value
interval	Specifies the minimum interval for receiving BFD packets of a BFD session supporting the BFD echo function.	The value is an integer that ranges from 100 to 1000, in milliseconds. • After the **set service-mode enhanced** command is configured on the S5731-H, S5731-S, S5731S-H, and S5731S-S, the value ranges from 3 to 1000. • After the **set service-mode enhanced-bfd** command is configured on the S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S, the value ranges from 3 to 1000.

Views

BFD session view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After creating a BFD session supporting the BFD echo function, you can set the minimum interval for receiving BFD packets of a BFD session supporting the BFD echo function.

Prerequisites

A BFD session supporting the echo function has been configured using the **bfd one-arm-echo** command.

Example

Set the minimum interval for receiving BFD packets of a BFD session supporting the BFD echo function to 100 ms.


```
<HUAWEI> system-view
[HUAWEI] bfd test
[HUAWEI-bfd-session-test] min-echo-rx-interval 100
```

12.1.25 min-rx-interval

Function

The **min-rx-interval** command sets the minimum interval for receiving BFD packets.

The **undo min-rx-interval** command restores the default minimum interval for receiving BFD packets.

By default, the minimum interval for receiving BFD packets is 1000 ms.

Format

min-rx-interval *interval*

undo min-rx-interval

Parameters

Parameter	Description	Value
interval	Specifies the minimum interval for receiving BFD packets.	The value is an integer that ranges from 100 to 1000, in milliseconds. • After the **set service-mode enhanced** command is configured on the S5731-H, S5731-S, S5731S-H, and S5731S-S, the value ranges from 3 to 1000. • After the **set service-mode enhanced-bfd** command is configured on the S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S, the value ranges from 3 to 1000.

Views

BFD session view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The local detection multiplier determines the detection time of a BFD session.

Detection time = Received Detect Multi of the remote system x Max (Local RMRI/ Received DMTI)

where

- Detect Multi: local detection multiplier, which is set by using the **detect-multiplier** command
- Required Min Rx Interval (RMRI): minimum interval for receiving BFD packets, which is set by using the **min-rx-interval** command
- Desired Min Tx Interval (DMTI): minimum interval for sending BFD packets, which is set by using the **min-tx-interval** command

Precaution

- You can increase or reduce the minimum interval for receiving BFD packets based on actual networking. The minimum interval for receiving BFD packets determines the detection time of a BFD session. On an unstable link, if the minimum interval for receiving BFD packets is small, the BFD session may flap. You can increase the minimum interval for receiving BFD packets. The default value is recommended. Do not randomly change the minimum interval for receiving BFD packets.
- If no BFD packet is received from the peer device within the detection time, the link is considered as faulty and the BFD session enters the Down state. To reduce the usage of system resources, when the BFD session is detected in Down state, the system adjusts the sending interval to a random value greater than 1000 ms. When the BFD session becomes Up, the configured interval is restored.
- On the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S, when the minimum interval for receiving BFD packets is smaller than 100 ms and the working mode of the switch is normal, the original BFD session needs to be deleted. Then set the working mode of the switch and reconfigure the BFD session.

Example

Set the minimum interval for receiving BFD packets to 500 ms.

```
<HUAWEI> system-view
[HUAWEI] bfd session
[HUAWEI-bfd-session-session] min-rx-interval 500
```


12.1.26 min-tx-interval

Function

The **min-tx-interval** command sets the minimum interval for sending BFD packets.

The **undo min-tx-interval** command restores the default minimum interval for sending BFD packets.

By default, the minimum interval for sending BFD packets is 1000 ms.

Format

min-tx-interval *interval*

undo min-tx-interval

Parameters

Parameter	Description	Value
interval	Specifies the minimum interval for sending BFD packets.	The value is an integer that ranges from 100 to 1000, in milliseconds. • After the **set service-mode enhanced** command is configured on the S5731-H, S5731-S, S5731S-H, and S5731S-S, the value ranges from 3 to 1000. • After the **set service-mode enhanced-bfd** command is configured on the S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S, the value ranges from 3 to 1000.

Views

BFD session view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The local detection multiplier determines the detection time of a BFD session.

Detection time = Received Detect Multi of the remote system x Max (Local RMRI/ Received DMTI)

where

- Detect Multi: local detection multiplier, which is set by using the **detect-multiplier** command
- Required Min Rx Interval (RMRI): minimum interval for receiving BFD packets, which is set by using the **min-rx-interval** command
- Desired Min Tx Interval (DMTI): minimum interval for sending BFD packets, which is set by using the **min-tx-interval** command

Precaution

- You can increase or reduce the minimum interval for sending BFD packets based on actual networking. The minimum interval for sending BFD packets determines the detection time of a BFD session. On an unstable link, if the minimum interval for sending BFD packets is small, the BFD session may flap. You can increase the minimum interval for sending BFD packets. The default value is recommended. Do not randomly change the minimum interval for sending BFD packets.
- If no BFD packet is received from the peer device within the detection time, the link is considered as faulty and the BFD session enters the Down state. To reduce the usage of system resources, when the BFD session is detected in Down state, the system adjusts the sending interval to a random value greater than 1000 ms. When the BFD session becomes Up, the configured interval is restored.
- On the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S, when the minimum interval for sending BFD packets is smaller than 100 ms and the working mode of the switch is normal, the original BFD session needs to be deleted. Then set the working mode of the switch and reconfigure the BFD session.

Example

Set the minimum interval for sending BFD packets to 500 ms.

```
<HUAWEI> system-view
[HUAWEI] bfd session
[HUAWEI-bfd-session-session] min-tx-interval 500
```

12.1.27 multi-hop

Function

The **multi-hop** command configures the destination port number for a multi-hop BFD session.

The **undo multi-hop** command restores the default destination port number for a multi-hop BFD session.

By default, destination port 3784 is used in multi-hop BFD control packets.

Format

multi-hop destination-port { **3784** | **4784** }

undo multi-hop destination-port

Parameters

Parameter	Description	Value
3784	Indicates that destination port 3784 is used in multi-hop BFD control packets.	-
4784	Indicates that destination port 4784 is used in multi-hop BFD control packets.	-

Views

BFD view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

As defined in the BFD draft, destination port 4784 is used by multi-hop BFD control packets. When the device running the latest version interworks with devices running earlier versions, destination port 3784 is used by multi-hop BFD control packets. When the device interworks with non-Huawei devices, destination port 4784 is used by multi-hop BFD control packets.

Precautions

- If destination port 4784 is used by multi-hop BFD control packets, the device fails to negotiate with the remote device on which destination port 3784 is used by multi-hop BFD control packets.
- If destination port 3784 is used by multi-hop BFD control packets, the device can successfully negotiate with the remote device on which destination port 4784 is used by multi-hop BFD control packets. On the device that is configured with destination port 3784, destination port 3784 is automatically updated to destination port 4784.
- If destination port 3784 is used by both multi-hop and single-hop BFD control packets, the single-hop and multi-hop BFD control packets are processed according to their TTLs.

- When a large number of multi-hop BFD sessions are set up, updating the destination ports may take a long time. Therefore, when a smaller interval for configuring multi-hop BFD sessions is used, the system displays a message indicating that the BFD session is being updated and you may try later.
- When the number of the destination port used in a multi-hop BFD control packet is updated, the BFD session in Up state may change to Down and then the BFD session is renegotiated.

NOTE

Determine to use port 3784 or 4784 before configuring a multi-hop BFD session between a Huawei device and a non-Huawei device. If the port number is not specified, you must change the port number after the BFD session becomes Up. Before changing the port number, shut down the BFD session. This is because changing the port number may cause all multi-hop BFD session to flap and affect services.

Example

Set the default destination port number to 4784 for multi-hop BFD control packets.

```
<HUAWEI> system-view
[HUAWEI] bfd
[HUAWEI-bfd] multi-hop destination-port 4784
```

12.1.28 oam-bind ingress bfd-session trigger if-down egress interface

Function

The **oam-bind ingress bfd-session trigger if-down egress interface** command enables a BFD session to report faults to an interface.

The **undo oam-bind ingress bfd-session trigger if-down egress interface** command disables a BFD session from reporting faults to an interface.

By default, a BFD session is not enabled to report faults to an 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

oam-bind ingress bfd-session *bfd-session-id* **trigger if-down egress interface** *interface-type interface-number*

undo oam-bind ingress bfd-session *bfd-session-id* **trigger if-down egress interface** *interface-type interface-number*

Parameters

Parameter	Description	Value
bfd-session *bfd-session-id*	Specifies the local discriminator.	The value is an integer that ranges from 1 to 8191.
trigger if-down	Indicates that an interface goes Down when the BFD session associated with the interface detects a fault.	-
interface-type interface-number	Specifies the type and number of the interface bound to a BFD session. • *interface-type* specifies the interface type. • *interface-number* specifies the interface number.	-

Views

OAM management view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To enable a BFD session to report faults to an interface, run the **oam-bind ingress bfd-session trigger if-down egress interface** command.

Precautions

Before configuring a BFD session to report faults to an interface, pay attention to the following points:

- A BFD session has been created and its status is Up.
- The BFD session is a static BFD session.
- The BFD session and the interface are associated with each other. That is, after an interface is associated with BFD session 1, the interface cannot be associated with other BFD sessions. Similarly, BFD session 1 cannot be associated with other interfaces.

The ingress BFD session reports faults to the egress interface.

Example

Configure BFD session 1 to report faults to GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] oam-mgr
[HUAWEI-oam-mgr] oam-bind ingress bfd-session 1 trigger if-down egress interface gigabitethernet 0/0/1
```

12.1.29 peer-ip ttl

Function

The **peer-ip ttl** command configures the TTL value in BFD packets.

The **undo peer-ip ttl** command restores the default TTL value in BFD packets.

By default, the TTL value in BFD packets varies with the BFD session type. By default, for a static BFD session, the TTL value of a single-hop BFD packet is 255 and the TTL value of a multi-hop BFD packet is 254. For a dynamic BFD session, the TTL value of a single-hop BFD packet is 255 and the TTL value of a multi-hop BFD packet is 253.

Format

peer-ip *peer-ip mask-length* **ttl** { **single-hop** | **multi-hop** } *ttl-value*

undo peer-ip *peer-ip mask-length* **ttl** { **single-hop** | **multi-hop** }

Parameters

Parameter	Description	Value
peer-ip	Specifies the peer IP address bound to the BFD session.	-
mask-length	Specifies the mask length of the IP address.	The value is an integer that ranges from 8 to 32.
single-hop	Indicates the single-hop BFD session.	-
multi-hop	Indicates the multi-hop BFD session.	-
ttl-value	Specifies the TTL value in BFD packets.	The value is an integer that ranges from 1 to 255.

Views

BFD view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can set the TTL value in BFD packets to enable the Huawei device to interwork with each other in different versions, with upgraded devices, and with non-Huawei devices.

Precautions

- The length of the IP segment address must match the mask. A long mask takes precedence over a short mask.
- The same IP segment addresses, masks, and TTL values of specified BFD session types cannot be configured simultaneously.
- When the IP network segment addresses and mask lengths are the same, the TTL value of a single-hop BFD session must be greater than the TTL value of a multi-hop BFD session.
- When a large number of BFD sessions are set up, updating the TTL value may take a long time. Therefore, when a smaller interval for configuring BFD sessions is used, the system displays a message indicating that the BFD session is being updated and you may try later.
- After the TTL value in multi-hop BFD packets is configured, you must configure the same peer IP address, mask length longer than the mask length for the TTL value in multi-hop BFD packets, and TTL value in single-hop BFD packets. This is because the TTL value in multi-hop BFD packets affects dynamic single-hop BFD sessions.

Example

Set the TTL value of single-hop BFD sessions to 254, the IP segment address to 10.10.10.0, and the mask length to 24.

```
<HUAWEI> system-view
[HUAWEI] bfd
[HUAWEI-bfd] peer-ip 10.10.10.0 24 ttl single-hop 254
```

12.1.30 process-interface-status

Function

The **process-interface-status** command associates the BFD session status with the bound interface status.

The **undo process-interface-status** command restores the default setting.

By default, the BFD session status is not associated with the interface status. That is, the change of the BFD session status does not affect the interface status.

Format

process-interface-status [**reboot-no-impact**] [**protocol-down**]

undo process-interface-status [**reboot-no-impact**] [**protocol-down**]

Parameters

Parameter	Description	Value
reboot-no-impact	Disables the association between a multicast BFD session and interface during device startup.	-
protocol-down	After **protocol-down** is configured, when a BFD session detects a fault and enters the Down state, the protocol status of the associated interface becomes Down. In this case, the interface discards Layer 2 and Layer 3 packets but permits BFD packets.	-

Views

BFD session view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If a transmission device exists on a direct link, BFD detects a link fault faster than a link protocol on an interface. The link protocol status of a trunk or VLANIF interface depends on the link protocol status of member interfaces.

To help BFD rapidly report the detection result to the application, a BFD status attribute is added to the interface management module of each interface. This attribute indicates the status of the BFD session that is bound to the interface. The system obtains the interface status based on the link status, protocol status, and BFD status on the interface, and then reports the interface status to the application.

Precautions

When configuring the **process-interface-status** command, pay attention to the following points:

- The **process-interface-status** command takes effect for only the single-hop BFD session that uses the default multicast address. The BFD session can be associated to an interface status.
- After the **trigger if-down delay** and **commit** commands are run in sequence, if BFD negotiation fails, the Down state is reported to the interface.
- If multiple BFD sessions are bound to an interface, you can use the **process-interface-status** command for only one BFD session. The change of only one BFD session changes the status of the bound interface.
- The BFD session does not report the BFD status to the bound interface immediately after the **commit** command is executed because the BFD session may not be set up or not Up. This prevents the BFD session from reporting an incorrect state to the interface. When the BFD status changes, the BFD session reports the BFD status to the interface to trigger the interface status change.
- If the **process-interface-status** command is saved in the configuration file, the BFD session for which the **process-interface-status** command is run notifies an interface that the BFD session becomes Down when the device is restarted. This is because the initial status of the interface is Down.
- Before the BFD session status is associated with the interface status, the BFD configurations on two ends must be correct and matched. If the BFD session status on the local interface is Down, check whether the BFD configuration on the peer end is correct or whether the BFD session is shut down.
- If the BFD session must be synchronized to an interface immediately, ensure that the BFD configurations on the two ends are the same and run the **shutdown (BFD session view)** and **undo shutdown (BFD session view)** commands on the BFD session. When the **undo shutdown (BFD session view)** command is executed for a BFD session, a BFD session detection timer is started. If the BFD session becomes Up through negotiation before the timer times out, the BFD session notifies an interface of the Up state. Otherwise, the BFD session considers the link faulty and notifies the interface of the Down state. The status of a BFD session and the status of an interface can be synchronized in real time.
- After a master/slave main control board switchover is performed, BFD notifies the associated interface to update the interface status during data smoothing based on the post-switchover BFD session status and diagnostic information. Specifically:
  a. If the BFD session is up, BFD notifies the interface to go up.
  b. If the BFD session is down, BFD differentiates between authentication and non-authentication scenarios.
     - BFD notifies the interface to go down in an authentication scenario.
     - In a non-authentication scenario, if the diagnostic word is "Receive AdminDown" and the receiving-admindown trigger if-down command is run before the switchover is performed, BFD notifies the interface to go down. If the diagnostic word is not "Receive AdminDown", BFD notifies the interface to go down.

Example

Associate the BFD session with an interface to which the BFD session is bound.


```
<HUAWEI> system-view
[HUAWEI] bfd test
[HUAWEI-bfd-session-test] process-interface-status
```

12.1.31 process-pst

Function

The **process-pst** command enables the system to modify the port status table (PST) when the BFD session status changes.

The **undo process-pst** command restores the default configuration.

By default, the device is disabled from modifying the PST.

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

process-pst

undo process-pst

Parameters

None

Views

BFD session view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After a BFD session that is enabled to modify the PST detects a BFD session Down event, the system modifies the corresponding entry in the PST.

Precautions

- You can only run the **process-pst** command in the BFD session view that is bound to LDP LSP, Static LSP, or MPLS TE.
- When configuring static BFD-based LDP FRR, you must configure the **process-pst** command.
- When configuring static BFD for CR-LSP and static BFD for TE, you must configure the **process-pst** command.
- For applications in which a fault detected by BFD is not sensed through the PST, you do not need to configure the **process-pst** command.

- In IP FRR scenarios, the PST function is automatically enabled for dynamic BFD sessions but cannot be configured for IP static BFD sessions bound to the same interface.

Example

Enable the system to modify the PST when the BFD session status changes.

```
<HUAWEI> system-view
[HUAWEI] bfd 4ldplsp bind ldp-lsp peer-ip 10.10.9.9 nexthop 10.10.10.10
[HUAWEI-bfd-lsp-session-4ldplsp] process-pst
```

12.1.32 receiving-admindown trigger if-down

Function

The **receiving-admindown trigger if-down** command enables a local device to instruct the interface protocol to go down immediately after receiving an admindown packet.

The **undo receiving-admindown trigger if-down** command disables a local device from instructing the interface protocol to go down immediately after receiving an admindown packet.

By default, the local device is disabled from instructing the interface protocol to go down immediately after receiving an admindown packet.

Format

receiving-admindown trigger if-down

undo receiving-admindown trigger if-down

Parameters

None

Views

BFD session view

Default Level

2: Configuration level

Usage Guidelines

After the **process-interface-status** command associates a BFD session with the status of an interface bound to the BFD session, a local device does not instruct the interface protocol to go down after the device receives an admindown packet. To enable an immediate notification, run the **receiving-admindown trigger if-down** command.

Prerequisites

The BFD session status has been associated with the status of the interface bound to the BFD session using the **process-interface-status** command.

Precautions

- This command is supported in both BFD authentication and non-authentication scenarios.
- This command takes effect only on multicast BFD.
- If the **trigger if-down delay** command is run, the local device can instruct the interface protocol to go down immediately after receiving an admindown packet.

Example

Enable the local device to instruct the interface protocol to go down immediately after receiving an admindown packet.

```
<HUAWEI> system-view
[HUAWEI] bfd test bind peer-ip default-ip interface gigabitethernet0/0/1
[HUAWEI-bfd-session-test] process-interface-status
[HUAWEI-bfd-session-test] receiving-admindown trigger if-down
```

12.1.33 reset bfd statistics

Function

The **reset bfd statistics** command clears statistics on received and sent packets of a BFD session.

Format

reset bfd statistics { **all** | **discriminator** *discr-value* }

Parameters

Parameter	Description	Value
all	Clears statistics on received and sent packets of all the BFD sessions.	-
discriminator *discr-value*	Clears statistics on received and sent packets of a BFD session with a specified discriminator.	The value is an integer that ranges from 1 to 16383.

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

The **reset bfd statistics** command clears statistics on received and sent packets of a BFD session.

Precautions

The deleted statistics on received and sent packets of a BFD session cannot be restored. Exercise caution when you use this command.

Example

Clear statistics on packets of all BFD sessions.

```
<HUAWEI> reset bfd statistics all
```

12.1.34 session-damping disable

Function

The **session-damping disable** command disables BFD session flapping suppression.

The **undo session-damping disable** command enables BFD session flapping suppression.

By default, BFD session flapping suppression is enabled.

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

session-damping disable

undo session-damping disable

Parameters

None

Views

BFD view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If a BFD session frequently flaps, frequent link switchovers may occur, which results in packet loss. If multiple BFD sessions frequently flap on a device within a certain time, many device resources are consumed. When BFD session flapping suppression is enabled, the system establishes a more intelligent punishment mechanism for each BFD session, properly reducing the establishment of the BFD session. The system also periodically checks the flapping of all BFD sessions on the device, and more strictly suppresses the sessions with the most frequent flapping if necessary.

To allow the system to immediately start the next negotiation after a BFD session goes Down (excluding AdminDown), run the **session-damping disable** command to disable BFD session flapping suppression.

Precautions

When BFD session flapping suppression is enabled, the device can adjust the flapping suppression time based on the penalty value in addition to the value of the intelligent timer (**dampening timer-interval**). The penalty value is adjusted as follows:

1. When a BFD session goes Down each time, the penalty value of the BFD session increases by 20. The initial value is 0 and the maximum penalty value is 240.
2. When a BFD session keeps Up for 1s each time, the penalty value decreases by 1. The minimum penalty value is 0.
3. If the penalty value of a BFD session exceeds 45, the flapping suppression time is twice (that is, 2^1) the value of *maximum-milliseconds*. If the penalty value of a BFD session exceeds 90, the flapping suppression time is four times (that is, 2^2) the value of *maximum-milliseconds*, and so on. The *maximum-milliseconds* is configured using the **dampening timer-interval** command.
4. If a BFD session is suppressed by the intelligent timer, the penalty value is adjusted based on rules 1 and 2 and the BFD session does not enter the penalty suppression state. That is, rule 3 does not take effect. Rule 3 takes effect only when suppression by the intelligent timer ends.

When multiple BFD sessions exist on the device, the penalty value is adjusted considering Down events of all BFD sessions in a period of time.

The **session-damping disable** command takes effect for all types of BFD sessions.

Example

Disable BFD session flapping suppression.

```
<HUAWEI> system-view
[HUAWEI] bfd
[HUAWEI-bfd] session-damping disable
```


12.1.35 shutdown (BFD session view)

Function

The **shutdown** command enables the BFD session to enter the AdminDown state.

The **undo shutdown** command enables a BFD session.

By default, a BFD session is enabled.

Format

shutdown

undo shutdown

Parameters

None

Views

BFD session view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **shutdown** command enables the BFD session to enter the AdminDown state.

Prerequisites

A BFD session has been created.

Precautions

- To modify the configuration of a BFD session, run the **shutdown** command to disable the BFD session. After the configuration is modified successfully, run the **undo shutdown** command to enable the BFD session again.
- To disable a BFD session without affecting the upper-layer application, run the **shutdown** command to enable the BFD session to enter the AdminDown state.
- If a BFD session is associated with an interface, the status of the BFD session is not reported to the interface when the BFD session is shut down.

Example

Stop the BFD session **atoc**.

```
<HUAWEI> system-view
[HUAWEI] bfd atoc
[HUAWEI-bfd-session-atoc] shutdown
```


12.1.36 snmp-agent bfd trap-interval

Function

The **snmp-agent bfd trap-interval** command sets the interval at which traps are sent.

The **undo snmp-agent bfd trap-interval** command restores the default interval at which traps are sent.

By default, the interval at which traps are sent is 120s.

Format

snmp-agent bfd trap-interval *interval*

undo snmp-agent bfd trap-interval

Parameters

Parameter	Description	Value
interval	Specifies the interval at which traps are sent.	The value is an integer that ranges from 1 to 600, in seconds.

Views

BFD view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If the BFD module is enabled with the SNMP alarm function, the NMS will receive BFD Up or Down messages. If the BFD session flaps, the NMS receives a large number of traps. In this case, BFD traps need to be suppressed. Run the **snmp-agent bfd trap-interval** command to set the interval at which traps are sent to prevent overflow of traps.

Prerequisites

Global BFD has been enabled using the **bfd** command.

Example

Set the interval at which traps are sent to 100s.


```
<HUAWEI> system-view
[HUAWEI] bfd
[HUAWEI-bfd] snmp-agent bfd trap-interval 100
```

12.1.37 tos-exp

Function

The **tos-exp** command sets the priority of BFD packets.

The **undo tos-exp** command restores the default priority of BFD packets.

By default, the priority of BFD packets is 7.

Format

tos-exp *tos-value*

undo tos-exp

Parameters

Parameter	Description	Value
tos-value	Specifies the priority of BFD packets. A larger value indicates a higher priority of BFD packets.	The value is an integer that ranges from 0 to 7. The default value is 7.

Views

BFD session view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can change the priority of BFD packets in the following scenarios:

- Detect whether packets with different priorities on a link can be forwarded.
- Ensure that BFD packets with a higher priority are forwarded first.

Precautions

When congestion occurs, the system first sends BFD packets with a higher priority.

Only the priority of BFD packets of the BFD session that is established using single-hop BFD, multi-hop BFD, and BFD Echo function can be changed. The priority of BFD packets of the BFD session that is established through automatically negotiated discriminators cannot be changed.

Example

Set the priority of BFD packets for the BFD session **atob** to 5.

```
<HUAWEI> system-view
[HUAWEI] bfd atob
[HUAWEI-bfd-session-atob] tos-exp 5
```

12.1.38 trigger if-down delay

Function

The **trigger if-down delay** command sets a delay time after which a local device instructs the interface protocol to go down after the device detects a BFD down event.

The **undo trigger if-down delay** command restores the default delay time.

The default delay time is 0s.

Format

trigger if-down delay *delay-time*

undo trigger if-down delay

Parameters

Parameter	Description	Value
delay-time	Sets the delay time, after which a local device instructs the interface protocol to go down after the device detects a BFD down event.	The value is an integer ranging from 1 to 10000, in seconds.

Views

BFD session view

Default Level

2: Configuration level

Usage Guidelines

If no link fault is detected and negotiation of a BFD session times out, the BFD session goes down. In this case, if the BFD session is associated with the status of the interface bound to the BFD session, the link protocol of the interface also goes down. To delay the associated notification, run the **trigger if-down delay** command. If the BFD session is still down after the delay time elapses, the link status of the associated interface goes down.

Prerequisites

The BFD session status has been associated with the status of the interface bound to the BFD session using the **process-interface-status** command.

Precautions

- This command takes effect on multicast BFD only in BFD non-authentication scenarios and is mutually exclusive with the **authentication-mode** command.
- If the **receiving-admindown trigger if-down** command is run, the local device can instruct the interface protocol to go down immediately after receiving an admindown packet.

Example

Set the delay time to 50s, after which a local device instructs the interface protocol to go down after the device detects a BFD down event.

```
<HUAWEI> system-view
[HUAWEI] bfd test bind peer-ip default-ip interface gigabitethernet0/0/1
[HUAWEI-bfd-session-test] process-interface-status
[HUAWEI-bfd-session-test] trigger if-down delay 50
```

12.1.39 unlimited-negotiate

Function

The **unlimited-negotiate** command enables unlimited negotiation for a multicast BFD session.

The **undo unlimited-negotiate** command disables unlimited negotiation for a multicast BFD session.

By default, unlimited negotiation is disabled for a multicast BFD session.

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

unlimited-negotiate

undo unlimited-negotiate

Parameters

None

Views

BFD session view

Default Level

2: Configuration level

Usage Guidelines

If a multicast BFD session is bound to a Layer 3 interface to which the line protocol current state of the interface is Down, the status of the session is set to Down. You can run the **unlimited-negotiate** command to restart session negotiation. If the link is normal, the session can go Up through negotiation.

Example

Enable unlimited negotiation for a multicast BFD session.

```
<HUAWEI> system-view
[HUAWEI] bfd
[HUAWEI-bfd] quit
[HUAWEI] bfd atob bind peer-ip default-ip interface gigabitethernet 0/0/1
[HUAWEI-bfd-session-atob] unlimited-negotiate
```

12.1.40 wtr

Function

The **wtr** command sets the WTR time of a BFD session.

The **undo wtr** command restores the default WTR time of a BFD session.

By default, the WTR time is 0, indicating that the status change of a BFD session is reported immediately.

Format

wtr *wtr-value*

undo wtr

Parameters

Parameter	Description	Value
wtr-value	Specifies the WTR time of a BFD session.	The value is an integer that ranges from 0 to 60, in minutes. The default value is 0.

Views

BFD session view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When a BFD session flaps, the WTR time prevents frequent active/standby switchovers of the application associated with the BFD session.

Precautions

- If the WTR time is set, the system reports the BFD session Up event to the upper-layer application only after the WTR timer expires. Other status change events are reported immediately, which are not affected by the WTR time.
- Both ends must use the same WTR time. Otherwise, when the session status changes at one end, applications at both ends detect different BFD session status.
- If the WTR time is set and a BFD session goes Down within the WTR time, the **Down Count** value is recorded, but the **Last Up Time** and **Last Up Lasting Time** values are not recorded.

Example

Set the WTR time of a BFD session to 10 minutes.

```
<HUAWEI> system-view
[HUAWEI] bfd atoc
[HUAWEI-bfd-session-atoc] wtr 10
```

12.2 VRRP Configuration Commands

12.2.1 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.

12.2.2 admin-vrrp vrid

Function

The **admin-vrrp vrid** command specifies an mVRRP group.

The **undo admin-vrrp vrid** command deletes the specified mVRRP group.

By default, no mVRRP group is configured.

Format

admin-vrrp vrid *virtual-router-id*

undo admin-vrrp vrid *virtual-router-id*

Parameters

Parameter	Description	Value
vrid *virtual-router-id*	Specifies the virtual router ID (VRID) of an mVRRP group.	The value is an integer that ranges from 1 to 255.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

An mVRRP group can be bound to VRRP groups. Once bound, the mVRRP group determines the master and backup status of the bound VRRP groups. mVRRP is used when multiple VRRP groups coexist, decreasing the number of VRRP Advertisement packets sent and minimize network bandwidth and system resource consumption.

NOTE

mVRRP provides the following functions:

- An mVRRP group used as the gateway can process both VRRP Advertisement packets and service packets.
- An mVRRP group that is not used as the gateway can only process VRRP Advertisement packets.

Precautions

An mVRRP group cannot be bound to another mVRRP group.

Example

Create VRRP group 1 on VLANIF 10 and configure it as an mVRRP group.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 10
[HUAWEI-Vlanif10] ip address 10.1.1.1 24
[HUAWEI-Vlanif10] vrrp vrid 1 virtual-ip 10.1.1.111
[HUAWEI-Vlanif10] admin-vrrp vrid 1
```

Create VRRP group 1 on GE0/0/1 and configure it as an mVRRP group.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] ip address 10.1.1.1 24
[HUAWEI-GigabitEthernet0/0/1] vrrp vrid 1 virtual-ip 10.1.1.111
[HUAWEI-GigabitEthernet0/0/1] admin-vrrp vrid 1
```


12.2.3 admin-vrrp6 vrid

Function

The **admin-vrrp6 vrid** command configures a VRRP6 group as an mVRRP6 group.

The **undo admin-vrrp6 vrid** command deletes the specified mVRRP6 group.

By default, no mVRRP6 group is configured.

Format

admin-vrrp6 vrid *virtual-router-id*

undo admin-vrrp6 vrid *virtual-router-id*

Parameters

Parameter	Description	Value
vrid *virtual-router-id*	Specifies the virtual router ID (VRID) of an mVRRP6 group.	The value is an integer that ranges from 1 to 255.

Views

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

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

An mVRRP6 group can be bound to common VRRP6 groups. Once bound, the mVRRP6 group determines the status of the bound VRRP6 groups based on the binding. mVRRP6 is used when multiple VRRP6 groups coexist, decreasing the number of VRRP Advertisement packets sent and minimizing network bandwidth consumption.

NOTE

mVRRP6 provides the following functions:

- An mVRRP6 group used as the gateway can process both VRRP6 Advertisement packets and service packets.
- An mVRRP6 group that is not used as the gateway can only process VRRP6 Advertisement packets.

Precautions

An mVRRP6 group cannot be bound to another mVRRP6 group.

Example

Create VRRP6 group 1 on VLANIF 10 and configure it as an mVRRP6 group.

```
<HUAWEI> system-view
[HUAWEI] ipv6
[HUAWEI] interface vlanif 10
[HUAWEI-Vlanif10] ipv6 enable
[HUAWEI-Vlanif10] ipv6 address FC00::1 64
[HUAWEI-Vlanif10] vrrp6 vrid 1 virtual-ip FE80::1 link-local
[HUAWEI-Vlanif10] admin-vrrp6 vrid 1
```

Create a VRRP6 group 1 on GE0/0/1 and configure it as an mVRRP6 group.

```
<HUAWEI> system-view
[HUAWEI] ipv6
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] ipv6 enable
[HUAWEI-GigabitEthernet0/0/1] ipv6 address FC00::1 64
[HUAWEI-GigabitEthernet0/0/1] vrrp6 vrid 1 virtual-ip FE80::1 link-local
[HUAWEI-GigabitEthernet0/0/1] admin-vrrp6 vrid 1
```

12.2.4 arp learning passive enable

Function

The **arp learning passive enable** command enables passive ARP that allows a backup device in a VRRP backup group to learn ARP entries when receiving an ARP request message sent to a virtual IP address.

The **undo arp learning passive enable** command disables passive ARP.

By default, passive ARP is disabled so that a backup device in a VRRP backup group does not learn ARP entries when receiving an ARP request message sent to a virtual IP address.

NOTE

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

Format

arp learning passive enable

undo arp learning passive enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the master and backup devices in a VRRP backup group receive an ARP request message sent to a virtual IP address, only the master device learns ARP entries and responds to the sender with the virtual MAC address. If a link or device fault causes the VRRP backup group to perform a master/backup switchover, a backup device must learn ARP entries on the user side before taking over traffic. As a result, service traffic is interrupted for a short time.

After you run the **arp learning passive enable** command to enable passive ARP, a backup device in a VRRP backup group learns ARP entries when receiving an ARP request message sent to a virtual IP address. If a VRRP backup group performs a master/backup switchover, the new master device can take over traffic without needing to relearn ARP entries, ensuring service continuity.

Precautions

Passive ARP cannot be configured together with strict ARP entry learning.

The passive ARP function is invalid for a VRRP group created on a VLANIF interface.

Example

Enable passive ARP.

```
<HUAWEI> system-view
[HUAWEI] arp learning passive enable
```

12.2.5 clear admin-vrrp

Function

The **clear admin-vrrp** command deletes the binding of an mVRRP group on the subcard that is not functioning.

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

clear admin-vrrp binding interface *interface-type interface-number* **vrid** *virtual-router-id*

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Specifies the type and number of an interface where an mVRRP group is configured.	-
vrid *virtual-router-id*	Specifies the VRID of an mVRRP group.	The value is an integer that ranges from 1 to 255.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

An mVRRP group is often bound to VRRP groups on an interface. If the subcard on which the mVRRP group is configured fails or is not properly installed, the binding is retained and will take effect when the subcard begins working properly. You can run the **display vrrp binding admin-vrrp member-vrrp** command to check whether configuration recovery is successful.

If the binding is not required, run the **clear admin-vrrp** command to delete the binding.

Prerequisites

The mVRRP group has been configured and VRRP groups have been bound to the mVRRP group.

Precautions

If the binding between the mVRRP group and VRRP groups is deleted, the status of the mVRRP group no longer determines the status of the bound VRRP groups.

The binding deleted using the **clear admin-vrrp** command cannot be restored.

Ensure that the interface name is correct when executing the **clear admin-vrrp** command. This is because the system does not verify the interface name.

Example

Delete the binding of the mVRRP group on the specified subcard that is not properly installed.

```
<HUAWEI> system-view
[HUAWEI] clear admin-vrrp binding interface gigabitethernet 0/0/1 vrid 1
```


12.2.6 clear admin-vrrp6

Function

The **clear admin-vrrp6** command deletes the binding of an mVRRP6 group on the member switch that is not functioning in a stack.

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

clear admin-vrrp6 binding interface *interface-type interface-number* **vrid** *virtual-router-id*

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Specifies the type and number of an interface where an mVRRP6 group is configured.	-
vrid *virtual-router-id*	Specifies the VRID of an mVRRP6 group.	The value is an integer that ranges from 1 to 255.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In a stack, an mVRRP6 group is often bound to VRRP6 groups on an interface. If the member switch on which the mVRRP6 group is configured fails or is not properly installed, the binding is retained and will take effect when the member switch begins working properly. You can run the **display vrrp6 binding admin-vrrp6 member-vrrp** command to check whether configuration recovery is successful.

If the binding is not required, run the **clear admin-vrrp6** command to delete the binding.

Prerequisites

The mVRRP6 group has been configured and VRRP6 groups have been bound to the mVRRP6 group.

Precautions

If the binding between the mVRRP6 group and VRRP6 groups is deleted, the status of the mVRRP6 group no longer determines the status of the bound VRRP6 groups.

The binding deleted using the **clear admin-vrrp6** command cannot be restored.

Ensure that the interface name is correct when executing the **clear admin-vrrp6** command. This is because the system does not verify the interface name.

Example

Delete the binding of the mVRRP6 group on the specified member switch that is not properly installed.

```
<HUAWEI> system-view
[HUAWEI] clear admin-vrrp6 binding interface gigabitethernet 0/0/1 vrid 1
```

12.2.7 display vrrp

Function

The **display vrrp** command displays the status and configuration parameters of VRRP groups.

Format

display vrrp [**interface** *interface-type interface-number*] [*virtual-router-id*] [**brief**]

display vrrp { **interface** *interface-type interface-number* [*virtual-router-id*] | *virtual-router-id* } **verbose**

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Displays the status of all VRRP groups on the specified interface. • *interface-type* specifies the interface type. • *interface-number* specifies the interface number.	-
virtual-router-id	Displays the status of a VRRP group with the specified VRID.	The VRID of the VRRP group must have been created.

Parameter	Description	Value
brief	Displays brief information about a specified VRRP group. If this parameter is not specified, detailed information about a VRRP group is displayed.	-
verbose	Displays detailed information about a VRRP group.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The **display vrrp** command displays information about VRRP groups.

Example

Display information about all VRRP groups on the switch.

```
<HUAWEI> display vrrp
Vlanif100 | Virtual Router 1
    State : Master
    Virtual IP : 10.1.1.100
    Master IP : 10.1.1.2
    PriorityRun : 120
    PriorityConfig : 120
    MasterPriority : 120
    Preempt : YES   Delay Time : 20 s
    TimerRun : 2 s
    TimerConfig : 2 s
    Auth type : MD5   Auth key : ******
    Virtual MAC : 0000-5e00-0101
    Check TTL : YES
    Config type : normal-vrrp
    Backup-forward : disabled
    Track IF : Eth-Trunk0   Priority reduced : 60
    IF state : UP
    Track BFD : 69                  Priority reduced : 10
    BFD-session state : UP
    Create time : 2011-10-07 15:43:42 UTC-08:00
    Last change time : 2011-10-07 15:44:03 UTC-08:00
```


Table 12-9 Description of the **display vrrp** command output

Item	Description
Vlanif100 | Virtual Router 1	Interface where the VRRP group is configured and VRID of the VRRP group.
State	VRRP status of the device: ● Master: The device functions as the master in the VRRP group. ● Backup: The device functions as the backup in the VRRP group. ● Initialize: All VRRP groups begin in Initialize state. When the interface where a VRRP group is configured becomes Down or is Administratively Down, the VRRP group status is switched to Initialize.
Virtual IP	Virtual IP address of a VRRP group. To configure a virtual IP address for a VRRP group, run the **vrrp vrid virtual-ip** command.
Master IP	Primary IP address of the interface configured with the VRRP group on the master.
PriorityRun	Priority of the switch when the VRRP group runs. If the switch is the IP address owner in a VRRP group, the running priority of the switch in the group is displayed as **255**.
PriorityConfig	Priority configured for the switch using the **vrrp vrid priority** command. If the switch is the IP address owner and this value is not configured, the default priority 100 but not 255 is displayed.
MasterPriority	Priority of the master in the VRRP group. If the switch is the IP address owner in a VRRP group, the priority of the switch in the group is displayed as **255**.
Preempt	Preemption mode: ● YES: preemption ● NO: no preemption To disable the preemption mode, run the **vrrp vrid preempt-mode disable** command.
Delay Time	Preemption delay, in seconds. To set the preemption delay, run the **vrrp vrid preempt-mode timer delay** command.
TimerRun	Interval at which the master in the VRRP group sends VRRP Advertisement packets, in seconds.

Item	Description
TimerConfig	Configured interval at which the master in the VRRP group sends VRRP Advertisement packets, in seconds. To set the interval at which the master in the VRRP group sends VRRP Advertisement packets, run the **vrrp vrid timer advertise** command.
Auth type	VRRP Advertisement packet authentication mode: ● NONE: non-authentication ● SIMPLE: simple authentication ● MD5: MD5 authentication To set an authentication mode, run the **vrrp vrid authentication-mode** command. VRRPv3 does not support authentication.
Auth key	Authentication key. If authentication is configured, ****** is displayed. If no authentication is configured, this field is not displayed.
Virtual MAC	Virtual MAC address of the VRRP group.
Check TTL	Whether the TTL value of a VRRP Advertisement packet is checked: ● YES: The TTL value of a VRRP Advertisement packet is checked. ● NO: The TTL value of a VRRP Advertisement packet is not checked. To configure the switch to check the TTL value in a VRRP Advertisement packet, run the **vrrp un-check ttl** command.
Config type	VRRP group type: ● normal-vrrp: common VRRP group ● admin-vrrp: mVRRP group ● member-vrrp: service VRRP group
Backup-forward	Whether the backup is enabled to forward traffic: ● enabled ● disabled To configure the backup to forward traffic, run the **vrrp vrid backup-forward** command.
Track IF	Name of a monitored interface when the interface monitoring function of VRRP backup group is enabled. To configure the parameter, run the **vrrp vrid track interface** command.

Item	Description
Priority reduced or Priority increased	Value to which the device decreases or increases a priority if the tracked interface, BFD session, or EFM session goes Down. When the interface, BFD session, or EFM session tracked by the VRRP backup group goes Down, and the priority of the VRRP backup group is configured to increase, **Priorityincreased** is displayed. To configure the parameter, run the **vrrp vrid track bfd-session** or **vrrp vrid track interface** command.
IF state	Status of the interface monitored by VRRP: ● UP ● DOWN ● REMOVE
Track BFD	Local discriminator or name of the BFD session associated with the VRRP group. This field is displayed when only the BFD session is associated with the VRRP group. To configure the BFD session associate with the VRRP group, run the **vrrp vrid track bfd-session** command.
BFD-session state	Status of the BFD session associated with the VRRP group: ● UP: A BFD session is in Up state. ● DOWN: A BFD session is in Down state. ● AdminDown: A BFD session is in AdminDown state.
Create time	Time when the VRRP group was created.
Last change time	Last time the VRRP group status changed.

Display brief information about all VRRP groups on the switch.

```
<HUAWEI> display vrrp brief
Total:1     Master:0     Backup:0     Non-active:1
VRID  State        Interface                Type     Virtual IP
------------------------------------------------------------------------------
1     Initialize   Vlanif23                 Normal   10.1.1.100
```

Table 12-10 Description of the **display vrrp brief** command output

Item	Description
VRID	VRID of the VRRP group.

Item	Description
State	VRRP status of the switch: • Master: The switch functions as the master in the VRRP group. • Backup: The switch functions as the backup in the VRRP group. • Initialize: All VRRP groups begin in Initialize state. When the interface where a VRRP group is configured becomes Down or is Administratively Down, the VRRP group status changes to Initialize.
Interface	Interface configured with the VRRP group.
Type	Type of a VRRP group: • normal-vrrp: common VRRP group • admin-vrrp: mVRRP group • member-vrrp: service VRRP group
Virtual IP	Virtual IP address of the VRRP group.
Total	Number of VRRP groups.
Master	Number of VRRP groups in Master state.
Backup	Number of VRRP groups in Backup state.
Non-active	Number of VRRP groups in Non-active state.

12.2.8 display vrrp admin-vrrp

Function

The **display vrrp admin-vrrp** command displays the status and configuration of all mVRRP groups.

Format

display vrrp admin-vrrp

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

You can view basic information about an mVRRP group, including the interface where the mVRRP group is configured, and the VRID and status of the mVRRP group.

Example

Display the status and configuration of all mVRRP groups on the device.

```
<HUAWEI> display vrrp admin-vrrp
Admin-vrrp number: 1
Interface: Vlanif10,  admin-vrrp vrid: 1, state: Master
```

Table 12-11 Description of the **display vrrp admin-vrrp** command output

Item	Description
Admin-vrrp number	Number of mVRRP groups.
Interface	Name and number of the interface where the mVRRP group is configured.
admin-vrrp vrid	VRID of the mVRRP group.
state	Status of the mVRRP group: • Master • Backup • Initialize

12.2.9 display vrrp binding admin-vrrp

Function

The **display vrrp binding admin-vrrp** command displays the binding of an mVRRP group, including member VRRP groups and interfaces where member VRRP groups are configured.

Format

display vrrp binding admin-vrrp [**interface** *interface-type interface-number*] [**vrid** *virtual-router-id*]

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Specifies the type and number of an interface where an mVRRP group is configured. • *interface-type* specifies the interface type. • *interface-number* specifies the interface number.	-
vrid *virtual-router-id*	Specifies the VRID of an mVRRP group.	The value is an integer that ranges from 1 to 255.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display vrrp binding admin-vrrp** command to view the binding of an mVRRP group.

Example

Display the binding of an mVRRP group.

```
<HUAWEI> display vrrp binding admin-vrrp
Interface: Vlanif10,  admin-vrrp vrid: 1, state:Master
  Member-vrrp number: 3
    Interface: Vlanif11, vrid: 1, state: Master
    Interface: Vlanif12, vrid: 2, state: Master
    Interface: Vlanif13, vrid: 3, state: Master
```

Table 12-12 Description of the **display vrrp binding admin-vrrp** command output

Item	Description
Interface	Interface configured with the mVRRP group.
admin-vrrp vrid	VRID of the mVRRP group.

Item	Description
state	Status of the mVRRP group: • Master • Backup • Initialize
Member-vrrp number	Number of member VRRP groups bound to the mVRRP group.
Interface	Interface where the member VRRP group bound to the mVRRP group is configured.
vrid	VRID of the member VRRP group bound to the mVRRP group.
state	Status of the member VRRP group bound to the mVRRP group: • Master • Backup • Initialize

12.2.10 display vrrp binding admin-vrrp member-vrrp

Function

The **display vrrp binding admin-vrrp member-vrrp** command displays information about the binding between an mVRRP group and member VRRP groups.

Format

display vrrp binding admin-vrrp [**interface** *interface-type1 interface-number1*] [**vrid** *virtual-router-id1*] **member-vrrp** [**interface** *interface-type2 interface-number2*] [**vrid** *virtual-router-id2*]

Parameters

Parameter	Description	Value
interface *interface-type1 interface-number1*	Specifies the type and number of an interface configured with an mVRRP group. • *interface-type1* specifies the interface type. • *interface-number1* specifies the interface number.	-

Parameter	Description	Value
vrid *virtual-router-id1*	Specifies the VRID of an mVRRP group.	The value is an integer that ranges from 1 to 255.
interface *interface-type2 interface-number2*	Specifies the type and number of an interface configured with a member VRRP group. • *interface-type2* specifies the interface type. • *interface-number2* specifies the interface number.	-
vrid *virtual-router-id2*	Specifies the VRID of a member VRRP group.	The value is an integer that ranges from 1 to 255.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

You can run the **display vrrp binding admin-vrrp member-vrrp** command to view information about the binding between an mVRRP group and member VRRP groups.

Example

Display information about the binding between an mVRRP group and member VRRP groups.

```
<HUAWEI> display vrrp binding admin-vrrp member-vrrp
Interface: Vlanif11,  admin-vrrp vrid: 1, state: Master
  Member-vrrp number: 3
    Interface: Vlanif10, vrid: 1, state: Master
    Interface: Vlanif10, vrid: 2, state: Master
    Interface: Vlanif12, vrid: 3, state: Master
```


Table 12-13 Description of the **display vrrp binding admin-vrrp member-vrrp** command output

Item	Description
Interface	Interface configured with the mVRRP group.
admin-vrrp vrid	VRID of the mVRRP group.
state	Status of the mVRRP group: • Master • Backup • Initialize
Member-vrrp number	Number of member VRRP groups bound to the mVRRP group.
Interface	Interface where the member VRRP group bound to the mVRRP group is configured.
vrid	VRID of the member VRRP group bound to the mVRRP group.
state	Status of the member VRRP group bound to the mVRRP group: • Master • Backup • Initialize

12.2.11 display vrrp protocol-information

Function

The **display vrrp protocol-information** command displays VRRP information.

Format

display vrrp protocol-information

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display vrrp protocol-information** command to view VRRP information.

Example

Display VRRP information.

```
<HUAWEI> display vrrp protocol-information
 VRRP protocol information is shown as below:
   VRRP protocol version : V2
   Send advertisement packet mode : send v2 only
```

Table 12-14 Description of the **display vrrp protocol-information** command output

Item	Description
VRRP protocol version	VRRP version number: • V2 • V3 To configure a VRRP version number, run the **vrrp version** command.
Send advertisement packet mode	Mode in which VRRP Advertisement packets are sent: • send v2 only: Only VRRPv2 Advertisement packets are sent. • send v3 only: Only VRRPv3 Advertisement packets are sent. It is displayed only when VRRPv3 is used. • send v2v3 both: VRRPv2 and VRRPv3 Advertisement packets are sent. It is displayed only when VRRPv3 is used. To configure the mode in which VRRP Advertisement packets are sent, run the **vrrp vrid version-3 send-packet-mode** command in the interface view or run the **vrrp version-3 send-packet-mode** command in the system view.

12.2.12 display vrrp state-change interface vrid

Function

The **display vrrp state-change interface vrid** command displays status changes of a specified VRRP group. This command can display a maximum of 10 of the latest status changes of a VRRP group.

Format

display vrrp state-change interface *interface-type interface-number* **vrid** *virtual-router-id*

Parameters

Parameter	Description	Value
interface-type interface-number	Specifies the type and number of an interface where status changes of a VRRP group are displayed. • *interface-type* specifies the interface type. • *interface-number* specifies the interface number.	-
vrid *virtual-router-id*	Specifies the VRID of a VRRP group.	The VRID of the VRRP group must have been created.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

When the VRRP status becomes abnormal, run the **display vrrp state-change interface vrid** command to view the last 10 status changes of the VRRP group, including the time at which the VRRP group status changed, the VRRP group status before and after the change, and the cause of the VRRP group status change. The command output helps you locate faults.

Example

Display status changes of VRRP group 1 on VLANIF 100.

```
<HUAWEI> display vrrp state-change interface vlanif 100 vrid 1
 Time                 SourceState  DestState    Reason
 ------------------------------------------------------------------
 2012-01-27 15:29:45      Backup       Master       Protocol timer expired
 2012-01-27 15:29:42      Initialize   Backup       Interface UP
```


Table 12-15 Description of the **display vrrp state-change interface vrid** command output

Item	Description
Time	Time when the VRRP group status changed.
SourceState	VRRP group status before the change: • Master • Backup • Initialize
DestState	VRRP group status after the change: • Master • Backup • Initialize
Reason	Cause of the VRRP status change: • Admin-vrrp drove • BFD configure deleted • CFM session down • CFM session up • EFM configure deleted • EFM session down • EFM session up • Interface up • Interface down • Ignore interface down • Link BFD session down • Link BFD session up • Link BFD session deleted • Link BFD down-number changed • Peer BFD session down • Priority calculation • Protocol timer expired • Track interface • Track BFD session

12.2.13 display vrrp statistics

Function

The **display vrrp statistics** command displays statistics about sent and received packets of VRRP groups.

Format

display vrrp [**interface** *interface-type interface-number*] [*virtual-router-id*] **statistics**

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Displays statistics about sent and received packets of all VRRP groups on a specified interface. • *interface-type* specifies the interface type. • *interface-number* specifies the interface number. If this parameter is not specified, statistics about sent and received packets of all VRRP groups or a specified VRRP group on the device are displayed.	-
virtual-router-id	Displays statistics about sent and received packets of a specified VRRP group. If this parameter is not specified, statistics about sent and received packets of all VRRP groups on the device or a specified interface are displayed.	The VRID of the VRRP group must have been created.
statistics	Displays statistics about sent and received packets of a VRRP group.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The **display vrrp statistics** command displays information about sent and received packets of VRRP groups.

Example

Display statistics about sent and received packets of VRRP group 1 on VLANIF100.

```
<HUAWEI> display vrrp interface vlanif 100 1 statistics
 Vlanif 100 | Virtual Router 1
                      Transited to master : 1
                      Transited to backup : 1
                   Transited to initialize : 0
                   Received advertisements : 0
                      Sent advertisements : 1000
              Advertisement interval errors : 0
             Failed to authentication check : 0
                   Received ip ttl errors : 0
         Received packets with priority zero : 0
            Sent packets with priority zero : 0
             Received invalid type packets : 0
     Received unmatched address list packets : 0
        Unknown authentication type packets : 0
           Mismatched authentication type : 0
                  Packet length errors : 0
    Discarded packets since track admin-vrrp : 0
               Received attacking packets : 0
               Received selfsend packets : 0
```

Display statistics about all VRRP Advertisement packets on the device.

```
<HUAWEI> display vrrp statistics
 Checksum errors : 0
  Version errors : 0
    Vrid errors : 0
   Other errors : 0

 Vlanif 100 | Virtual Router 1
                      Transited to master : 1
                      Transited to backup : 1
                   Transited to initialize : 0
                   Received advertisements : 0
                      Sent advertisements : 1000
              Advertisement interval errors : 0
             Failed to authentication check : 0
                   Received ip ttl errors : 0
         Received packets with priority zero : 0
            Sent packets with priority zero : 0
             Received invalid type packets : 0
     Received unmatched address list packets : 0
        Unknown authentication type packets : 0
           Mismatched authentication type : 0
                  Packet length errors : 0
    Discarded packets since track admin-vrrp : 0
               Received attacking packets : 0
               Received selfsend packets : 0
```


Table 12-16 Description of the display vrrp statistics command output

Item	Description
Checksum errors	CRC error count.
Version errors	Version error count.
Vrid errors	Number of VRID errors.
Other errors	Number of other errors.
Vlanif 100 | Virtual Router 1	Interface where the VRRP group is configured and VRID of the VRRP group.
Transited to master	Number of times the switch transitions to the Master state.
Transited to backup	Number of times the switch transitions to the Backup state.
Transited to initialize	Number of times the switch transitions to the Initialize state.
Received advertisements	Number of received VRRP Advertisement packets.
Sent advertisements	Number of sent VRRP Advertisement packets.
Advertisement interval errors	Number of times VRRP Advertisement packets are sent at an incorrect interval.
Failed to authentication check	Number of authentication failures.
Received ip ttl errors	Number of packets with TTL errors.
Received packets with priority zero	Number of received VRRP Advertisement packets with the priority of 0.
Sent packets with priority zero	Number of sent VRRP Advertisement packets with the priority of 0.
Received invalid type packets	Number of received VRRP Advertisement packets of invalid type.
Received unmatched address list packets	Number of packets with incorrect virtual IP address lists.
Unknown authentication type packets	Number of packets with an unknown authentication mode.
Mismatched authentication type	Number of packets with a non-matched authentication mode.
Packet length errors	Number of packets with incorrect length.
Discarded packets since track admin-vrrp	Number of received packets that are discarded after a VRRP group is bound to a management VRRP (mVRRP) group.

Item	Description
Received attacking packets	Number of received attack packets.
Received selfsend packets	Number of received packets sent by the switch.

12.2.14 display vrrp track bfd gratuitous-arp information

Function

The **display vrrp track bfd gratuitous-arp information** command displays information when a sub-interface is enabled to rapidly send gratuitous ARP packets during an active/standby switchover of a VRRP group triggered by its associated peer BFD session.

Format

display vrrp track bfd gratuitous-arp information

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

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The **display vrrp track bfd gratuitous-arp information** command displays information when a sub-interface is enabled to rapidly send gratuitous ARP packets during an active/standby switchover of a VRRP group triggered by its associated peer BFD session.

Example

Display information when a sub-interface is enabled to rapidly send gratuitous ARP packets during an active/standby switchover of a VRRP group triggered by its associated peer BFD session.

```
<HUAWEI> display vrrp track bfd gratuitous-arp information
------------------------------------------------------------------------------
Interface                   Vrid      BFD-session Name       Status
```



```
--------------------------------------------------------------------------------
GigabitEthernet0/0/19.1          32         atob                 Active
--------------------------------------------------------------------------------
Total:1          Active:1          InActive:0
```

Table 12-17 Description of the **display vrrp track bfd gratuitous-arp information** command output

Item	Description
Interface	Interface configured with the VRRP group.
Vrid	VRID of the VRRP group.
BFD-session Name	Name of a BFD session.
Status	Status of the BFD session.
Total	Total number of peer BFD sessions.
Active	Number of BFD sessions in active state.
InActive	Number of BFD sessions in inactive state.

12.2.15 display vrrp6

Function

The **display vrrp6** command displays the status and configuration parameters of VRRP6 groups.

Format

display vrrp6 [**interface** *interface-type interface-number*] [**vrid** *virtual-router-id*] [**brief**]

display vrrp6 { **interface** *interface-type interface-number* [**vrid** *virtual-router-id*] | **vrid** *virtual-router-id* } **verbose**

Parameters

Parameter	Description	Description
interface *interface-type interface-number*	Displays the status of all VRRP6 groups on the specified interface. • *interface-type* specifies the interface type. • *interface-number* specifies the interface number. If this parameter is not specified, information about all VRRP6 groups is displayed.	-
vrid *virtual-router-id*	Displays the status of a VRRP6 group with the specified VRID.	The VRID of the VRRP6 group must have been created.
brief	Displays brief information about a specified VRRP6 group.	-
verbose	Displays detailed information about a specified VRRP6 group.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can view the status and configuration of all VRRP6 groups based on networking, including interfaces where mVRRP6 groups are configured, and VRIDs and statuses of VRRP6 groups.

Example

Display information about all VRRP6 groups on the switch with VRID 4.

```
<HUAWEI> display vrrp6 vrid 4
Vlanif100 | Virtual Router 4
   State          : Master
   Virtual IP     : FE80::1:2
   Master IP : FE80::218:82FF:FED3:2AF1
```



```
PriorityRun      : 200
PriorityConfig   : 200
MasterPriority   : 200
Preempt          : YES                Delay Time : 0 s
TimerRun         : 100 cs
TimerConfig      : 100 cs
Virtual Mac      : 0000-5e00-0101
Check hop limit  : YES
Config type      : normal-vrrp
Backup-forward   : disabled
Create time      : 2012-05-22 17:40:56 UTC-08:00
Last change time : 2012-05-22 17:41:03 UTC-08:00
```

Table 12-18 Description of the display vrrp6 command output

Item	Description
Vlanif100 | Virtual Router 4	Interface where the VRRP6 group is configured and VRID of the VRRP6 group.
State	VRRP6 status of the device: ● Master: The device functions as the master in the VRRP6 group. ● Backup: The device functions as the backup in the VRRP6 group. ● Initialize: All VRRP6 groups begin in Initialize state. When the status of an interface is Down or administratively Down, the VRRP6 group status changes to Initialize.
Virtual IP	Virtual IP address of the VRRP6 group. To configure a virtual IP address for a VRRP6 group, run the **vrrp6 vrid virtual-ip** command.
Master IP	Primary IP address of the interface configured with the VRRP6 group on the master.
PriorityRun	Priority of the switch when the VRRP6 group runs. If the switch is the IP address owner in a VRRP6 group, the running priority of the switch in the group is displayed as **255**.
PriorityConfig	Priority configured for the switch using the **vrrp6 vrid priority** command. If the switch is the IP address owner, the default priority 100 but not 255 is displayed.
MasterPriority	Priority of the master in the VRRP6 group. If the switch is the IP address owner in a VRRP6 group, the priority of the switch in the group is displayed as **255**.
Preempt	Preemption mode: ● YES: preemption ● NO: no preemption To disable the preemption mode, run the **vrrp6 vrid preempt-mode disable** command.

Item	Description
Delay Time	Preemption delay, in seconds. To set the preemption delay, run the **vrrp6 vrid preempt-mode timer delay** command.
TimerRun	Interval at which the master in the VRRP6 group sends VRRP Advertisement packets, in centiseconds.
TimerConfig	Configured interval at which the master in the VRRP6 group sends VRRP6 Advertisement packets, in centiseconds. To set the interval at which the master in the VRRP6 group sends VRRP6 Advertisement packets, run the **vrrp6 vrid timer advertise** command.
Virtual Mac	Virtual MAC address of the VRRP6 group.
Check hop limit	Whether the TTL value of a VRRP6 Advertisement packet is checked: ● YES: The TTL value of a VRRP6 Advertisement packet is checked. ● NO: The TTL value of a VRRP6 Advertisement packet is not checked. To configure the device to check the TTL value in a VRRP6 Advertisement packet, run the **vrrp6 un-check hop-limit** command.
Config type	Type of a VRRP6 group: ● normal-vrrp: common VRRP6 group ● admin-vrrp: mVRRP6 group ● member-vrrp: service VRRP6 group
Backup-forward	Whether the backup is enabled to forward traffic: ● enabled ● disabled
Create time	Time when the VRRP6 group was created.
Last change time	Last time the VRRP6 group status changed.

Display brief information about all VRRP6 groups on the device.

```
<HUAWEI> display vrrp6 brief
Total:2     Master:2     Backup:0     Non-active:0
VRID  State        Interface              Type     Virtual IP
------------------------------------------------------------------------------
1     Master       Vlanif66               Normal   FE80::1
2     Master       Vlanif67               Normal   FE80::1:3
```


Table 12-19 Description of the display vrrp6 brief command output

Item	Description
VRID	VRID of the VRRP6 group.
State	VRRP6 status of the switch: • Master: The device functions as the master in the VRRP6 group. • Backup: The device functions as the backup in the VRRP6 group. • Initialize: All VRRP6 groups begin in Initialize state. When the interface where a VRRP group is configured becomes Down or is Administratively Down, the VRRP6 group status is switched to Initialize.
Interface	Interface configured with the VRRP6 group.
Type	Type of a VRRP6 group: • normal-vrrp: common VRRP6 group • admin-vrrp: mVRRP6 group • member-vrrp: service VRRP6 group
Virtual IP	Virtual IP address of the VRRP6 group.
Total	Number of VRRP6 groups.
Master	Number of VRRP6 groups in Master state.
Backup	Number of VRRP6 groups in Backup state.
Non-active	Number of VRRP6 groups in Non-active state.

12.2.16 display vrrp6 admin-vrrp6

Function

The **display vrrp6 admin-vrrp6** command displays the status and configuration of all mVRRP6 groups.

Format

display vrrp6 admin-vrrp6

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can view the status and configuration of all mVRRP6 groups, including interfaces where mVRRP6 groups are configured, and VRIDs and statuses of the mVRRP6 groups.

Example

Display the status and configuration of all mVRRP6 groups on the device.

```
<HUAWEI> display vrrp6 admin-vrrp6
  Admin-vrrp6 number: 1
Interface: Vlanif100,  admin-vrrp6 vrid: 1, state: Master
```

Table 12-20 Description of the **display vrrp6 admin-vrrp6** command output

Item	Description
Admin-vrrp6 number	Number of mVRRP6 groups.
Interface	Interface configured with the mVRRP6 group.
admin-vrrp6 vrid	VRID of the mVRRP6 group.
state	Status of the mVRRP6 group: • Master • Backup • Initialize

12.2.17 display vrrp6 binding admin-vrrp6

Function

The **display vrrp6 binding admin-vrrp6** command displays the binding of an mVRRP6 group and its member VRRP6 groups.

Format

display vrrp6 binding admin-vrrp6 [**interface** *interface-type interface-number*] [**vrid** *virtual-router-id*]

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Specifies the type and number of an interface where an mVRRP6 group is configured.	-
vrid *virtual-router-id*	Specifies the VRID of an mVRRP6 group.	The value is an integer that ranges from 1 to 255.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

If the **interface** *interface-type interface-number* parameter is not specified, the **display vrrp6 binding admin-vrrp6** command displays the binding of mVRRP6 groups on all interfaces of the device.

Example

Display the binding of mVRRP6 groups on all interfaces.

```
<HUAWEI> display vrrp6 binding admin-vrrp6
Interface: Vlanif100,  admin-vrrp6 vrid: 1, state:Master
  Member-vrrp6 number: 1
    Interface: Vlanif200, vrid: 2, state: Master
```

Table 12-21 Description of the **display vrrp6 binding admin-vrrp6** command output

Item	Description
Interface	Interface configured with the mVRRP6 group.
admin-vrrp6 vrid	VRID of the mVRRP6 group.
state	Status of the mVRRP6 group: • Master • Backup • Initialize
Member-vrrp6 number	Number of member VRRP6 groups bound to the mVRRP6 group.
Interface	Interface configured with a member VRRP6 group that is bound to the mVRRP6 group.

Item	Description
vrid	VRID of a member VRRP6 group bound to the mVRRP6 group.
state	Status of a member VRRP6 group bound to the mVRRP6 group: • Master • Backup • Initialize

12.2.18 display vrrp6 binding admin-vrrp6 member-vrrp

Function

The **display vrrp6 binding admin-vrrp6 member-vrrp** command displays information about the binding between an mVRRP6 group and member VRRP6 groups.

Format

display vrrp6 binding admin-vrrp6 [**interface** *interface-type1 interface-number1*] [**vrid** *virtual-router-id1*] **member-vrrp** [**interface** *interface-type2 interface-number2*] [**vrid** *virtual-router-id2*]

Parameters

Parameter	Description	Value
interface *interface-type1 interface-number1*	Specifies the type and number of an interface configured with an mVRRP6 group.	-
vrid *virtual-router-id1*	Specifies the VRID of an mVRRP6 group.	The value is an integer that ranges from 1 to 255.
interface *interface-type2 interface-number2*	Specifies the type and number of an interface configured with a member VRRP6 group.	-
vrid *virtual-router-id2*	Specifies the VRID of a member VRRP6 group.	The value is an integer that ranges from 1 to 255.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The **display vrrp6 binding admin-vrrp6 member-vrrp** command displays the bindings between mVRRP6 backup groups and member VRRP6 backup groups on the network as required.

- If *interface-type1 interface-number1* is merely specified in the command, the command output displays all the bindings between mVRRP6 backup groups and member VRRP6 backup groups on the specified interface.
- If the command is specified with only *virtual-router-id1*, the command output displays the bindings between the specified mVRRP6 backup group and member VRRP6 backup groups.
- If the command is specified with only *interface-type1 interface-number1* and *virtual-router-id1*, the command output displays the bindings between the specified mVRRP6 backup group on the specified interface and member VRRP6 backup groups.
- If the command is only specified with *interface-type2 interface-number2*, the command output displays the bindings between member VRRP6 backup groups on the specified interface and mVRRP6 backup groups.
- If the command is specified with only *virtual-router-id2*, the command output displays the bindings between the specified member VRRP6 backup group and mVRRP6 backup groups.
- If the command is specified with only *interface-type2 interface-number2* and *virtual-router-id2*, the command output displays the bindings between the specified member VRRP6 backup group on the specified interface and mVRRP6 backup groups, and information about the mVRRP6 backup groups.

Example

Display information about the binding between an mVRRP6 group and member VRRP6 groups.

```
<HUAWEI> display vrrp6 binding admin-vrrp6 member-vrrp
Interface: Vlanif100, admin-vrrp6 vrid: 1, state: Master
  Member-vrrp number: 2
    Interface: Vlanif101, vrid: 2, state: Master
    Interface: Vlanif102, vrid: 3, state: Master
```

Display information about the binding between mVRRP6 group 1 and member VRRP6 groups on VLANIF 10.

```
<HUAWEI> display vrrp6 binding admin-vrrp6 interface vlanif 10 vrid 1 member-vrrp
Interface: Vlanif10,  admin-vrrp6 vrid: 1, state:Master
  Member-vrrp number: 3
        Interface: Vlanif100, vrrp6 vrid: 1, state: Master
        Interface: Vlanif101, vrrp6 vrid: 2, state: Master
        Interface: Vlanif102, vrrp6 vrid: 3, state: Master
```


Table 12-22 Description of the **display vrrp6 binding admin-vrrp6 member-vrrp** command output

Item	Description
Interface	Interface configured with the mVRRP6 group.
admin-vrrp6 vrid	VRID of the mVRRP6 group.
state	Status of the mVRRP6 group: • Master • Backup • Initialize
Member-vrrp number	Number of member VRRP6 groups bound to the mVRRP6 group.
Interface	Interface configured with the member VRRP6 group.
vrrp6 vrid	VRID of the member VRRP6 group.
state	Status of the member VRRP6 group.

12.2.19 display vrrp6 state-change interface vrid

Function

The **display vrrp6 state-change interface vrid** command displays status changes of a specified VRRP6 group. This command can display a maximum of the latest 10 status changes of a VRRP6 group.

Format

display vrrp6 state-change interface *interface-type interface-number* **vrid** *virtual-router-id*

Parameters

Parameter	Description	Value
interface-type interface-number	Specifies the type and number of an interface where status changes of a VRRP6 group are displayed.	-
virtual-router-id	Specifies the VRID of a VRRP6 group.	The VRID of the VRRP6 group must have been created.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

When the VRRP6 status becomes abnormal, run the **display vrrp6 state-change interface vrid** command to view the latest 10 status changes of the VRRP6 group. The command output includes the time when the VRRP6 group status changed, VRRP6 group status before and after each change, and causes of the status changes. The command output helps you locate faults.

Example

Display status changes of VRRP6 group 1 on VLANIF 100.

```
<HUAWEI> display vrrp6 state-change interface vlanif 100 vrid 1
Time                        SourceState  DestState   Reason
--------------------------------------------------------------------------------
2012-05-19 20:36:44             Initialize   Backup      interface up
2012-05-19 20:37:07             Backup       Master      protocol timer expired
```

Table 12-23 Description of the **display vrrp6 state-change interface vrid** command output

Item	Description
Time	Time when the VRRP6 status changed.
SourceState	Status before the change: • Master • Backup • Initialize
DestState	Status after the change: • Master • Backup • Initialize

Item	Description
Reason	Reason of the change in the status of the VRRP6 backup group: • Admin-vrrp drove • BFD configure deleted • Interface up • Interface down • Link BFD session down • Link BFD session up • Link BFD session deleted • Peer BFD session down • Priority calculation • Protocol timer expired • Track interface • Track BFD session

12.2.20 display vrrp6 statistics

Function

The **display vrrp6 statistics** command displays statistics about sent and received packets of VRRP6 groups.

Format

display vrrp6 [**interface** *interface-type interface-number*] [**vrid** *virtual-router-id*] **statistics**

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Displays statistics about sent and received packets of all VRRP6 groups on a specified interface. • *interface-type* specifies the interface type. • *interface-number* specifies the interface number. If this parameter is not specified, statistics about sent and received packets of all VRRP6 groups or a specified VRRP6 group on the switch are displayed.	-
vrid *virtual-router-id*	Displays statistics about sent and received packets of a specified VRRP6 group. If this parameter is not specified, statistics about sent and received packets of all VRRP6 groups on the switch or a specified interface are displayed.	The VRID of the VRRP6 group must have been created.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The **display vrrp6 statistics** command displays information about sent and received packets of VRRP6 groups.

Example

Display statistics about all VRRP6 Advertisement packets on the switch.


```
<HUAWEI> display vrrp6 statistics
  Checksum errors : 0
  Version errors : 0
    Vrid errors : 0
    Other errors : 0

  Vlanif100 | Virtual Router 1
                        Transited to master : 1
                        Transited to backup : 1
                    Transited to initialize : 0
                    Received advertisements : 0
                        Sent advertisements : 1000
                Advertisement interval errors : 0
                Failed to authentication check : 0
                    Received ip ttl errors : 0
          Received packets with priority zero : 0
              Sent packets with priority zero : 0
              Received invalid type packets : 0
        Received unmatched address list packets : 0
          Unknown authentication type packets : 0
            Mismatched authentication type : 0
                Packet length errors : 0
      Discarded packets since track admin-vrrp : 0
                Received attacking packets : 0
                Received selfsend packets : 0
```

Table 12-24 Description of the **display vrrp6 statistics** command output

Item	Description
Checksum errors	CRC error count.
Version errors	Version error count.
Vrid errors	Number of VRID errors.
Other errors	Number of other errors.
Vlanif100 | Virtual Router 1	Interface where the VRRP6 group is configured and VRID of the VRRP6 group.
Transited to master	Number of times the switch transitions to the Master state.
Transited to backup	Number of times the switch transitions to the Backup state.
Transited to initialize	Number of times the switch transitions to the Initialize state.
Received advertisements	Number of received VRRP Advertisement packets.
Sent advertisements	Number of sent VRRP Advertisement packets.
Advertisement interval errors	Number of times VRRP Advertisement packets are sent at an incorrect interval.
Failed to authentication check	Number of authentication failures.
Received ip ttl errors	Number of packets with TTL errors.

Item	Description
Received packets with priority zero	Number of received VRRP Advertisement packets with the priority of 0.
Sent packets with priority zero	Number of sent VRRP Advertisement packets with the priority of 0.
Received invalid type packets	Number of received VRRP6 Advertisement packets of invalid type.
Received unmatched address list packets	Number of packets with incorrect virtual IPv6 address lists.
Unknown authentication type packets	Number of invalid authentication packets.
Mismatched authentication type	Number of packets with mismatching authentication types.
Packet length errors	Number of packets with incorrect length.
Discarded packets since track admin-vrrp	Number of received packets that are discarded after a VRRP6 group is bound to a management VRRP6 (mVRRP6) group.
Received attacking packets	Number of received attack packets.
Received selfsend packets	Number of received packets sent by the switch.

12.2.21 reset vrrp statistics

Function

The **reset vrrp statistics** command clears statistics about received and sent packets of VRRP groups.

Format

reset vrrp [**interface** *interface-type interface-number*] [**vrid** *virtual-router-id*] **statistics**

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Clears statistics about sent and received packets of all VRRP groups on a specified interface. • *interface-type* specifies the interface type. • *interface-number* specifies the interface number. If this parameter is not specified, statistics about sent and received packets of all VRRP groups or a specified VRRP group on the device are cleared.	-
vrid *virtual-router-id*	Clears statistics about sent and received packets of a specified VRRP group. If this parameter is not specified, statistics about sent and received packets of all VRRP groups or a specified VRRP group on the device are cleared.	The value is an integer that ranges from 1 to 255.

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

Before recollecting statistics about VRRP Advertisement packets, run the **reset vrrp statistics** command to clear existing statistics.

Precautions

The cleared statistics cannot be restored. Exercise caution when executing the **reset vrrp statistics** command.

Example

Clear statistics about sent and received packets of VRRP group 1 on VLANIF100.

```
<HUAWEI> reset vrrp interface vlanif 100 vrid 1 statistics
```

Clear statistics about all the packets of VRRP group 1.

```
<HUAWEI> reset vrrp vrid 1 statistics
```

Clear statistics about packets of all VRRP groups on the switch.

```
<HUAWEI> reset vrrp statistics
```

12.2.22 reset vrrp6 statistics

Function

The **reset vrrp6 statistics** command clears statistics about received and sent packets of VRRP6 groups.

Format

reset vrrp6 [**interface** *interface-type interface-number*] [**vrid** *virtual-router-id*] **statistics**

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Clears statistics about sent and received packets of all VRRP6 groups on a specified interface. • *interface-type* specifies the interface type. • *interface-number* specifies the interface number. If this parameter is not specified, statistics about sent and received packets of all VRRP6 groups or a specified VRRP6 group on the device are cleared.	-

Parameter	Description	Value
vrid *virtual-router-id*	Clears statistics about sent and received packets of a specified VRRP6 group. If this parameter is not specified, statistics about sent and received packets of all VRRP6 groups or a specified VRRP6 group on the device are cleared.	The value is an integer that ranges from 1 to 255.

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

Before recollecting statistics about VRRP6 Advertisement packets, run the **reset vrrp6 statistics** command to clear existing statistics.

Precautions

The cleared statistics cannot be restored. Exercise caution when executing the **reset vrrp6 statistics** command.

Example

Clear statistics about sent and received packets of VRRP6 group 1 on VLANIF100.

```
<HUAWEI> reset vrrp6 interface vlanif 100 vrid 1 statistics
```

Clear statistics about all the packets of VRRP6 group 1.

```
<HUAWEI> reset vrrp6 vrid 1 statistics
```

Clear statistics about packets of all VRRP6 groups on the switch.

```
<HUAWEI> reset vrrp6 statistics
```

12.2.23 set vrrp max-group-number

Function

The **set vrrp max-group-number** command sets the maximum number of allowed VRRP groups (sum of VRRP4 and VRRP6 groups).

The **undo set vrrp max-group-number** command restores the default maximum number of allowed VRRP groups.

By default, a maximum of 64 VRRP groups can be configured.

Format

set vrrp max-group-number *max-group-number*

undo set vrrp max-group-number

Parameters

Parameter	Description	Value
max-group-number	Specifies the maximum number of allowed VRRP groups.	Enumerated type. The values are as follows: • S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S: 64, 128, 192, 256, 320, 384, 448, 512, or 1000 • S6735-S, S6720S-EI and S6720-EI: 64, 128, 192, 256, 320, or 384 • S5720I-SI, S5735-S, S5735S-S, S5735-S-I, S5735S-H, S5736-S, and S6720S-S: 64, 128, 192, or 256 • S1720GW-E, S1720GWR-E, SS5720-LI, S2730S-S, S5735-L-I, S5735-L1,S300, S500, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, and S5720S-LI: 64 or 128

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When more than 64 VRRP groups need to be configured, run this command to set the maximum number of allowed VRRP groups.

Precautions

- You are not advised to configure more than 64 VRRP groups.
- When more than 64 VRRP groups are configured, to reduce the frequency of sending VRRP Advertisement packets and the impact of VRRP Advertisement packets on network bandwidth and CPU performance, perform one of the following operations as prompted in addition to executing the **set vrrp max-group-number** command (You are advised to configure an mVRRP group):
  - Run the **vrrp vrid timer advertise** command to increase the interval for sending VRRP Advertisement packets (recommended interval: > 3s), and run the **cpu-defend dynamic-car enable** command to enable a switch to dynamically adjust the default CIR value for protocol packets.
  - Run the **vrrp vrid timer advertise** command to increase the interval for sending VRRP Advertisement packets (recommended interval: > 3s), and run the

    car { **packet-type** *packet-type* | **user-defined-flow** *flow-id* } **cir** *cir-value* [**cbs** *cbs-value*]

    command to increase the CPCAR for VRRP Advertisement packets. Adjust the CPCAR value as prompted. Improper CPCAR settings will affect services on your network.
  - Run the **admin-vrrp vrid** command to configure an mVRRP group.
  - For the S5735S-H, S5736-S, and S6720S-S:
    - When the number of VRRP groups on the device exceeds a specified value, ACL resources are occupied. In this situation, MAC mirroring may become invalid.
    - When a VRRP group is configured for a super-VLAN, the device delivers virtual MAC address entries corresponding to sub-VLANs of the super-VLAN. This occupies many resources. When configuring a VRRP group for a super-VLAN, pay attention to the following points:
      - The VRRP group can be configured for a maximum of 16 super-VLANs on the device.
      - The device allows a maximum of 312 virtual MAC address entries for VRRP. For example, there are 10 sub-VLANs in super-VLAN 100. When a VRRP group is configured on VLANIF 100, 11 virtual MAC address entries are occupied (1 super-VLAN + 10 sub-VLANs).

Example

Set the maximum number of allowed VRRP groups to 192.

```
<HUAWEI> system-view
[HUAWEI] set vrrp max-group-number 192
```

12.2.24 vrrp advertise send-mode

Function

The **vrrp advertise send-mode** command configures a mode in which the master sends VRRP Advertisement packets in a super-VLAN.

The **undo vrrp advertise send-mode** command restores the default mode in which the master sends VRRP Advertisement packets in a super-VLAN.

By default, the master sends VRRP Advertisement packets to a sub-VLAN that is Up and has the smallest VLAN ID in a super-VLAN.

NOTE

Only the S5720I-SI, S5735-S, S500, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6720S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Format

vrrp advertise send-mode { *sub-vlan-id* | **all** }

undo vrrp advertise send-mode

Parameters

Parameter	Description	Value
sub-vlan-id	Specifies the ID of a sub-VLAN where the master sends VRRP Advertisement packets.	The value is an integer that ranges from 1 to 4094.
all	Indicates that the master sends VRRP Advertisement packets to all sub-VLANs in a super-VLAN.	-

Views

VLANIF interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When a VRRP group is configured in a super-VLAN, run the **vrrp advertise send-mode** command to configure the master to send VRRP Advertisement packets to a specified sub-VLAN or all sub-VLANs in the super-VLAN. If there are a large number of sub-VLANs in a super-VLAN, to save bandwidth, configure the master to send VRRP Advertisement packets to a specified sub-VLAN.

Prerequisites

A VRRP group has been configured on the VLANIF interface corresponding to the super-VLAN.

Precautions

Using **all** is not recommended. If **all** is configured, a super VLAN broadcasts a VRRP Advertisement packet to all its Sub-VLANs. This causes CPU usage to increase.

If both VRRP and static ARP are configured on a device, note the following issues:

- If VRRP is enabled on a VLANIF interface, a virtual IP address cannot be an IP address that maps to a MAC address in a static ARP entry. If a virtual IP address maps to a MAC address in a static ARP entry, a forwarding failure occurs. For example, if a MAC address in a static ARP entry on a VLANIF interface maps to an IP address of 10.1.1.1, the IP address of 10.1.1.1 cannot be a virtual IP address of a VRRP IPv4 backup group configured on the VLANIF interface.
- After a VLANIF interface is configured with a VRRP IPv4 backup group and a static ARP entry, the virtual IP address of the VRRP IPv4 backup group cannot be an IP address that maps to the MAC address in the static ARP entry. Otherwise, a forwarding failure occurs. For example, if a VRRP IPv4 backup group on a VLANIF interface is assigned an IP address of 10.1.1.1, the IP address of 10.1.1.1 cannot map to a MAC address in a static ARP entry configured on the VLANIF interface.

Example

Configure the master to broadcast VRRP Advertisement packets to sub-VLAN 50 in super-VLAN 100.

```
<HUAWEI> system-view
[HUAWEI] vlan 100
[HUAWEI-vlan100] aggregate-vlan
[HUAWEI-vlan100] quit
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] vrrp vrid 1 virtual-ip 10.10.10.10
[HUAWEI-Vlanif100] vrrp advertise send-mode 50
```

12.2.25 vrrp arp send-mode simple

Function

The **vrrp arp send-mode simple** command configures the master on a QinQ termination sub-interface to send gratuitous ARP packets to the VLAN specified by the outer VLAN tag and the first VLAN in the VLAN range specified by the inner VLAN tag.

The **undo vrrp arp send-mode simple** command restores the default setting.

By default, the master on a QinQ termination sub-interface sends gratuitous ARP packets to the VLAN specified by the outer VLAN tag and all VLANs in the VLAN range specified by the inner VLAN tag.

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

vrrp arp send-mode simple

undo vrrp arp send-mode simple

Parameters

None

Views

VE sub-interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When VRRP is deployed on a QinQ termination sub-interface, the system sends double-tagged ARP packets. If the inner VLAN tag specifies a VLAN range, the system sends ARP packets to all the VLANs in the VLAN range specified by the inner VLAN tag. This ensures that MAC address entries on the downstream device are updated immediately, but causes a heavy burden. The **vrrp arp send-mode simple** command configures the master on a QinQ termination sub-interface to send gratuitous ARP packets to the VLAN specified by the outer VLAN tag and the first VLAN in the VLAN range specified by the inner VLAN tag. This prevents excess gratuitous ARP packets from affecting the system.

NOTE

The **vrrp arp send-mode simple** command takes effect in VLANs specified only by the inner VLAN tag but not VLANs specified by the outer VLAN tag. For example, the VLAN ID in the outer tag ranges from 1 to 10 and the VLAN ID in the inner tag ranges from 1 to 10. After the **vrrp arp send-mode simple** command is run, gratuitous ARP packets are transmitted in only VLAN 1 (specified by the inner VLAn tag). A total of 10 gratuitous ARP packets (10 outer VLAN IDs x 1 inner VLAN ID) are sent.

Precautions

The **vrrp arp send-mode simple** command must be executed on a QinQ termination sub-interface.

Example

Configure VE sub-interface Virtual-Ethernet0/0/2.1 to send gratuitous ARP packets in VLAN 3.

```
<HUAWEI> system-view
[HUAWEI] interface virtual-ethernet0/0/2
[HUAWEI-Virtual-Ethernet0/0/2] ve-group 1 l3-access
[HUAWEI-Virtual-Ethernet0/0/2] quit
[HUAWEI] interface virtual-ethernet0/0/2.1
[HUAWEI-Virtual-Ethernet0/0/2.1] qinq termination pe-vid 5 ce-vid 3 to 20
[HUAWEI-Virtual-Ethernet0/0/2.1] vrrp vrid 1 virtual-ip 10.1.1.1
[HUAWEI-Virtual-Ethernet0/0/2.1] vrrp arp send-mode simple
```


12.2.26 vrrp gratuitous-arp timeout

Function

The **vrrp gratuitous-arp timeout** command configures an interval at which the master in a VRRP group sends gratuitous ARP packets or the master in a VRRP6 group sends ND packets.

The **undo vrrp gratuitous-arp timeout** command restores the default interval at which the master in a VRRP group sends gratuitous ARP packets or the master in a VRRP6 group sends ND packets.

The default interval is 120 seconds.

Format

vrrp gratuitous-arp timeout *time*

undo vrrp gratuitous-arp timeout

Parameters

Parameter	Description	Value
timeout *time*	Specifies an interval at which the master in a VRRP group sends gratuitous ARP packets or the master in a VRRP6 group sends ND packets.	The value is an integer that ranges from 30 to 1200, in seconds.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The master in a VRRP group sends gratuitous ARP packets or the master in a VRRP6 group sends ND packets to its connected downstream switch to update the MAC entries on the downstream switch.

Precautions

- If a short interval is used, bandwidth resources will be consumed. If a long interval is used, MAC address entries on the downstream switch cannot be updated immediately.
- The interval at which the master sends gratuitous ARP or ND packets must be shorter than the aging time of MAC address entries on user devices.

Set the interval based on actual networking:

- To restore the default interval at which the master sends gratuitous ARP or ND packets, run the **undo vrrp gratuitous-arp timeout** command in the system view.
- If gratuitous ARP or ND packet do not need to be sent, run the **vrrp gratuitous-arp timeout disable** command in the system view.

Example

Set the interval at which the master in a VRRP group sends gratuitous ARP packets or the master in a VRRP6 group sends ND packets to 100 seconds.

```
<HUAWEI> system-view
[HUAWEI] vrrp gratuitous-arp timeout 100
```

12.2.27 vrrp gratuitous-arp timeout disable

Function

The **vrrp gratuitous-arp timeout disable** command disables the master device in a Virtual Router Redundancy Protocol for IPv4 (VRRP4) backup group from sending gratuitous ARP packets or the master device in a Virtual Router Redundancy Protocol for IPv6 (VRRP6) backup group from sending ND packets.

By default, the master device in a VRRP4 (or VRRP6) backup group sends gratuitous ARP (or ND) packets every 120 seconds.

Format

vrrp gratuitous-arp timeout disable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The master device in a VRRP4 (or VRRP6) backup group sends gratuitous ARP (or ND) packets to its connected downstream switch to update the MAC entries on the downstream switch. Because ARP and NDP do not provide any security mechanisms, attackers can send spoofed ARP or ND packets to attack network devices. If high network security is required, run the **vrrp gratuitous-arp timeout disable** command to disable the master device in a VRRP4 backup group from sending gratuitous ARP packets or the master device in a VRRP6 backup group from sending ND packets.

Precautions

After the **vrrp gratuitous-arp timeout disable** command is run, the master device in a VRRP4 (or VRRP6) backup group no longer periodically sends gratuitous ARP (or ND) packets to its connected downstream switch. If a master/backup switchover occurs, the MAC entries on the downstream switch cannot be promptly updated. As a result, traffic is interrupted.

Example

Disable the master device in a VRRP4 backup group from sending gratuitous ARP packets or the master device in a VRRP6 backup group from sending ND packets.

```
<HUAWEI> system-view
[HUAWEI] vrrp gratuitous-arp timeout disable
```

12.2.28 vrrp recover-delay

Function

The **vrrp recover-delay** command sets the delay before a VRRP or VRRP6 group recovers.

The **undo vrrp recover-delay** command restores the default delay before a VRRP or VRRP6 group recovers.

By default, the delay before a VRRP or VRRP6 group recovers is 0.

Format

vrrp recover-delay *delay-value*

undo vrrp recover-delay

Parameters

Parameter	Description	Value
delay-value	Specifies the delay before a VRRP or VRRP6 group recovers.	The value is an integer that ranges from 0 to 60, in seconds.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When an interface or a BFD session associated with a VRRP or VRRP6 group alternates between Up and Down states, the VRRP or VRRP6 group status may flap, causing user traffic loss. To solve this problem, run the **vrrp recover-delay** command to set the delay before a VRRP or VRRP6 group recovers. A VRRP or VRRP6 group then only responds to the interface or BFD session Up event after the delay expires.

Precautions

- When the device in a VRRP or VRRP6 group restarts, the VRRP or VRRP6 group status may flap. It is recommended that the delay be set based on actual networking.
- After an interface or a BFD session associated with a VRRP or VRRP6 group alternates between Up and Down states, the system only records logs and alarms at one time during each delay. This prevents the same alarms from being displayed repeatedly.

Example

Set the delay before a VRRP group recovers to 5 seconds.

```
<HUAWEI> system-view
[HUAWEI] vrrp recover-delay 5
```

12.2.29 vrrp smooth-switching timer

Function

The **vrrp smooth-switching timer** command enables VRRP smooth switching and sets the interval contained in VRRP Advertisement packets during VRRP smooth switching.

The **undo vrrp smooth-switching timer** command disables VRRP smooth switching.

By default, VRRP smooth switching is enabled and the interval contained in VRRP Advertisement packets is 100s.

Format

vrrp smooth-switching timer *timer-value*

undo vrrp smooth-switching timer

Parameters

Parameter	Description	Value
timer-value	Specifies the interval contained in VRRP Advertisement packets during VRRP smooth switching. After VRRP smooth switching is enabled on the master, the master sends VRRP Advertisement packets at this interval during an active/standby switchover.	The value is an integer that ranges from 1 to 255, in seconds.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If an active/standby switchover occurs on the master in the stack system in a VRRP group, the master and backup may fail to communicate with each other during the switchover. During the switchover, the backup with the highest priority becomes the new master if backups receive no VRRP Advertisement packet after the VRRP Advertisement packet sending interval expires. In this situation, two masters coexist. After the active/standby switchover is complete on the original master, the original master switches to the master because its priority is higher than the new master. During this process, services are switched twice, causing unstable service transmission.

After VRRP smooth switching is enabled on the device in the stack system, backups learn the smooth switching time. This implementation extends the timeout interval for receiving VRRP Advertisement packets during VRRP smooth switching, ensuring stability of the VRRP group status.

Prerequisites

The device has been enabled to learn the interval for sending VRRP Advertisement packets using the **vrrp timer-advertise learning enable** command.

Precautions

After receiving VRRP Advertisement packets from the master, the non-master device checks the interval in VRRP Advertisement packets. If the interval in VRRP Advertisement packets is different from the interval of the non-master device, the non-master device learns the interval and adjusts its own interval to be the same as the learned interval.

- *timer-value* must be greater than the interval at which VRRP Advertisement packets are sent. Otherwise, the master may be busy during the switchover and unable to send VRRP Advertisement packets in a timely manner. As a result, a backup switches to the master.
- After the **undo vrrp timer-advertise learning enable** command is executed, VRRP smooth switching is also disabled.

Example

Enable VRRP smooth switching and set the interval contained in VRRP Advertisement packets during VRRP smooth switching to 20 seconds.

```
<HUAWEI> system-view
[HUAWEI] vrrp smooth-switching timer 20
```


12.2.30 vrrp timer-advertise learning enable

Function

The **vrrp timer-advertise learning enable** command enables the device to learn the interval for sending VRRP Advertisement packets.

The **vrrp timer-advertise learning disable** command disables the device from learning the interval for sending VRRP Advertisement packets.

The **undo vrrp timer-advertise learning enable** command disables the device from learning the interval for sending VRRP Advertisement packets.

By default, the device is enabled to learn the interval for sending VRRP Advertisement packets.

Format

vrrp timer-advertise learning enable

vrrp timer-advertise learning disable

undo vrrp timer-advertise learning enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When a link fault triggers an active/standby switchover, VRRP smooth switching is enabled to prevent traffic loss. Before enabling VRRP smooth switching, run the **vrrp timer advertise learning enable** command to enable the device to learn the interval for sending VRRP Advertisement packets. Then non-master devices in the VRRP group will learn the interval at which VRRP Advertisement packets are sent and update their interval to be the same as the learned interval.

Prerequisites

A VRRP group has been created.

Precautions

If VRRP smooth switching has been enabled, running the **undo vrrp timer-advertise learning enable** command disables VRRP smooth switching.

The **undo vrrp timer-advertise learning enable** command is valid only for VRRPv2. If VRRPv3 is enabled using the **vrrp version** command, this function does not take effect.

Example

Enable the device to learn the interval for sending VRRP Advertisement packets.

```
<HUAWEI> system-view
[HUAWEI] vrrp timer-advertise learning enable
```

12.2.31 vrrp track bfd gratuitous-arp send enable

Function

The **vrrp track bfd gratuitous-arp send enable** command enables a sub-interface to rapidly send gratuitous ARP packets during an active/standby switchover of a VRRP group triggered by its associated peer BFD session.

The **undo vrrp track bfd gratuitous-arp send enable** command cancels the configuration.

By default, a sub-interface is not enabled to rapidly send gratuitous ARP packets during an active/standby switchover of a VRRP group triggered by its associated peer BFD session.

Format

vrrp track bfd gratuitous-arp send enable

undo vrrp track bfd gratuitous-arp send enable

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

None

Views

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

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On a network where association between a VRRP group and a peer BFD session is configured, when the peer BFD session on the backup detects a fault on the active link, the peer BFD session notifies the VRRP group of performing an active/standby switchover. The new master sends gratuitous ARP packets to its downstream Layer 2 device through the software protocol stack so that traffic is switched to the new master.

To speed up traffic switching, run this command to enable a sub-interface to rapidly send gratuitous ARP packets during an active/standby switchover of a VRRP group triggered by its associated peer BFD session. When the peer BFD session on the backup detects the fault on the active link, the hardware rapidly sends gratuitous ARP packets to its downstream Layer 2 device so that traffic is switched to the new master.

Prerequisites

The **vrrp vrid** *virtual-router-id* **track bfd-session** { *bfd-session-id* | **session-name** *bfd-configure-name* } **peer** command has been configured on the sub-interface.

Precautions

Each peer BFD session triggers only one VRRP group to send gratuitous ARP packets.

Example

Enable gigabitethernet0/0/1.1 to rapidly send gratuitous ARP packets during an active/standby switchover of a VRRP group triggered by its associated peer BFD session.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1.1
[HUAWEI-GigabitEthernet0/0/1.1] vrrp vrid 1 track bfd-session 1 peer
[HUAWEI-GigabitEthernet0/0/1.1] vrrp track bfd gratuitous-arp send enable
```

12.2.32 vrrp un-check ttl

Function

The **vrrp un-check ttl** command disables the device from checking the TTL value in VRRP Advertisement packets.

The **undo vrrp un-check ttl** command enables the device to check the TTL value in VRRP Advertisement packets.

By default, the system checks the TTL value in VRRP Advertisement packets.

Format

vrrp un-check ttl

undo vrrp un-check ttl

Parameters

None

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

The device checks the TTL value in received VRRP Advertisement packets. If the TTL value in a VRRP Advertisement packet is not 255, the device discards the VRRP Advertisement packet and generates a log about the VRRP Advertisement packet error.

On certain networks, especially on a network where the device interworks with non-Huawei devices, valid packets may be discarded if TTL check is enabled. You can configure the device not to check the TTL value in VRRP Advertisement packets.

Example

Disable the switch from checking the TTL value in VRRP Advertisement packets on VLANIF 100.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] vrrp un-check ttl
```

Disable the switch from checking the TTL value in VRRP Advertisement packets on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] vrrp un-check ttl
```

12.2.33 vrrp version

Function

The **vrrp version** command configures a VRRP version number.

The **undo vrrp version** command restores the default VRRP version number.

By default, VRRPv2 is used.

Format

vrrp version { **v2** | **v3** }

undo vrrp version

Parameters

Parameter	Description	Value
v2	Indicates that VRRPv2 is used.	-
v3	Indicates that VRRPv3 is used.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If VRRPv2 and VRRPv3 are used on a network and devices running VRRPv2 need to communicate with devices running VRRPv3, run the **vrrp version** command to specify a VRRP version number.

Precautions

A VRRPv2 group can only send and receive VRRPv2 Advertisement packets. It discards the received VRRPv3 Advertisement packets.

A VRRPv3 group can send and receive both VRRPv2 and VRRPv3 Advertisement packets. You can configure a mode in which VRRPv3 Advertisement packets are sent so that devices running VRRPv2 and VRRPv3 can communicate.

Follow-up Procedure

After VRRPv3 is used, run the **vrrp version-3 send-packet-mode** command in the system view or the **vrrp vrid version-3 send-packet-mode** command in the interface view to configure a mode in which VRRP Advertisement packets are sent.

Example

Set the VRRP version of the device to VRRPv3.

```
<HUAWEI> system-view
[HUAWEI] vrrp version v3
```

12.2.34 vrrp version-3 send-packet-mode

Function

The **vrrp version-3 send-packet-mode** command configures a mode in which VRRPv3 Advertisement packets are sent.

The **undo vrrp version-3 send-packet-mode** command restores the default mode in which VRRPv3 Advertisement packets are sent.

By default, the mode is **v3-only**.

Format

vrrp version-3 send-packet-mode { **v2-only** | **v3-only** | **v2v3-both** }

undo vrrp version-3 send-packet-mode

Parameters

Parameter	Description	Value
v2-only	Indicates that the device sends only VRRPv2 Advertisement packets.	-
v3-only	Indicates that the device sends only VRRPv3 Advertisement packets.	-
v2v3-both	Indicates that the device sends both VRRPv2 and VRRPv3 Advertisement packets.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If devices in a VRRP group use different VRRP version numbers, the VRRP group may fail to negotiate the status. This is because a VRRPv2-enabled device can only receive VRRPv2 Advertisement packets and discards the received VRRPv3 Advertisement packets. You can configure a mode in which VRRP Advertisement packets are sent so that devices running VRRPv2 and VRRPv3 in the VRRP group can negotiate the status.

Precautions

- Only VRRPv3 supports this command.
- If both the **vrrp version-3 send-packet-mode** and **vrrp vrid version-3 send-packet-mode** commands are run, the **vrrp vrid version-3 send-packet-mode** command takes precedence over the **vrrp version-3 send-packet-mode** command.

NOTE

If a large number of VRRP groups are configured, **v2v3-both** is not recommended.

Example

Set the mode in which VRRPv3 Advertisement packets are sent to **v2-only**.


```
<HUAWEI> system-view
[HUAWEI] vrrp version-3 send-packet-mode v2-only
```

12.2.35 vrrp virtual-ip ping enable

Function

The **vrrp virtual-ip ping enable** command enables the master to respond to ping packets sent to a virtual IP address.

The **vrrp virtual-ip ping disable** command disables the master from responding to ping packets sent to a virtual IP address.

The **undo vrrp virtual-ip ping enable** command disables the master from responding to ping packets sent to a virtual IP address.

By default, the master is enabled to respond to ping packets sent to a virtual IP address.

Format

vrrp virtual-ip ping enable

vrrp virtual-ip ping disable

undo vrrp virtual-ip ping enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The switch allows user devices to ping a virtual IP address to serve the following purposes:

- Monitors the operating status of the master in a VRRP group.
- Monitors communication between a user device and a network connected by a default gateway using the virtual IP address.

Precautions

If the ping to a virtual IP address is enabled, a device on an external network can ping a virtual IP address. This imposes the switch to ICMP-based attacks.

After the **undo vrrp virtual-ip ping enable** command is run to disable the master from responding to ping packets sent to a virtual IP address, the host route for the

virtual IP address is deleted. As a result, services transmitted using the host route are interrupted. For example, after the **undo vrrp virtual-ip ping enable** command is run, the GRE tunnel with the source IP address of a virtual IP address goes Down.

Example

Disable the master from responding to ping packets.

```
<HUAWEI> system-view
[HUAWEI] undo vrrp virtual-ip ping enable
```

12.2.36 vrrp virtual-ip route-advertise disable

Function

The **vrrp virtual-ip route-advertise disable** command disables a dynamic routing protocol from advertising routes generated by the virtual IP address of a VRRP group.

The **undo vrrp virtual-ip route-advertise disable** command enables a dynamic routing protocol to advertise routes generated by the virtual IP address of a VRRP group.

By default, a dynamic routing protocol is enabled to advertise routes generated by the virtual IP address of a VRRP group.

Format

vrrp virtual-ip route-advertise disable [**isis** | **ospf** | **rip**] *

undo vrrp virtual-ip route-advertise disable

NOTE

Only the S5720I-SI, S5735-S, S500, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6720S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S support **isis**.

Parameters

Parameter	Description	Value
isis	Disables IS-IS from advertising the routes generated by the virtual IP address of a VRRP group.	-
ospf	Disables OSPF from advertising the routes generated by the virtual IP address of a VRRP group.	-
rip	Disables RIP from advertising the routes generated by the virtual IP address of a VRRP group.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Direct routes generated by the virtual IP address of a VRRP group can be imported to a dynamic routing protocol. By default, these routes are advertised by a dynamic routing protocol to neighbors. In practice, a large number of routes may be generated by the virtual IP address of a VRRP group. If a dynamic routing protocol imports theses routes and advertises them to neighbors, there is a heavy burden on network devices and network performance deteriorates. You can run the **vrrp virtual-ip route-advertise disable** command to disable a dynamic routing protocol from advertising routes generated by the virtual IP address of a VRRP group.

Prerequisites

- A virtual IP address has been configured for a VRRP group.
- A dynamic routing protocol has imported routes generated by the virtual IP address of the VRRP group.

Precautions

After the **vrrp virtual-ip route-advertise disable** command is executed, routes generated by virtual IP addresses of all VRRP groups cannot be advertised by a dynamic routing protocol.

The **vrrp virtual-ip route-advertise disable** command is only valid for OSPF and IS-IS.

If routes generated by the virtual IP address of a VRRP group must be advertised by a dynamic routing protocol, do not run the **vrrp virtual-ip route-advertise disable** command.

Example

Disable a dynamic routing protocol from advertising routes generated by the virtual IP address of a VRRP group.

```
<HUAWEI> system-view
[HUAWEI] vrrp virtual-ip route-advertise disable
```

12.2.37 vrrp vrid authentication-mode

Function

The **vrrp vrid authentication-mode** command configures an authentication mode and an authentication key for a VRRP group.

The **undo vrrp vrid authentication-mode** command cancels the authentication mode and authentication key for a VRRP group.

By default, a VRRP group uses non-authentication.

Format

vrrp vrid *virtual-router-id* **authentication-mode** { **simple** { *key* | **plain** *key* | **cipher** *cipher-key* } | **md5** *md5-key* }

undo vrrp vrid *virtual-router-id* **authentication-mode**

Parameters

Parameter	Description	Value
vrid *virtual-router-id*	Specifies the VRID of a VRRP group.	The value is an integer that ranges from 1 to 255.
simple	Indicates simple authentication.	-
key	Specifies the authentication key in simple authentication mode.	The value is a string of 1 to 8 case-sensitive characters without spaces. When double quotation marks are used around the string, spaces are allowed in the string.
plain *key*	Specifies the authentication key in plain text authentication mode. **NOTE** If **plain** is selected, the password is saved in the configuration file in plain text. This brings security risks. It is recommended that you select **cipher** to save the password in cipher text.	The value is a string of 1 to 8 case-sensitive characters without spaces. When double quotation marks are used around the string, spaces are allowed in the string.

Parameter	Description	Value
cipher *cipher-key*	Specifies the authentication key in cipher text authentication mode.	The value a string of case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string. Passwords are saved in ciphertext in the configuration file with the length of 48. 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 32 or 48 characters. **NOTE** A 32-character ciphertext password configured in an earlier version is also supported in this version.
md5 *md5-key*	Specifies the authentication key in MD5 authentication mode.	The value a string of case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string. Passwords are saved in ciphertext in the configuration file with the length of 48. 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 24, or 32, or 48 characters. **NOTE** A 32-character ciphertext password configured in an earlier version is also supported in this version.

NOTE

For security purposes, you are advised to use MD5 as the authentication algorithm of VRRP.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To be compatible with VRRP defined in earlier version and interwork with other devices, VRRP provides simple authentication and MD5 authentication. The **vrrp vrid authentication-mode** command configures an authentication mode and an authentication key for a VRRP group.

Prerequisites

A VRRP group has been configured on a specified interface.

Precautions

Devices in a VRRP group must be configured with the same authentication mode and authentication key; otherwise, the VRRP group cannot negotiate the Master and Backup states.

Example

Set the authentication mode of the VRRP group with VRID 2 on VLANIF100 to MD5 authentication and set the authentication key to **Huawei-1**.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] vrrp vrid 2 virtual-ip 10.1.1.1
[HUAWEI-Vlanif100] vrrp vrid 2 authentication-mode md5 Huawei-1
```

Set the authentication mode of the VRRP group with VRID 2 on GE0/0/1 to MD5 authentication and set the authentication key to **Huawei-1**.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] vrrp vrid 2 virtual-ip 10.1.1.1
[HUAWEI-GigabitEthernet0/0/1] vrrp vrid 2 authentication-mode md5 Huawei-1
```

12.2.38 vrrp vrid backup-forward

Function

The **vrrp vrid backup-forward** command enables the backup device in a VRRP backup group to forward traffic.

The **undo vrrp vrid backup-forward** command disables the backup device in a VRRP backup group from forwarding traffic.

By default, the backup device in a VRRP backup group is disabled from forwarding traffic.

Format

vrrp vrid *virtual-router-id* **backup-forward**

undo vrrp vrid *virtual-router-id* **backup-forward**

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
virtual-router-id	Specifies the ID of a VRRP backup group.	The value is an integer ranging from 1 to 255.

Views

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

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On large aggregation networks of enterprises, terminal users use active and standby links to access aggregation devices that have a VRRP backup group deployed. The aggregation device connects to the active link is the master device, and that connects to the standby link is the backup device. If the active link or the master device fails, a link switchover occurs. However, the master/backup switchover in the VRRP backup group has not yet completed. Therefore, a traffic interruption occurs and lasts for a short period.

To prevent traffic interruptions in such scenarios, run the **vrrp vrid backup-forward** command to enable the backup device in a VRRP backup group to forward traffic. This configuration ensures carrier-class reliability.

Prerequisites

A VRRP backup group has been created using the **vrrp vrid virtual-ip** command in the interface view.

Precautions

The backup device can forward traffic with the destination MAC address being the virtual MAC address. If a downstream switch broadcasts a packet with the

destination MAC address being the virtual MAC address, the backup device will also forward this packet. Therefore, two copies of this packet will be sent. To prevent duplicate traffic, do not run the **vrrp vrid backup-forward** command in scenarios other than the one where high reliability is required on large aggregation networks of enterprises.

Example

Create VRRP backup group 1 on GE0/0/2.1 and enable the backup device in the VRRP backup group to forward traffic.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/2.1
[HUAWEI-GigabitEthernet0/0/2.1] vrrp vrid 1 virtual-ip 10.1.1.100
[HUAWEI-GigabitEthernet0/0/2.1] vrrp vrid 1 backup-forward
```

12.2.39 vrrp vrid preempt-mode disable

Function

The **vrrp vrid preempt-mode disable** command configures the device in a VRRP group in non-preemption mode.

The **undo vrrp vrid preempt-mode** command restores the default preemption mode.

By default, the device uses the immediate preemption mode.

Format

vrrp vrid *virtual-router-id* **preempt-mode disable**

undo vrrp vrid *virtual-router-id* **preempt-mode**

Parameters

Parameter	Description	Value
vrid *virtual-router-id*	Specifies the VRID of a VRRP group.	The value is an integer that ranges from 1 to 255.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To enable the device with higher priority in a VRRP group to be the master, set the preemption mode on the device. In non-preemption mode, as long as the master is working properly, the backup with higher priority cannot be the master.

NOTE

When non-preemption is disabled, the preemption delay is restored to 0 seconds immediately.

Prerequisites

The **vrrp vrid virtual-ip** command has been executed on an interface to create a VRRP group.

Example

Configure VRRP group 1 in non-preemption mode on the VLANIF interface.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] vrrp vrid 1 virtual-ip 10.1.1.2
[HUAWEI-Vlanif100] vrrp vrid 1 preempt-mode disable
```

Configure VRRP group 1 in non-preemption mode on the Ethernet interface.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] vrrp vrid 1 virtual-ip 10.1.1.2
[HUAWEI-GigabitEthernet0/0/1] vrrp vrid 1 preempt-mode disable
```

12.2.40 vrrp vrid preempt-mode timer delay

Function

The **vrrp vrid preempt-mode timer delay** command sets the preemption delay for the device in a VRRP group.

The **undo vrrp vrid preempt-mode timer delay** command restores the default preemption delay for the device in a VRRP group.

By default, the preemption delay is 0 seconds.

Format

vrrp vrid *virtual-router-id* **preempt-mode timer delay** *delay-value*

undo vrrp vrid *virtual-router-id* **preempt-mode timer delay**

Parameters

Parameter	Description	Value
vrid *virtual-router-id*	Specifies the VRID of a VRRP group.	The value is an integer that ranges from 1 to 255.

Parameter	Description	Value
delay *delay-value*	Specifies the preemption delay.	The value is an integer that ranges from 0 to 3600, in seconds. The default value is 0.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If the backup in a VRRP group does not receive VRRP Advertisement packets from the master within a specified period of time, the backup becomes the master. On an unstable network, even if the master is working properly, the backup may not receive packets from the master because of network congestion. In this case, the VRRP group status will flap and traffic is lost. To prevent frequent switching of the VRRP group status, run the **vrrp vrid preempt-mode timer delay** command to set the preemption delay so that the backup becomes the master only after the delay expires.

Precautions

You are advised to set the preemption delay of the backup in a VRRP group to 0, configure the master in preemption mode, and set the preemption delay to be longer than 15s. These settings allow a period of time for status synchronization between the uplink and downlink on devices in a VRRP group on an unstable network. If the preceding settings are not used, two masters coexist and user devices may learn an incorrect master address. As a result, traffic is interrupted.

- The preemption delay refers to the delay before the backup switches to the master. Therefore, the IP address owner is irrelevant to the preemption delay. After the IP address owner recovers, it becomes the master immediately, without any delay.
- On a stable network, a short preemption delay is recommended. When the master is faulty, the backup with the highest priority can rapidly switch to the master. This prevents traffic loss. On an unstable network, a long preemption delay is recommended. This prevents traffic loss caused by frequent switching of the VRRP group status.

Example

Set the preemption delay of VRRP group 1 to 5 seconds on the VLANIF interface.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] vrrp vrid 1 preempt-mode timer delay 5
```


Set the preemption delay of VRRP group 1 to 5 seconds on the Ethernet interface.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] vrrp vrid 1 preempt-mode timer delay 5
```

12.2.41 vrrp vrid priority

Function

The **vrrp vrid priority** command sets the priority of the device in a VRRP group.

The **undo vrrp vrid priority** command restores the default priority of the device in a VRRP group.

By default, the priority of the device in a VRRP group is 100.

Format

vrrp vrid *virtual-router-id* **priority** *priority-value*

undo vrrp vrid *virtual-router-id* **priority**

Parameters

Parameter	Description	Value
vrid *virtual-router-id*	Specifies the VRID of a VRRP group.	The value is an integer that ranges from 1 to 255.
priority *priority-value*	Specifies the priority of the device in a VRRP group.	The value is an integer that ranges from 1 to 254. A larger value indicates a higher priority.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To configure the device in a VRRP group as the default gateway, run the **vrrp vrid priority** command to specify the highest priority for the device so that the device can become the master.

Prerequisites

The **vrrp vrid virtual-ip** command has been executed to create a VRRP group.

Precautions

- Priority 0 is reserved in the system. Priority 255 is reserved for the IP address owner.
- When devices in a VRRP group have the same priority, the device that first changes to master state becomes the master. If devices attempt to be the master simultaneously, the device where the interface with the largest IP address is located becomes the master.

Example

Set the priority of the switch in VRRP group 1 to 150 on the VLANIF interface.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] vrrp vrid 1 virtual-ip 10.1.1.2
[HUAWEI-Vlanif100] vrrp vrid 1 priority 150
```

Set the priority of the switch in VRRP group 1 to 150 on the Ethernet interface.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] vrrp vrid 1 virtual-ip 10.1.1.2
[HUAWEI-GigabitEthernet0/0/1] vrrp vrid 1 priority 150
```

12.2.42 vrrp vrid timer advertise

Function

The **vrrp vrid timer advertise** command sets the interval at which the master sends VRRP Advertisement packets.

The **undo vrrp vrid timer advertise** command restores the default interval at which the master sends VRRP Advertisement packets.

By default, the master sends VRRP Advertisement packets every 1 second.

Format

vrrp vrid *virtual-router-id* **timer advertise** *advertise-interval*

undo vrrp vrid *virtual-router-id* **timer advertise**

Parameters

Parameter	Description	Value
vrid *virtual-router-id*	Specifies the VRID of a VRRP group.	The value is an integer that ranges from 1 to 255.

Parameter	Description	Value
advertise *advertise-interval*	Specifies the interval at which the master sends VRRP Advertisement packets.	The value is an integer, in seconds. In VRRPv2, the value ranges from 1 to 255. In VRRPv3, the value ranges from 1 to 40.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The master in a VRRP group sends VRRP Advertisement packets to backups at intervals to notify that it is working properly. If the backup with the highest priority does not receive any VRRP Advertisement packets from the master at the specified interval, it considers the master faulty and becomes the master. The **vrrp vrid timer advertise** command sets the interval at which the master sends VRRP Advertisement packets.

Prerequisites

The **vrrp vrid virtual-ip** command has been executed on an interface to create a VRRP group.

Precautions

If a longer interval is used, backups in the same VRRP group cannot detect the fault on the master in a timely manner, causing packet loss. If a shorter interval is used, system resources are occupied. In addition, when network traffic is heavy or the network is unstable, backups may not receive packets after the Master_Down_Interval timer expires. As a result, the VRRP group status is incorrectly switched. Set the interval based on actual networking. The algorithm for calculating the value of the Master_Down_Interval timer is as follows:

Master_Down_Interval = (3 x Advertisement_Interval) + Skew_time

Skew_Time = (256 – Priority) / 256

When the interval for sending VRRP Advertisement packets on the master and backup in the same VRRP group is different, the master sends VRRP Advertisement packets at the configured interval.

Example

Set the interval at which the master in VRRP group 1 sends VRRP Advertisement packets to 5 seconds on the VLANIF interface.


```
<HUAWEI> system-view
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] vrrp vrid 1 virtual-ip 10.1.1.2
[HUAWEI-Vlanif100] vrrp vrid 1 timer advertise 5
```

Set the interval at which the master in VRRP group 1 sends VRRP Advertisement packets to 5 seconds on the Ethernet interface.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] vrrp vrid 1 virtual-ip 10.1.1.2
[HUAWEI-GigabitEthernet0/0/1] vrrp vrid 1 timer advertise 5
```

12.2.43 vrrp vrid track admin-vrrp vrid

Function

The **vrrp vrid track admin-vrrp vrid** command binds a VRRP group to an mVRRP group.

The **undo vrrp vrid track admin-vrrp** command unbinds a VRRP group from an mVRRP group.

By default, no VRRP group is bound to an mVRRP group.

Format

vrrp vrid *virtual-router-id1* **track admin-vrrp interface** *interface-type interface-number* **vrid** *virtual-router-id2* **unflowdown**

undo vrrp vrid *virtual-router-id1* **track admin-vrrp**

Parameters

Parameter	Description	Value
vrid *virtual-router-id1*	Specifies the VRID of a VRRP group.	The value is an integer that ranges from 1 to 255.
vrid *virtual-router-id2*	Specifies the VRID of an mVRRP group.	The value is an integer that ranges from 1 to 255.
interface-type interface-number	Specifies the type and number of an interface configured with an mVRRP group. • *interface-type* specifies the interface type. • *interface-number* specifies the interface number.	-

Parameter	Description	Value
unflowdown	Allows the interface where a VRRP group bound to an mVRRP group is configured to remain in Up state if the mVRRP group is in Backup or Initialize state.	-

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If multiple VRRP groups are configured on the device, each group sends VRRP Advertisement packets to maintain its state machine. As a result, a large number of VRRP Advertisement packets are generated, which occupy network bandwidth resources and cause CPU performance to deteriorate. To solve the problem, run the **vrrp vrid track admin-vrrp vrid** command to bind a VRRP group to an mVRRP group. After a VRRP group is bound to an mVRRP group, the VRRP group does not send VRRP Advertisement packets to negotiate the Master and Backup states. The mVRRP group determines the status of the bound VRRP group. This method greatly reduces the impact of VRRP Advertisement packets on network bandwidth and CPU performance.

This mode is used on a network where uplink and downlink traffic can be transmitted along different paths. **unflowdown** can be configured to allow the mVRRP group to determine the status of its bound VRRP group. Uplink traffic travels through the master and then reaches the upper-layer network, and downlink traffic travels through either the master or backup to reach users.

Prerequisites

A VRRP group and an mVRRP group have been created.

Precautions

The **vrrp vrid track admin-vrrp vrid** command can be used only on the interface where the bound VRRP group is configured. This command cannot be used on the interface where an mVRRP group is configured.

VRRP4 and VRRP6 can be configured on an interface simultaneously. However, there are limitations:

- A VRRP4 group can be bound to only an mVRRP4 group, and a VRRP6 group can be bound to only an mVRRP6 group.

- At most one VRRP4 group and one VRRP6 group can be configured on an interface. In addition, **unflowdown** must be used. An interface cannot be configured with multiple VRRP4 or VRRP6 groups.

If multiple service VRRP backup groups are configured on an interface, a single service VRRP backup group can be bound to the mVRRP backup group.

Example

Bind VRRP group 1 to mVRRP group 2 on the VLANIF interface.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 10
[HUAWEI-Vlanif10] vrrp vrid 1 track admin-vrrp interface vlanif 20 vrid 2 unflowdown
```

Bind VRRP group 1 to mVRRP group 2 on the Ethernet interface.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] vrrp vrid 1 track admin-vrrp interface GigabitEthernet 0/0/2 vrid 2 unflowdown
```

12.2.44 vrrp vrid track bfd-session

Function

The **vrrp vrid track bfd-session** command associates a VRRP group with a BFD session.

The **undo vrrp vrid track bfd-session** command disassociates a VRRP group from a BFD session.

By default, a VRRP group is not associated with a BFD session.

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

vrrp vrid *virtual-router-id* **track bfd-session** { *bfd-session-id* | **session-name** *bfd-configure-name* } [**increased** *value-increased* | **reduced** *value-reduced*]

undo vrrp vrid *virtual-router-id* **track bfd-session** [*bfd-session-id* | **session-name** *bfd-configure-name*]

vrrp vrid *virtual-router-id* **track bfd-session** { *bfd-session-id* | **session-name** *bfd-configure-name* } **peer** (Only the sub-interfaces of 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
vrid *virtual-router-id*	Specifies the VRID of a VRRP group.	The value is an integer that ranges from 1 to 255.
bfd-session-id	Specifies the local discriminator of the monitored BFD session.	The value is an integer that ranges from 1 to 8191.
session-name *bfd-configure-name*	Specifies the name of the monitored BFD session.	The value is a string of 1 to 15 case-insensitive characters without spaces. When double quotation marks are used around the string, spaces are allowed in the string.
increased *value-increased*	Specifies the value by which the priority increases when the monitored BFD session becomes Down.	The value is an integer that ranges from 1 to 255. The maximum priority value is 254.
reduced *value-reduced*	Specifies the value by which the priority decreases when the monitored BFD session becomes Down.	The value is an integer that ranges from 1 to 255. The priority can decrease to 1. By default, when the monitored BFD session becomes Down, the VRRP priority decreases by 10.
peer	Indicates that the monitored BFD session is a peer BFD session.	-

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Association between a VRRP group and a BFD session implements the following functions:

1. Rapid active/standby switchover: When the link of a VRRP group or the master is faulty, the backup becomes the master after a certain period of time (second level), causing packet loss. You can associate the VRRP group with a BFD session on the backup so that the BFD session can rapidly detect communication faults of the VRRP group. When the BFD session detects a fault, it notifies the VRRP group that the priority of the backup needs to be increased. Then an active/standby switchover is triggered immediately. This millisecond-level switchover reduces traffic loss. When the monitored BFD session recovers, the original priority of the device in the VRRP group is restored.
2. Monitoring the uplink: Because VRRP cannot detect faults on the uplink of a VRRP group, services are interrupted. You can associate the VRRP group with a BFD session on the master so that the BFD session monitors the uplink status of the master. When the BFD session detects a fault on the uplink, it notifies the VRRP group that the priority of the master needs to be decreased. Then an active/standby switchover is triggered immediately. This reduces the impact of the uplink fault on service forwarding. When the monitored BFD session recovers, the original priority of the device in the VRRP group is restored.

Prerequisites

A VRRP group has been created and a static BFD session or a static BFD session with automatically negotiated discriminators has been created.

Precautions

After a VRRP group is associated with a BFD session, the BFD session type cannot be modified. Before deleting the BFD session type, you must delete all original configurations.

After a VRRP group is associated with a BFD session, set **increased** *value-increased* or **reduced** *value-reduced* to an appropriate value. This setting ensures that an active/standby switchover is performed immediately when the monitored BFD session becomes Down.

Multiple VRRP groups can monitor a BFD session, and a VRRP group can monitor a maximum of eight BFD sessions simultaneously.

NOTE

When associating a VRRP group with a BFD session, note the following points:

- The master and backup in the VRRP group must work in preemption mode. It is recommended that the preemption delay be 0 on the backup and larger than 0 on the master.
- If an IP address owner exists in the VRRP group, the VRRP group cannot monitor the BFD session.
- If **session-name** *bfd-configure-name* is specified, the VRRP group can be bound to only the static BFD session with automatically negotiated discriminators.
- If *bfd-session-id* is specified, the VRRP group can be bound to only the static BFD session.

Example

Configure VRRP group 1 to monitor the BFD session with local discriminator 1 on VLANIF 100.


```
<HUAWEI> system-view
[HUAWEI] bfd
[HUAWEI-bfd] quit
[HUAWEI] bfd abc bind peer-ip 10.1.1.1 interface vlanif 100
[HUAWEI-bfd-session-abc] discriminator local 1
[HUAWEI-bfd-session-abc] discriminator remote 2
[HUAWEI-bfd-session-abc] commit
[HUAWEI-bfd-session-abc] quit
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] vrrp vrid 1 virtual-ip 10.1.1.12
[HUAWEI-Vlanif100] vrrp vrid 1 track bfd-session 1 reduced 40
```

Configure VRRP group 1 to monitor the BFD session with local discriminator 1 on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] bfd
[HUAWEI-bfd] quit
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] quit
[HUAWEI] bfd abc bind peer-ip 10.1.1.1 interface gigabitethernet 0/0/1
[HUAWEI-bfd-session-abc] discriminator local 1
[HUAWEI-bfd-session-abc] discriminator remote 2
[HUAWEI-bfd-session-abc] commit
[HUAWEI-bfd-session-abc] quit
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] vrrp vrid 1 virtual-ip 10.1.1.12
[HUAWEI-GigabitEthernet0/0/1] vrrp vrid 1 track bfd-session 1 reduced 40
```

Configure VRRP group 1 to monitor the BFD session **hello** on VLANIF 100.

```
<HUAWEI> system-view
[HUAWEI] bfd
[HUAWEI-bfd] quit
[HUAWEI] bfd hello bind peer-ip 10.2.1.1 interface vlanif 100 source-ip 10.2.1.2 auto
[HUAWEI-bfd-session-hello] commit
[HUAWEI-bfd-session-hello] quit
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] vrrp vrid 1 virtual-ip 10.2.1.12
[HUAWEI-Vlanif100] vrrp vrid 1 track bfd-session session-name hello reduced 40
```

Configure VRRP group 1 to monitor the BFD session **hello** on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] bfd
[HUAWEI-bfd] quit
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] quit
[HUAWEI] bfd hello bind peer-ip 10.2.1.1 interface gigabitethernet 0/0/1 source-ip 10.2.1.2 auto
[HUAWEI-bfd-session-hello] commit
[HUAWEI-bfd-session-hello] quit
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] vrrp vrid 1 virtual-ip 10.2.1.12
[HUAWEI-GigabitEthernet0/0/1] vrrp vrid 1 track bfd-session session-name hello reduced 40
```

12.2.45 vrrp vrid track interface

Function

The **vrrp vrid track interface** command associates a VRRP group with an interface.

The **undo vrrp vrid track interface** command disassociates a VRRP group from an interface.

By default, a VRRP group is not associated with an interface.

Format

vrrp vrid *virtual-router-id* **track interface** *interface-type interface-number* [**increased** *value-increased* | **reduced** *value-reduced*]

undo vrrp vrid *virtual-router-id* **track interface** [*interface-type interface-number*]

Parameters

Parameter	Description	Value
vrid *virtual-router-id*	Specifies the VRID of a VRRP group.	The value is an integer that ranges from 1 to 255.
interface *interface-type interface-number*	Specifies the type and number of an interface monitored by a VRRP group. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number. **NOTE** A VRRP backup group can track Layer 2 and Layer 3 interfaces. ● If the tracked interface is a Layer 2 interface, the VRRP backup group tracks the physical status of the Layer 2 interface and changes its own priority based on the tracked physical status. ● If the tracked interface is a Layer 3 interface, the VRRP backup group tracks the protocol status of the Layer 3 interface and changes its own priority based on the tracked protocol status.	-
increased *value-increased*	Specifies the value by which the priority increases when the monitored interface becomes Down.	The value is an integer that ranges from 1 to 255. The maximum priority value is 254.

Parameter	Description	Value
reduced *value-reduced*	Specifies the value by which the priority decreases when the monitored interface becomes Down.	The value is an integer that ranges from 1 to 255. The priority can decrease to 1. By default, when the monitored interface goes Down, the VRRP priority of the device decreases by 10.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

VRRP can only detect the status change of the interface on which a VRRP group is configured. VRRP cannot detect faults on the uplink interface, causing service interruption. You can run the **vrrp vrid track interface** command to associate a VRRP group with a device interface not in the VRRP group. When the monitored interface becomes Down, the priority of the device is adjusted and an active/standby switchover is triggered. Therefore, services can be forwarded correctly. When the status of the monitored interface recovers, the original priority of the device in the VRRP group is restored.

Prerequisites

The **vrrp vrid virtual-ip** command has been executed on an interface to create a VRRP group.

Precautions

After a VRRP group is associated with an interface, set **increased** *value-increased* or **reduced** *value-reduced* to an appropriate value. This setting ensures that an active/standby switchover is performed immediately when the monitored interface becomes Down.

NOTE

- The master and backup in the VRRP group must work in preemption mode. It is recommended that the preemption delay be 0 on the backup and larger than 0 on the master.
- If the device is the IP address owner (the virtual router IP address is used as the actual interface address), you cannot associate a VRRP group with an interface.
- Multiple VRRP groups can monitor an interface, and a VRRP group can monitor a maximum of 8 interfaces simultaneously.

Example

Associate VRRP group 1 with VLANIF 10 and set **reduced** *value-reduced* to 50 when VLANIF 10 becomes Down.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 20
[HUAWEI-Vlanif20] vrrp vrid 1 virtual-ip 10.1.1.1
[HUAWEI-Vlanif20] vrrp vrid 1 track interface vlanif 10 reduced 50
```

Associate VRRP group 1 with GE0/0/2 and set reduced *value-reduced* to 50 when GE0/0/2 becomes Down.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] vrrp vrid 1 virtual-ip 10.1.1.1
[HUAWEI-GigabitEthernet0/0/1] vrrp vrid 1 track interface gigabitethernet0/0/2 reduced 50
```

12.2.46 vrrp vrid track ip route

Function

The **vrrp vrid track ip route** command associates a VRRP group with a route.

The **undo vrrp vrid track ip route** command disassociates a VRRP group from a route.

By default, a VRRP group is not associated with a route.

Format

vrrp vrid *virtual-router-id* **track ip route** *ip-address* { *mask-address* | *mask-length* } [**vpn-instance** *vpn-instance-name*] [**reduced** *value-reduced*]

undo vrrp vrid *virtual-router-id* **track ip route** [*ip-address* { *mask-address* | *mask-length* } [**vpn-instance** *vpn-instance-name*]]

Parameters

Parameter	Description	Value
vrid *virtual-router-id*	Specifies the VRID of a VRRP group.	The value is an integer that ranges from 1 to 255.
ip-address	Specifies the destination address of the monitored route.	The value is in dotted decimal notation.
mask-address	Specifies the mask of the destination address of the monitored route.	The value is in dotted decimal notation.
mask-length	Specifies the mask length of the destination address of the monitored route.	The value is an integer that ranges from 0 to 32.

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Specifies the name of a VPN instance.	The value must be an existing VPN instance name.
reduced *value-reduced*	Specifies the value by which the master's priority decreases if the monitored route is withdrawn or becomes inactive.	The value is an integer that ranges from 1 to 255. The priority can decrease to 1. By default, the master's priority decreases by 10 if the associated route is withdrawn or becomes inactive.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To improve device reliability, two user gateways are configured to work in master/backup mode, and VRRP is enabled on these gateways to determine their Master and Backup states. Although a VRRP group has been configured, access devices may not detect route changes caused by the faulty uplink or network topology change. Consequently, data traffic is lost.

You can associate a VRRP group with a route for forwarding uplink traffic. When the route is withdrawn or becomes inactive, the master' priority is adjusted and an active/standby switchover is performed. When the status of the monitored route recovers, the original priority of the master in the VRRP group is restored.

Pre-configuration Tasks

A VRRP group and a routing protocol such as OSPF or IS-IS have been configured.

Precautions

The VRRP group to be associated with a route cannot contain an IP address owner.

The master and backup in the VRRP group must work in preemption mode. It is recommended that the preemption delay be 0 on the backup and non-0 on the master.

When associating a VRRP group with a route in a VPN instance, note the following points:

- If the VPN instance does not exist, association between the VRRP group and the VPN route cannot work.
- If the VPN instance is deleted after the VRRP group is associated with the VPN route, association between the VRRP group and the VPN route is also deleted.

Multiple VRRP groups can monitor a route, and a VRRP group can monitor a maximum of eight routes simultaneously.

Example

Configure VRRP group 1 to monitor the route on 10.2.1.0, and set the value by which the master's priority decreases if the monitored route is withdrawn or becomes inactive to 20.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] vrrp vrid 1 virtual-ip 10.1.1.12
[HUAWEI-Vlanif100] vrrp vrid 1 track ip route 10.2.1.0 24 reduced 20
```

12.2.47 vrrp vrid track nqa

Function

The **vrrp vrid track nqa** command associates a VRRP group with an NQA test instance to implement a rapid active/standby switchover.

The **undo vrrp vrid track nqa** command disassociates a VRRP group from an NQA test instance.

By default, a VRRP group is not associated with an NQA test instance.

Format

vrrp vrid *virtual-router-id* **track nqa** *admin-name test-name* [**reduced** *value-reduced*]

undo vrrp vrid *virtual-router-id* **track nqa** [*admin-name test-name*]

Parameters

Parameter	Description	Value
vrid *virtual-router-id*	Specifies the VRID of a VRRP group.	The value is an integer that ranges from 1 to 255.
admin-name	Specifies the administrator name of an NQA test instance.	The value is a string of 1 to 32 case-sensitive characters without spaces. When double quotation marks are used around the string, spaces are allowed in the string.

Parameter	Description	Value
test-name	Specifies the name of an NQA test instance.	The value is a string of 1 to 32 case-sensitive characters without spaces. When double quotation marks are used around the string, spaces are allowed in the string.
reduced *value-reduced*	Specifies the value by which the master's priority reduces if the NQA test instance detects that the uplink is unavailable.	The value is an integer that ranges from 1 to 255. The priority can decrease to 1. By default, the master's priority value decreases by 10 if the associated NQA test instance detects that the uplink is unavailable.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To improve device reliability, two user gateways are configured to work in master/backup mode, and VRRP is enabled on these gateways to determine their Master and Backup states. Although a VRRP group has been configured, the uplink may be unreachable and access devices may not detect the faulty uplink. Consequently, data traffic is lost.

You can associate a VRRP group with an NQA test instance to solve this problem. The NQA test instance periodically sends ICMP packets to detect whether the destination IP address of the uplink is reachable. When the destination IP address is unreachable, the NQA test instance reports the fault to the associated VRRP group and instructs the VRRP group to adjust the priority, implementing an active/standby switchover. When the status of the monitored NQA test instance recovers, the original priority of the master in the VRRP group is restored.

Prerequisites

An NQA test instance of ICMP has been configured.

Precautions

- The master and backup in the VRRP group must work in preemption mode. It is recommended that the preemption delay be 0 on the backup and non-0 on the master.
- The VRRP group to be associated with a route cannot contain an IP address owner.
- The VRRP group can only be associated with an NQA test instance of ICMP.
- A VRRP group can monitor a maximum of eight NQA test instances.

Example

Associate a VRRP group with NQA test instance **user user1** on VLANIF100 and set **reduced** *value-reduced* to 20 when the destination IP address is unreachable.

```
<HUAWEI> system-view
[HUAWEI] nqa test-instance user user1
[HUAWEI-nqa-user-user1] test-type icmp
[HUAWEI-nqa-user-user1] destination-address ipv4 10.1.1.1
[HUAWEI-nqa-user-user1] frequency 10
[HUAWEI-nqa-user-user1] probe-count 2
[HUAWEI-nqa-user-user1] start now
[HUAWEI-nqa-user-user1] quit
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] vrrp vrid 1 virtual-ip 10.2.1.12
[HUAWEI-Vlanif100] vrrp vrid 1 track nqa user user1 reduced 20
```

12.2.48 vrrp vrid version-3 send-packet-mode

Function

The **vrrp vrid version-3 send-packet-mode** command configures a mode in which VRRPv3 Advertisement packets are sent on an interface.

The **undo vrrp vrid version-3 send-packet-mode** command restores the default mode.

By default, VRRPv3 Advertisement packets are sent in **v3-only** mode.

Format

vrrp vrid *virtual-router-id* **version-3 send-packet-mode** { **v2-only** | **v3-only** | **v2v3-both** }

undo vrrp vrid *virtual-router-id* **version-3 send-packet-mode**

Parameters

Parameter	Description	Value
vrid *virtual-router-id*	Specifies the VRID of a VRRP group.	The value is an integer that ranges from 1 to 255.
v2-only	Indicates that only VRRPv2 Advertisement packets are sent.	-

Parameter	Description	Value
v3-only	Indicates that only VRRPv3 Advertisement packets are sent.	-
v2v3-both	Indicates that both VRRPv2 and VRRPv3 Advertisement packets are sent.	-

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If devices in a VRRP group use different VRRP version numbers, the VRRP group may fail to negotiate the status. This is because a VRRPv2-enabled device can only receive VRRPv2 Advertisement packets and discards the received VRRPv3 Advertisement packets. You can set the mode in which VRRP Advertisement packets are sent on the VRRPv3-enabled device so that the VRRPv2-enabled and VRRPv3-enabled devices can negotiate the status.

Precautions

- Only VRRPv3 supports this command.
- If the **vrrp version-3 send-packet-mode** command is used in the system view and interface view simultaneously, the configuration in the interface view takes effect.

NOTE

If a large number of VRRP groups are configured, **v2v3-both** is not recommended.

Example

Set the mode in which VRRPv3 Advertisement packets are sent to **v2-only** on VLANIF100.

```
<HUAWEI> system-view
[HUAWEI] vrrp version v3
[HUAWEI] vrrp version-3 send-packet-mode v2-only
Warning: The globally configured packet sending mode will take effect for every VRRP backup group.Continue?[Y/N]:y
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] vrrp vrid 24 version-3 send-packet-mode v2-only
```

Set the mode in which VRRPv3 Advertisement packets are sent to **v2-only** on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] vrrp version v3
[HUAWEI] vrrp version-3 send-packet-mode v2-only
Warning: The globally configured packet sending mode will take effect for every VRRP backup group.Continue?[Y/N]:y
```



```
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] vrrp vrid 24 version-3 send-packet-mode v2-only
```

12.2.49 vrrp vrid virtual-ip

Function

The **vrrp vrid virtual-ip** command creates a VRRP group and assigns a virtual IP address to the group.

The **undo vrrp vrid virtual-ip** command deletes the virtual IP address of a VRRP group.

By default, no VRRP group is created.

Format

vrrp vrid *virtual-router-id* **virtual-ip** *virtual-address*

undo vrrp vrid *virtual-router-id* [**virtual-ip** *virtual-address*]

Parameters

Parameter	Description	Value
vrid *virtual-router-id*	Specifies the VRID of a VRRP group.	The value is an integer that ranges from 1 to 255.
virtual-ip *virtual-address*	Specifies the virtual IP address of a VRRP group.	The value is in dotted decimal notation.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In practice, hosts use the default gateway to communicate with external networks. As value-added services such as IPTV or video conferencing services are widely deployed, hosts may fail to communicate with external networks if the default gateway fails. Configuring dynamic routing protocols such as RIP, OSPF, or ICMP can improve system reliability. However, it is difficult to configure dynamic routing protocols and some hosts may not support dynamic routing protocols. VRRP virtualizes multiple routing devices into a virtual router without changing the networking. The virtual router IP address is configured as the default gateway address.

If users on a network have the same reliability requirements, configure multiple virtual IP addresses for a VRRP group. By doing this, one virtual IP address serves one separate user group, and the default gateway address remains consistent regardless of changes in VRRP device locations. A VRRP group can be assigned a maximum of 16 virtual IP addresses.

Precautions

The MAC address of the VBDIF must differ from the virtual MAC address of the VRRP group. (The last two bits of the VRRP virtual MAC address are determined by the VRID. For example, The VRID of the virtual router composed of SwitchA and SwitchB is 3, so the MAC address of the VRRP group is 00-00-5E-00-01-03).

If all the virtual IP addresses in a VRRP group are deleted, the VRRP group is deleted automatically.

For VRRP4 or VRRP6 groups configured on a device, each VRID can be bound to a maximum of 16 ports.

After the **vrrp vrid virtual-ip** command is run on an interface, when the ARP entries learned by the interface are aged, the device sends ARP aging probe packets with the source IP address being the interface's IP address. The virtual IP address of the interface is not used as the source IP address.

When VRRP and static ARP are configured simultaneously, note the following points:

- When VRRP is configured on a VLANIF interface or Ethernet interface, the IP address corresponding to the VLANIF interface or Ethernet interface in a static ARP entry cannot be set to the virtual IP address of a VRRP group. Otherwise, services cannot be forwarded between devices. For example, if a static ARP entry contains IP address 10.1.1.1, the IP address 10.1.1.1 cannot be used as the virtual IP address.
- When VRRP is configured on a VLANIF interface or Ethernet interface, the virtual IP address of a VRRP group cannot be used as the IP address corresponding to the VLANIF interface or Ethernet interface in a static ARP entry. Otherwise, services cannot be forwarded between devices. For example, if the VRRP group uses virtual IP address 10.1.1.1, the IP address 10.1.1.1 cannot be used in a static ARP entry.

NOTE

- VRRP groups must use different virtual IP addresses.
- Two devices in a VRRP group must be configured with the same VRID.
- VRRP groups on different interfaces of a device can be configured with the same VRID.
- A virtual IP address must be different from the IP address of a user host. If the user host IP address is the same as the virtual IP address, all packets on the local network segment are sent to the user host. As a result, data of this network segment cannot be forwarded correctly.

Example

Create a VRRP group on VLANIF 100 with ID 1 and virtual IP address 10.10.10.10.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] vrrp vrid 1 virtual-ip 10.10.10.10
```


Create a VRRP group with VRID 1 and virtual IP address 10.10.10.10 on GE0/0/1.
```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] vrrp vrid 1 virtual-ip 10.10.10.10
```

12.2.50 vrrp6 nd send-mode simple

Function

The **vrrp6 nd send-mode simple** command enables a sub-interface for QinQ VLAN tag termination to send double-tagged ND packets carrying only the minimal inner VLAN ID when the VRRP status of the sub-interface in the Virtual Router Redundancy Protocol for IPv6 (VRRP6) backup group is master.

The **undo vrrp6 nd send-mode simple** command enables a sub-interface for QinQ VLAN tag termination to send double-tagged ND packets to all VLANs specified by the outer VLAN IDs and inner VLAN IDs when the VRRP status of the sub-interface in the VRRP6 backup group is master.

By default, double-tagged ND packets are sent to all VLANs specified by the outer VLAN IDs and inner VLAN IDs.

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

vrrp6 nd send-mode simple

undo vrrp6 nd send-mode simple

Parameters

None

Views

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

Default Level

2: Configuration level

Usage Guidelines

A sub-interface for QinQ VLAN tag termination sends double-tagged ND packets when the VRRP status of the sub-interface in the VRRP backup group is master. If there is a range for the inner VLAN IDs, the sub-interface sends ND packets to all VLANs in this range to update VRRP backup group's MAC address entry on a downstream switch, exposing a heavy burden on the system. To prevent this

problem, you can use the **vrrp6 nd send-mode simple** command to allow an ND packet carrying only the minimal inner VLAN ID to be sent, reducing the number of ND packets to be sent.

NOTE

The **vrrp6 nd send-mode simple** command takes effect within VLANs specified only by inner VLAN IDs rather than outer VLAN IDs. For example, VLAN IDs in the outer tag range from 1 to 10 and VLAN IDs in the inner tag range from 1 to 10. After the **vrrp6 nd send-mode simple** command is run, ND packets carrying only inner VLAN 1 and outer VLAN IDs ranging from 1 to 10 are sent. 10 ND packets (10 outer VLAN IDs x 1 inner VLAN ID) are sent.

The **vrrp6 nd send-mode simple** command is configured only on a sub-interface for QinQ VLAN tag termination.

Example

Allow ND packets carrying only inner VLAN 1 to be sent.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet0/0/1.1
[HUAWEI-GigabitEthernet0/0/1.1] qinq termination pe-vid 5 ce-vid 1 to 10
[HUAWEI-GigabitEthernet0/0/1.1] quit
[HUAWEI] ipv6
[HUAWEI] interface gigabitethernet0/0/1.1
[HUAWEI-GigabitEthernet0/0/1.1] ipv6 enable
[HUAWEI-GigabitEthernet0/0/1.1] ipv6 address auto link-local
[HUAWEI-GigabitEthernet0/0/1.1] vrrp6 vrid 1 virtual-ip FE80::7 link-local
[HUAWEI-GigabitEthernet0/0/1.1] vrrp6 nd send-mode simple
```

12.2.51 vrrp6 un-check hop-limit

Function

The **vrrp6 un-check hop-limit** command disables the device from checking the TTL value in VRRP6 Advertisement packets.

The **undo vrrp6 un-check hop-limit** command enables the device to check the TTL value in VRRP6 Advertisement packets.

By default, the system checks the TTL value in VRRP6 Advertisement packets.

Format

vrrp6 un-check hop-limit

undo vrrp6 un-check hop-limit

Parameters

None

Views

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

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

Default Level

2: Configuration level

Usage Guidelines

The device checks the TTL value in received VRRP6 Advertisement packets. If the TTL value of a VRRP6 Advertisement packet is not 255, the device discards the packet.

On certain networks, especially on a network where the device interworks with non-Huawei devices, valid packets may be discarded if TTL check is enabled. You can configure the device not to check the TTL value in VRRP6 Advertisement packets.

Example

Disable the device from checking the TTL value in VRRP6 Advertisement packets on VLANIF 100.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] vrrp6 un-check hop-limit
```

Disable the device from checking the TTL value in VRRP6 Advertisement packets on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] vrrp6 un-check hop-limit
```

12.2.52 vrrp6 vrid preempt-mode disable

Function

The **vrrp6 vrid preempt-mode disable** command configures the device in a VRRP6 group in non-preemption mode.

The **undo vrrp6 vrid preempt-mode** command restores the default preemption mode.

By default, the device uses the immediate preemption mode.

Format

vrrp6 vrid *virtual-router-id* **preempt-mode disable**

undo vrrp6 vrid *virtual-router-id* **preempt-mode**

Parameters

Parameter	Description	Value
vrid *virtual-router-id*	Specifies the VRID of a VRRP6 group.	The value is an integer that ranges from 1 to 255.

Views

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

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To enable the device with higher priority in a VRRP6 group to be the master, set the preemption mode on the device. In non-preemption mode, as long as the master is working properly, the backup with higher priority cannot be the master.

NOTE

When non-preemption is disabled, the preemption delay is restored to 0 seconds immediately.

Prerequisites

The **vrrp6 vrid virtual-ip** command has been executed on an interface to create a VRRP6 group.

Example

Configure VRRP6 group 1 in non-preemption mode on the VLANIF interface.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] vrrp6 vrid 1 virtual-ip FE80::7 link-local
[HUAWEI-Vlanif100] vrrp6 vrid 1 preempt-mode disable
```

Configure VRRP6 group 1 in non-preemption mode on the Ethernet interface.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] vrrp6 vrid 1 virtual-ip FE80::7 link-local
[HUAWEI-GigabitEthernet0/0/1] vrrp6 vrid 1 preempt-mode disable
```


12.2.53 vrrp6 vrid preempt-mode timer delay

Function

The **vrrp6 vrid preempt-mode timer delay** command sets the preemption delay for the device in a VRRP6 group.

The **undo vrrp6 vrid preempt-mode timer delay** command restores the default preemption delay for the device in a VRRP6 group.

By default, the preemption delay is 0 seconds, indicating immediate preemption.

Format

vrrp6 vrid *virtual-router-id* **preempt-mode timer delay** *delay-value*

undo vrrp6 vrid *virtual-router-id* **preempt-mode timer delay**

Parameters

Parameter	Description	Value
vrid *virtual-router-id*	Specifies the VRID of a VRRP6 group.	The value is an integer that ranges from 1 to 255.
delay *delay-value*	Specifies the preemption delay.	The value is an integer that ranges from 0 to 3600, in seconds. The default value is 0.

Views

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

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If the backup in a VRRP6 group does not receive VRRP6 Advertisement packets from the master within a specified period of time, the backup becomes the master. On an unstable network, even if the master is working properly, the backup may not receive packets from the master because of network congestion. In this case, the VRRP6 group status will flap and traffic is lost. To prevent frequent switching of the VRRP6 group status, run the **vrrp6 vrid preempt-mode timer delay**

command to set the preemption delay so that the backup becomes the master only after the delay expires.

Prerequisites

The **vrrp6 vrid virtual-ip** command has been executed to create a VRRP6 group.

Precautions

You are advised to set the preemption delay of the backup in a VRRP6 group to 0, configure the master in preemption mode, and set the preemption delay to be longer than 15s. These settings allow a period of time for status synchronization between the uplink and downlink on devices on an unstable network. If the preceding settings are not used, two masters coexist and user devices may learn an incorrect master address. As a result, traffic is interrupted.

- The preemption delay refers to the delay before the backup switches to the master. Therefore, the IP address owner is irrelevant to the preemption delay. After the IP address owner recovers, it becomes the master immediately without a delay.
- On a stable network, a short preemption delay is recommended. When the master is faulty, the backup can rapidly switch to the master. This prevents traffic loss. On an unstable network, a long preemption delay is recommended. This prevents traffic loss caused by frequent switching of the VRRP6 group status.

Example

Set the preemption delay of VRRP6 group 1 to 10 seconds on the VLANIF interface.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] vrrp6 vrid 1 virtual-ip FE80::7 link-local
[HUAWEI-Vlanif100] vrrp6 vrid 1 preempt-mode timer delay 10
```

Set the preemption delay of VRRP6 group 1 to 10 seconds on the Ethernet interface.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] vrrp6 vrid 1 virtual-ip FE80::7 link-local
[HUAWEI-GigabitEthernet0/0/1] vrrp6 vrid 1 preempt-mode timer delay 10
```

12.2.54 vrrp6 vrid priority

Function

The **vrrp6 vrid priority** command sets the priority of the device in a VRRP6 group.

The **undo vrrp6 vrid priority** command restores the default priority of the device in a VRRP6 group.

By default, the priority of the device in a VRRP6 group is 100.

Format

vrrp6 vrid *virtual-router-id* **priority** *priority-value*

undo vrrp6 vrid *virtual-router-id* **priority**

Parameters

Parameter	Description	Value
vrid *virtual-router-id*	Specifies the VRID of a VRRP6 group.	The value is an integer that ranges from 1 to 255.
priority *priority-value*	Specifies the priority of the device in a VRRP6 group.	The value is an integer that ranges from 1 to 254. A larger value indicates a higher priority.

Views

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

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To configure the device in a VRRP6 group as the default gateway, run the **vrrp6 vrid priority** command to specify the highest priority for the device so that the device can become the master.

Prerequisites

The **vrrp6 vrid virtual-ip** command has been executed to create a VRRP6 group.

Precautions

- Priority 0 is reserved in the system. Priority 255 is reserved for the IP address owner.
- When devices in a VRRP6 group have the same priority, the device that first changes to master state becomes the master. If devices attempt to be the master simultaneously, the device where the interface with the largest IP address is located becomes the master.

Example

Set the priority of the switch in VRRP6 group 2 to 120 on the VLANIF interface.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 100
```



```
[HUAWEI-Vlanif100] vrrp6 vrid 2 virtual-ip FE80::7 link-local
[HUAWEI-Vlanif100] vrrp6 vrid 2 priority 120
```

Set the priority of the switch in VRRP6 group 2 to 120 on the Ethernet interface.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] vrrp6 vrid 2 virtual-ip FE80::7 link-local
[HUAWEI-GigabitEthernet0/0/1] vrrp6 vrid 2 priority 120
```

12.2.55 vrrp6 vrid timer advertise

Function

The **vrrp6 vrid timer advertise** command sets the interval at which the master sends VRRP6 Advertisement packets.

The **undo vrrp6 vrid timer advertise** command restores the default interval at which the master sends VRRP6 Advertisement packets.

By default, the master sends VRRP6 Advertisement packets every 1 second.

Format

vrrp6 vrid *virtual-router-id* **timer advertise** *advertise-interval*

undo vrrp6 vrid *virtual-router-id* **timer advertise**

Parameters

Parameter	Description	Value
vrid *virtual-router-id*	Specifies the VRID of a VRRP6 group.	The value is an integer that ranges from 1 to 255.
advertise *advertise-interval*	Specifies the interval at which the master sends VRRP6 Advertisement packets.	The value is an integer that ranges from 100 to 4095, in centiseconds.

Views

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

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The master in a VRRP6 group sends VRRP6 Advertisement packets to backups at intervals to notify that it is working properly. If the backup with the highest priority does not receive any VRRP6 Advertisement packets from the master at the specified interval (usually, three times the interval for sending VRRP6 Advertisement packets), it considers the master faulty and becomes the master. The **vrrp6 vrid timer advertise** command sets the interval at which the master sends VRRP6 Advertisement packets.

Prerequisites

The **vrrp6 vrid virtual-ip** command has been executed on an interface to create a VRRP6 group.

Precautions

If a longer interval is used, backups in the same VRRP6 group cannot detect the fault on the master in a timely manner, causing packet loss. If a shorter interval is used, system resources are occupied. In addition, when network traffic is heavy or the network is unstable, backups may not receive packets after the Master_Down_Interval timer expires. As a result, the VRRP6 group status is incorrectly switched. Set the interval based on actual networking.

NOTE

- For VRRP for IPv4, set the same interval for sending VRRP Advertisement packets for members in a VRRP group to prevent multiple masters in the VRRP group.
- For VRRP for IPv6, even if you set different intervals for sending VRRP Advertisement packets for members in a VRRP6 group, there is only one master in a VRRP6 group.

Example

Set the interval at which the master in VRRP6 group 1 sends VRRP6 Advertisement packets to 200 centiseconds on the VLANIF interface.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] vrrp6 vrid 1 virtual-ip FE80::7 link-local
[HUAWEI-Vlanif100] vrrp6 vrid 1 timer advertise 200
```

Set the interval at which the master in VRRP6 group 1 sends VRRP6 Advertisement packets to 200 centiseconds on the Ethernet interface.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] vrrp6 vrid 1 virtual-ip FE80::7 link-local
[HUAWEI-GigabitEthernet0/0/1] vrrp6 vrid 1 timer advertise 200
```

12.2.56 vrrp6 vrid track admin-vrrp6 vrid

Function

The **vrrp6 vrid track admin-vrrp6 vrid** command binds a VRRP6 group to an mVRRP6 group.

The **undo vrrp6 vrid track admin-vrrp6** command unbinds a VRRP6 group from an mVRRP6 group.

By default, no VRRP6 group is bound to an mVRRP6 group.

Format

vrrp6 vrid *virtual-router-id1* **track admin-vrrp6 interface** *interface-type interface-number* **vrid** *virtual-router-id2* **unflowdown**

undo vrrp6 vrid *virtual-router-id1* **track admin-vrrp6**

Parameters

Parameter	Description	Value
vrid *virtual-router-id1*	Specifies the VRID of a VRRP6 group.	The value is an integer that ranges from 1 to 255.
vrid *virtual-router-id2*	Specifies the VRID of an mVRRP6 group.	The value is an integer that ranges from 1 to 255.
interface-type interface-number	Specifies the type and number of an interface configured with an mVRRP6 group.	-
unflowdown	Allows the interface where a VRRP6 group bound to an mVRRP6 group is configured to retain the Up state if the mVRRP6 group is in Backup or Initialize state.	-

Views

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

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If multiple VRRP6 groups are configured on the device, each group sends VRRP6 Advertisement packets to maintain its state machine. As a result, a large number of VRRP6 Advertisement packets are generated, which occupy network bandwidth

resources and cause CPU performance to deteriorate. To solve the problem, run the **vrrp6 vrid track admin-vrrp6 vrid** command to bind a VRRP6 group to an mVRRP6 group. After a VRRP6 group is bound to an mVRRP6 group, the VRRP6 group does not send VRRP6 Advertisement packets to negotiate the Master and Backup states. The mVRRP6 group determines the status of the bound VRRP6 group. This method greatly reduces the impact of VRRP6 Advertisement packets on network bandwidth and CPU performance.

This mode is used on a network where uplink and downlink traffic can be transmitted along different paths. **unflowdown** can be configured to allow the mVRRP6 group to determine the status of its bound VRRP6 group. Uplink traffic travels through the master and then reaches the upper-layer network, and downlink traffic travels through either the master or backup to reach users.

Prerequisites

A VRRP6 group and an mVRRP6 group have been created.

Precautions

The **vrrp6 vrid track admin-vrrp6 vrid** command can be used only on the interface where the bound VRRP6 group is configured. This command cannot be used on the interface where an mVRRP6 group is configured.

VRRP4 and VRRP6 can be configured on an interface simultaneously. However, there are limitations:

- A VRRP4 group can be bound to only an mVRRP4 group, and a VRRP6 group can be bound to only an mVRRP6 group.
- At most one VRRP4 group and one VRRP6 group can be configured on an interface. An interface cannot be configured with multiple VRRP4 or VRRP6 groups.

Example

Bind VRRP6 group 1 to mVRRP6 group 2 on the VLANIF interface.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 10
[HUAWEI-Vlanif10] vrrp6 vrid 1 track admin-vrrp6 interface vlanif 11 vrid 2 unflowdown
```

Bind VRRP6 group 1 to mVRRP6 group 2 on the Ethernet interface.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] vrrp6 vrid 1 track admin-vrrp6 interface gigabitethernet 0/0/2 vrid 2
unflowdown
```

12.2.57 vrrp6 vrid track bfd-session

Function

The **vrrp6 vrid track bfd-session** command associates a VRRP6 group with a BFD session.

The **undo vrrp6 vrid track bfd-session** command disassociates a VRRP6 group from a BFD session.

By default, a VRRP6 group is not associated with a BFD session.

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

vrrp6 vrid *virtual-router-id* **track bfd-session** { *session-id* | **session-name** *bfd-configure-name* } [**increased** *value-increased* | **reduced** *value-reduced*]

undo vrrp6 vrid *virtual-router-id* **track bfd-session** [*session-id* | **session-name** *bfd-configure-name*]

Parameters

Parameter	Description	Value
vrid *virtual-router-id*	Specifies the VRID of a VRRP6 group.	The value is an integer that ranges from 1 to 255.
session-id	Specifies the local discriminator of the monitored BFD session.	The value is an integer that ranges from 1 to 8191.
session-name *bfd-configure-name*	Specifies the name of the monitored BFD session.	The value is a string of 1 to 15 case-insensitive characters without spaces. **NOTE** When double quotation marks are used around the string, spaces are allowed in the string.
increased *value-increased*	Specifies the value by which the priority increases when the monitored BFD session becomes Down.	The value is an integer that ranges from 1 to 255. The maximum priority value is 254.
reduced *value-reduced*	Specifies the value by which the priority decreases when the monitored BFD session becomes Down.	The value is an integer that ranges from 1 to 255. The priority can decrease to 1. By default, when the monitored BFD session becomes Down, the VRRP6 priority decreases by 10.

Views

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

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

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Association between a VRRP6 group and a BFD session implements the following functions:

1. Rapid active/standby switchover: When the link of a VRRP6 group or the master is faulty, the backup becomes the master after a certain time (second level), causing packet loss. You can associate the VRRP6 group with a BFD session on the backup so that the BFD session can rapidly detect communication faults of the VRRP6 group. When the BFD session detects a fault, it notifies the VRRP6 group that the priority of the backup needs to be increased. Then an active/standby switchover is triggered immediately. This millisecond-level switchover reduces traffic loss. When the monitored BFD session recovers, the original priority of the device in the VRRP6 group is restored.
2. Monitoring the uplink: Because VRRP6 cannot detect faults on the uplink of a VRRP6 group, services are interrupted. You can associate the VRRP6 group with a BFD session on the master so that the BFD session monitors the uplink status of the master. When the BFD session detects a fault on the uplink, it notifies the VRRP6 group that the priority of the master needs to be decreased. Then an active/standby switchover is triggered immediately. This reduces the impact of the uplink fault on service forwarding. When the monitored BFD session recovers, the original priority of the device in the VRRP6 group is restored.

Prerequisites

A VRRP6 group has been created and a static BFD session or a static BFD session with automatically negotiated discriminators has been created.

Precautions

Currently, the device supports only association between VRRP6 and BFD for IPv4.

After a VRRP6 group is associated with a BFD session, the BFD session type cannot be modified. Before deleting the BFD session type, you must delete all original configurations.

After a VRRP6 group is associated with a BFD session, set an appropriate value of **increased** *value-increased* or **reduced** *value-reduced*. This setting ensures that an active/standby switchover is performed immediately when the monitored BFD session becomes Down.

Multiple VRRP6 groups can monitor a BFD session, and a VRRP6 group can monitor a maximum of eight BFD sessions simultaneously.

NOTE

When associating a VRRP6 group with a BFD session, note the following points:

- If an IPv6 address owner exists in the VRRP6 group, the VRRP6 group cannot monitor the BFD session.
- If **session-name** *bfd-configure-name* is specified, the VRRP6 group can be bound to only the static BFD session with automatically negotiated discriminators.
- If *session-id* is specified, the VRRP6 group can bind to only a static BFD session.

Example

Associate VRRP6 group 1 with the BFD session **hello** on VLANIF 100.

```
<HUAWEI> system-view
[HUAWEI] bfd
[HUAWEI-bfd] quit
[HUAWEI] bfd hello bind peer-ip 10.1.1.1 interface vlanif 100
[HUAWEI-bfd-session-hello] quit
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] vrrp6 vrid 1 virtual-ip FE80::7 link-local
[HUAWEI-Vlanif100] vrrp6 vrid 1 virtual-ip FC00::100
[HUAWEI-Vlanif100] vrrp6 vrid 1 track bfd session-name hello reduced 40
```

Associate VRRP6 group 1 with the BFD session **hello** on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] bfd
[HUAWEI-bfd] quit
[HUAWEI] bfd hello bind peer-ip 10.1.1.1 interface gigabitethernet 0/0/1
[HUAWEI-bfd-session-hello] quit
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] vrrp6 vrid 1 virtual-ip FE80::7 link-local
[HUAWEI-GigabitEthernet0/0/1] vrrp6 vrid 1 virtual-ip FC00::100
[HUAWEI-GigabitEthernet0/0/1] vrrp6 vrid 1 track bfd session-name hello reduced 40
```

12.2.58 vrrp6 vrid track interface

Function

The **vrrp6 vrid track interface** command associates a VRRP6 group with an interface.

The **undo vrrp6 vrid track interface** command disassociates a VRRP6 group from an interface.

By default, a VRRP6 group is not associated with an interface.

Format

vrrp6 vrid *virtual-router-id* **track interface** *interface-type interface-number* [**increased** *value-increased* | **reduced** *value-reduced*]

undo vrrp6 vrid *virtual-router-id* **track interface** [*interface-type interface-number*]

Parameters

Parameter	Description	Value
vrid *virtual-router-id*	Specifies the VRID of a VRRP6 group.	The value is an integer that ranges from 1 to 255.
interface-type interface-number	Specifies the type and number of an interface monitored by a VRRP6 group. • *interface-type* specifies the interface type. • *interface-number* specifies the interface number.	-
increased *value-increased*	Specifies the value by which the priority increases when the monitored interface becomes Down.	The value is an integer that ranges from 1 to 255. The maximum priority value is 254.
reduced *value-reduced*	Specifies the value by which the priority decreases when the monitored interface becomes Down.	The value is an integer that ranges from 1 to 255. The priority can decrease to 1. By default, when the monitored interface goes Down, the VRRP6 priority of the device decreases by 10.

Views

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

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

VRRP6 can only detect the status change of the interface on which a VRRP6 group is configured. VRRP6 cannot detect faults on the uplink interface of the master, causing service interruption. You can associate a VRRP6 group with a device

interface that is not in the VRRP6 group. When the monitored interface is faulty, the priority of the master is reduced. This triggers an active/standby switchover and reduces the impact of services on the uplink interface. When the fault is rectified, the original master restores its priority and switches to the master to forward traffic.

Prerequisites

The **vrrp6 vrid virtual-ip** command has been executed on an interface to create a VRRP6 group.

Precautions

After a VRRP6 group is associated with an interface, set **increased** *value-increased* or **reduced** *value-reduced* to an appropriate value. This setting ensures that an active/standby switchover is performed immediately when the monitored interface becomes Down.

NOTE

- The master and backup in the VRRP6 group must work in preemption mode. It is recommended that the preemption delay be 0 on the backup and larger than 0 on the master.
- If the device is the IPv6 address owner (the virtual router IPv6 address is used as the actual interface address), you cannot associate a VRRP6 group with an interface.
- If the IPv4 protocol status on the monitored interface configured with an IPv4 address changes, a new master in the VRRP6 group is selected. If the IPv6 protocol status on the monitored interface configured with an IPv6 address changes, the VRRP6 group remains unchanged.

Example

Associate VRRP6 group 1 with VLANIF 100 and set **reduced** *value-reduced* to 50 when VLANIF 100 becomes Down.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 200
[HUAWEI-Vlanif200] vrrp6 vrid 1 virtual-ip FE80::7 link-local
[HUAWEI-Vlanif200] vrrp6 vrid 1 virtual-ip FC00::2
[HUAWEI-Vlanif200] vrrp6 vrid 1 track interface vlanif 100 reduced 50
```

Associate VRRP6 group 1 with GE0/0/2 and set reduced *value-reduced* to 50 when GE0/0/2 becomes Down.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] vrrp6 vrid 1 virtual-ip FE80::7 link-local
[HUAWEI-GigabitEthernet0/0/1] vrrp6 vrid 1 virtual-ip FC00::2
[HUAWEI-GigabitEthernet0/0/1] vrrp6 vrid 1 track interface gigabitethernet0/0/2 reduced 50
```

12.2.59 vrrp6 vrid virtual-ip

Function

The **vrrp6 vrid virtual-ip** command creates a VRRP6 group and assigns a virtual IPv6 address to the group.

The **undo vrrp6 vrid virtual-ip** command deletes the virtual IPv6 address of a VRRP6 group.

By default, no VRRP6 group is created.

Format

vrrp6 vrid *virtual-router-id* **virtual-ip** *virtual-ipv6-address* [**link-local**]

undo vrrp6 vrid *virtual-router-id* [**virtual-ip** *virtual-ipv6-address* [**link-local**]]

Parameters

Parameter	Description	Value
vrid *virtual-router-id*	Specifies the VRID of a VRRP6 group.	The value is an integer that ranges from 1 to 255.
virtual-ip *virtual-ipv6-address*	Specifies the virtual IPv6 address of a VRRP6 group.	The address is a 32-digit hexadecimal number, in the format X:X:X:X:X:X:X:X.
link-local	Indicates that a link-local address is used as the virtual IPv6 address of a VRRP6 group. The first virtual IPv6 address of a VRRP6 group must be a link-local address.	-

Views

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

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In practice, hosts use the default gateway to communicate with external networks. As value-added services such as IPTV or video conferencing services are widely deployed, hosts may fail to communicate with external networks if the default gateway fails. Configuring dynamic routing protocols such as RIPng, OSPFv3, or ICMPv6 can improve system reliability. However, it is difficult to configure dynamic routing protocols and some hosts may not support dynamic routing protocols. VRRP6 virtualizes multiple routing devices into a virtual router without changing

the networking. The virtual router IPv6 address is configured as the default gateway address.

If users on a network have the same reliability requirements, configure multiple virtual IPv6 addresses for a VRRP6 group. By doing this, one virtual IPv6 address serves one separate user group, and the default gateway address remains consistent regardless of changes in VRRP6 device locations. A VRRP6 group can be assigned a maximum of 16 virtual IPv6 addresses.

Precautions

For VRRP4 or VRRP6 groups configured on a device, each VRID can be bound to a maximum of 16 ports.

If all the virtual IPv6 addresses in a VRRP6 group are deleted, the VRRP6 group is deleted automatically.

NOTE

- The first virtual IPv6 address of a VRRP6 group must be a link-local address. That is, you must run the **vrrp6 vrid** *virtual-router-id* **virtual-ip** *virtual-ipv6-address* **link-local** command before assigning other virtual IPv6 addresses to the VRRP6 group.
- VRRP6 groups must use different virtual IP addresses.
- Two devices in a VRRP6 group must be configured with the same VRID.
- VRRP6 groups on different interfaces of a device can be configured with the same VRID.
- The VLANIF interface of a super VLAN does not support VRRP6.

Example

Configure a VRRP6 group on VLANIF 100 and configure the virtual IPv6 address FE80::7.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] vrrp6 vrid 1 virtual-ip FE80::7 link-local
```

Configure a VRRP6 group on GE0/0/1 and configure the virtual IPv6 address FE80::7.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] vrrp6 vrid 1 virtual-ip FE80::7 link-local
```

12.3 HSB Configuration Commands

12.3.1 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.

12.3.2 bind-service

Function

The **bind-service** command binds an HSB service to an HSB group.

The **undo bind-service** command unbinds the HSB service from the HSB group.

By default, no HSB service is bound to an HSB group.

Format

bind-service *service-index*

undo bind-service *service-index*

Parameters

Parameter	Description	Value
service-index	Specifies the ID of an HSB service.	The value is fixed as 0.

Views

HSB group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

An HSB group synchronizes backup information and responds to link status changes through the HSB channel established by the HSB service. To make the HSB group work properly, bind an HSB service to the HSB group.

Prerequisites

An HSB group has been configured.

Example

Bind HSB service 0 to an HSB group.

```
<HUAWEI> system-view
[HUAWEI] hsb-group 0
[HUAWEI-hsb-group-0] bind-service 0
```


12.3.3 display hsb statistics hsb-group

Function

The **display hsb statistics hsb-group** command displays statistics on processes of an HSB group.

Format

display hsb statistics hsb-group *group-index* **event**

Parameters

Parameter	Description	Value
group-index	Specifies the index of an HSB group.	The fixed value is 0.
event	Indicates process statistics.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The **display hsb statistics hsb-group** command displays statistics on processes. Two main processes are involved: negotiation process and switching process.

Example

Display statistics on processes of the HSB public mechanism.

```
<HUAWEI> display hsb statistics hsb-group 0 event
Hot Standby Statistic Event:
------------------------------------------------------------
Hot Standby Group Dealed Vrrp Group Record:
  Local_Vrrp Peer_Vrrp  Batch_Status Systime
  BACKUP     BACKUP     Ind          2019-8-23 11:55:2
  MASTER     BACKUP     Ind          2019-8-23 11:55:8

Hot Standby Group Event Record:
  Run Independent Event    : 0
  Realtime Sync Event      : 0
  Delete Event(Snd, Recv)  : 0, 0
  Add Event(Snd, Recv)     : 0, 0
  Switch Event(Snd, Recv)  : 0, 0
  Finish Status(Cur, Total): 0, 0

Hot Standby Group Process Record:
```



```
Negotiate Start Entry                : 0
Negotiate Has Started                : 0
Negotiate Start Send Pkt Failed      : 0

Negotiate Req Entry                  : 0
Negotiate Req Failed                 : 0
Negotiate Req Batch Status Error     : 0
Negotiate Req Vrrp Status Error      : 0
Negotiate Req Check Para Failed      : 0
Negotiate Req Notify Event Failed    : 0

Negotiate Del Entry                  : 0
Negotiate Del Batch Status Error     : 0
Negotiate Del Vrrp Status Error      : 0
Negotiate Del Send Pkt Failed        : 0


Negotiate Ack Entry                  : 0
Negotiate Ack Failed                 : 0
Negotiate Ack Batch Status Error     : 0
Negotiate Ack Vrrp Status Error      : 0
Negotiate Ack Notify Event Failed    : 0

Negotiate Add Entry                  : 0
Negotiate Add Batch Status Error     : 0
Negotiate Add Vrrp Status Error      : 0
Negotiate Add Send Pkt Failed        : 0

Negotiate End Entry                  : 0
Negotiate End Failed                 : 0
Negotiate End Batch Status Error     : 0
Negotiate End Vrrp Status Error      : 0
Negotiate End Batch Backup Mid Count : 0

Switch Start Entry                   : 0
Switch Has Started                   : 0
Switch Start Send Pkt Failed         : 0

Switch Req Entry                     : 0
Switch Req Failed                    : 0
Switch Req Batch Status Error        : 0
Switch Req Notify Event Failed       : 0

Switch Switching Entry               : 0
Switch Switching Batch Status Error  : 0
Switch Switching Send Pkt Failed     : 0
Switch Switching Vrrp Changed        : 0
Switch Switching Notify Vrrp Failed  : 0

Switch End Entry                     : 0
Switch End Failed                    : 0
Switch End Batch Status Error        : 0
Switch End Vrrp Changed              : 0
Switch End Notify Vrrp Failed        : 0

HSB Group Vrrp All Master            : 0
HSB Group Vrrp All Backup            : 0
HSB Group Received All Master Event  : 0
HSB Group Received All Backup Event  : 0

HSB Group Notify All Group Event Error: 0
HSB Group Notify One Group Event Error: 0
HSB Group Receive Group Event Error  : 0
HSB Group Vrrp State Change Event    : 2
HSB Group Vrrp State Received Event  : 0
HSB Group Vrrp State Dealed Event    : 0
HSB Group Packet To Task Error       : 0
HSB Group Packet To Task Failed      : 0
```



```
HSB Batch Backup Mid Error Count     : 0
------------------------------------------------------------
```

Table 12-25 Description of the display hsb statistics hsb-group command output

Item	Description
HSB Process/HSB Process ID	ID of an HSB process.
Hot Standby Statistic Event	Statistics about received and handled events of an HSB group.
Hot Standby Group Dealed Vrrp Group Record	Record of the VRRP group of which services are received and processed by the HSB group.
Local_Vrrp	Local VRRP group.
Peer_Vrrp	Remote VRRP group.
Batch_Status	Backup process status.
Systime	System time.
Hot Standby Group Event Record	Record of events notified by the backup service module and received events.
Run Independent Event	Number of events running independently.
Realtime Sync Event	Number of events synchronized in real time.
Delete Event(Snd, Recv)	Number of deleted events that are received or sent.
Add Event(Snd, Recv)	Number of added events that are received or sent.
Switch Event(Snd, Recv)	Number of switched events that are received or sent.
Finish Status(Cur, Total)	Number of current backup services or total number of backup services of which the backup process is complete.
Hot Standby Group Process Record	Statistics on backup processes of the HSB public mechanism.
Negotiate Start Entry	The master device starts to be negotiated.
Negotiate Has Started	Negotiating master and backup devices has started.
Negotiate Start Send Pkt Failed	Sending negotiation packets fails.
Negotiate Req Entry	Batch deletion of backup devices starts.
Negotiate Req Failed	The master device fails to send negotiation-start packets to the backup device.

Item	Description
Negotiate Req Batch Status Error	The backup process status is incorrect. The backup process status of the current backup group is not Independent.
Negotiate Req Vrrp Status Error	The VRRP group status is incorrect and is not Backup.
Negotiate Req Check Para Failed	The backup device checks that some backup parameters from the master device are invalid.
Negotiate Req Notify Event Failed	The backup device notifies that batch deleting backup services fails.
Negotiate Del Entry	Batch deleting firewall services on the backup device is complete.
Negotiate Del Batch Status Error	The backup device fails to check the negotiation process and is not none.
Negotiate Del Vrrp Status Error	The backup device fails to check the VRRP group status and is not Backup.
Negotiate Del Send Pkt Failed	The backup device fails to send batch deletion complete messages to the master device.
Negotiate Ack Entry	Batch backup on the master device starts.
Negotiate Ack Failed	The backup device notifies the master device that the negotiation end message fails to be sent.
Negotiate Ack Batch Status Error	The master device fails to check the negotiation process and is not Batch-Started.
Negotiate Ack Vrrp Status Error	The VRRP group status of the master device is incorrect and is not Master.
Negotiate Ack Notify Event Failed	The master device fails to notify batch backup events on the firewall forwarding plane.
Negotiate Add Entry	The master device receives a message indicating that batch backup on the firewall forwarding plane is complete.
Negotiate Add Batch Status Error	The master device fails to check the negotiation process and is not Batch-Adding.
Negotiate Add Vrrp Status Error	The master device fails to check the VRRP group status and is not Backup.

Item	Description
Negotiate Add Send Pkt Failed	The master device fails to send batch deletion complete messages to the backup device.
Negotiate End Entry	Negotiation ends.
Negotiate End Failed	The master device notifies the backup device that the negotiation end message fails to be sent.
Negotiate End Batch Status Error	The master device fails to check the negotiation process and is not Batch-Adding.
Negotiate End Vrrp Status Error	The VRRP group status is incorrect and is not Master.
Negotiate End Batch Backup Mid Count	Statistics about the services that indicate that batch backup ends and are received by the active device from the standby device.
Switch Start Entry	Switching starts.
Switch Has Started	Switch Has Started.
Switch Start Send Pkt Failed	Sending switching-start messages fails.
Switch Req Entry	The original master device responds to switching messages.
Switch Req Failed	The original backup device fails to initiate switching.
Switch Req Batch Status Error	The original master device fails to check the switching process status and is not Realtime.
Switch Req Notify Event Failed	The original master device fails to notify switching of backup services.
Switch Switching Entry	Switching is complete.
Switch Switching Batch Status Error	The original master device fails to check the switching process status and is not Switching.
Switch Switching Send Pkt Failed	The original backup service fails to send a message indicating that the switching is complete.
Switch Switching Vrrp Changed	During switching, the VRRP status of the original backup device changes.
Switch Switching Notify Vrrp Failed	During switching, the VRRP status of the backup device changes and is not Master. The change is notified to the remote device.
Switch End Entry	Switching ends.

Item	Description
Switch End Failed	The original backup device receives a message indicating the switching failure.
Switch End Batch Status Error	The original master device fails to check the switching process status and is not Switching.
Switch End Vrrp Changed	During switching, the VRRP status of the original backup device changes.
Switch End Notify Vrrp Failed	During switching, the VRRP status of the backup device changes and is not Backup. The change is notified to the remote device.
HSB Group Vrrp All Master	Number of times two master devices exist in a VRRP group.
HSB Group Vrrp All Backup	Number of times two backup devices exist in a VRRP group.
HSB Group Received All Master Event	Number of dual-active events received by the HSB group.
HSB Group Received All Backup Event	Number of dual-standby events received by the HSB group.
HSB Group Notify All Group Event Error	The HSB group fails to notify backup events of all VRRP groups.
HSB Group Notify One Group Event Error	The HSB group fails to notify backup events of a single VRRP group.
HSB Group Receive Group Event Error	The HSB group fails to receive a notification indicating that the backup service is complete.
HSB Group Vrrp State Change Event	VRRP group status change event.
HSB Group Vrrp State Received Event	Number of VRRP status events received by the HSB group.
HSB Group Vrrp State Dealed Event	Number of VRRP status change events processed and responded by the HSB group.
HSB Group Packet To Task Error	An error occurs when the HSB group delivers HSB service packets.
HSB Group Packet To Task Failed	The HSB group fails to deliver HSB service packets.
HSB Batch Backup Mid Error Count	Statistics about the IDs of the services that are processed incorrectly after batch backup ends.

12.3.4 display hsb statistics hsb-service

Function

The **display hsb statistics hsb-service** command displays statistics on packets or processes of the HSB public mechanism.

Format

display hsb statistics hsb-service *service-index* { **event** | **packet** }

Parameters

Parameter	Description	Value
service-index	Specifies the index of an HSB service.	The fixed value is 0.
packet	Indicates packet statistics.	-
event	Indicates process statistics.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The **display hsb statistics hsb-service** command displays statistics on received, sent, and discarded packets or processes of the HSB public mechanism.

Example

Display statistics on packets of the HSB public mechanism.

```
<HUAWEI> display hsb statistics hsb-service 0 packet
Hot Standby Service Packet Statistics:
-------------------------------------------------------------
  Packet Sent     : 0
  Packet Received  : 0
  Packet ID Error : 0
  Packet Sent Dropped    : 0
  Packet Received Dropped : 0
-------------------------------------------------------------
     Group and Group Register Module Packet:
  Group-ID/Module-ID  Packet Sent         Packet Recived
  0                0                 0
  400c0000           0                 0
  -------------------------------------------------------------
```


Display statistics on processes of the HSB public mechanism.

```
<HUAWEI> display hsb statistics hsb-service 0 event
Hot Standby Service Process Record:
-------------------------------------------------------------
  HSB Service Packet To Group Failed    : 0
  HSB Service Packet To Group Error     : 0
  HSB Service Packet To Task Error      : 0
  HSB Service Packet To Outer Error     : 0
  HSB Service Tunnel State Event        : 1
-------------------------------------------------------------
```

Table 12-26 Description of the **display hsb statistics hsb-service** command output

Item	Description
Hot Standby Service Packet Statistics	Statistics on packets of the HSB public mechanism.
Packet Sent	Number of sent packets.
Packet Received	Number of received packets.
Packet ID Error	Packet loss times recorded in PKD ID detection when the HSB receives packets.
Packet Sent Dropped	Number of sent packets that are discarded.
Packet Received Dropped	Number of received packets that are discarded.
Group and Group Register Module Packet	Number of packets of the HSB group or of the module bound to the HSB group.
Group-ID/Module-ID	HSB group ID or module ID.
Hot Standby Service Process Record	Statistics on processes of the HSB public mechanism.
HSB Service Packet To Group Failed	An error occurs when the HSB service delivers HSB service packets to the HSB group.
HSB Service Packet To Group Error	Failure to deliver HSB service packets to the HSB group.
HSB Service Packet To Task Error	Failure to deliver HSB service packets to the backup service.
HSB Service Packet To Outer Error	Failure to deliver HSB service packets to the external module (HSB group or HSB service).
HSB Service Tunnel State Event	HSB service tunnel status event.

12.3.5 display hsb-group

Function

The **display hsb-group** command displays information about an HSB group.

Format

display hsb-group *group-index*

Parameters

Parameter	Description	Value
group-index	Specifies the ID of an HSB group.	The value is 0.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run this command to view information about an HSB group.

Example

Display information about HSB group 0.

```
<HUAWEI> display hsb-group 0
Hot Standby Group Information:
-------------------------------------------------------------
  HSB-group ID                : 0
  Vrrp Group ID               : 2
  Vrrp Interface              : Vlanif100
  Service Index               : 0
  Group Vrrp Status           : Master
  Group Status                : Active
  Group Backup Process        : Realtime
  Backup State                : Ended
  Peer Group Device Name      : -
  Peer Group Software Version : -
  Group Backup Modules        : -
```

Table 12-27 Description of the **display hsb-group** command output

Item	Description
HSB-group ID	ID of an HSB group.

Item	Description
Vrrp Group ID	VRRP group ID.
Vrrp Interface	Interface configured with the VRRP group.
Service Index	HSB service ID.
Group Vrrp Status	Status of the VRRP group: ● Master ● Backup ● Initialize ● None
Group Status	HSB group status: ● Active ● Inactive ● Independent ● Switching
Group Backup Process	Backup process status: ● Independent: independent backup state ● Batch-Started: batch backup negotiation state ● Batch-Deleting: batch deletion state ● Batch-Delete-End: batch deletion end state ● Batch-Adding: batch backup state ● Realtime: real-time backup state ● Switching: switching state
Backup State	Backup status of the HSB group: ● Processing: Backup has been completed for the main core but is still ongoing for the sub core. ● Ended: Backup has been completed for both the main core and sub core. ● -: Backup has not been completed for the main core.
Peer Group Device Name	Device name corresponding to the peer HSB group.
Peer Group Software Version	Software version corresponding to the peer HSB group.

Item	Description
Group Backup Modules	Service module bound to the HSB group.

12.3.6 display hsb-service

Function

The **display hsb-service** command displays information about an HSB service.

Format

display hsb-service *service-index*

Parameters

Parameter	Description	Value
service-index	Specifies the ID of an HSB service.	The value is fixed as 0.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run this command to view information about an HSB service.

Example

Display the HSB service configuration.

```
<HUAWEI> display hsb-service 0
Hot Standby Service Information:
-------------------------------------------------------------
  Local IP Address       : 192.168.4.1
  Peer IP Address        : 192.168.4.2
  Source Port            : 10245
  Destination Port       : 10245
  Keep Alive Times       : 5
  Keep Alive Interval    : 3
  Service State          : Not Valid
  Service Batch Modules  :
  Shared-key             : ******
-------------------------------------------------------------
```


Table 12-28 Description of the **display hsb-service** command output

Item	Description
Local IP Address	IP address of the local device. To set this parameter, run the **service-ip-port** command.
Peer IP Address	IP address of the peer device. To set this parameter, run the **service-ip-port** command.
Source Port	Local port number. To set this parameter, run the **service-ip-port** command.
Destination Port	Destination port number. To set this parameter, run the **service-ip-port** command.
Keep Alive Times	Number of times that heartbeat packets are sent. To set this parameter, run the **service-keep-alive detect** command.
Keep Alive Interval	Interval for sending heartbeat packets. To set this parameter, run the **service-keep-alive detect** command.
Service State	Status of the HSB service: • Connected • Disconnected • Not Valid
Service Batch Modules	Service modules bound to an HSB service.
Shared-key	Key used by the HSB devices. To set this parameter, run the **key** command.

12.3.7 display hsb-resource map

Function

The **display hsb-resource map** command displays HSB resource mapping information.

Format

display hsb-resource map

Parameters

None.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

To view mappings between HSB logical resources and interfaces, run the **display hsb-resource map** command.

Example

Display HSB resource mapping information.

```
<HUAWEI> display hsb-resource map
Hot Standby Backup interface map Information:
HSB-interface           Interface
------------------------------------------------------------
hsb-interface512        Vlanif100
hsb-interface1          GigabitEthernet0/0/1
------------------------------------------------------------
Total number: 2
```

Table 12-29 Description of the **display hsb-resource map** command output

Item	Description
Hot Standby Backup interface map Information	Mapping information of the HSB backup interface.
HSB-interface	HSB logical interface.
Interface	Interface name.
Total number	Total number of interface mappings.

12.3.8 display hsb-service-type dhcp hsb-group

Function

The **display hsb-service-type dhcp hsb-group** command displays information about the HSB group bound to DHCP servers.

Format

display hsb-service-type dhcp hsb-group

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display hsb-service-type dhcp hsb-group** command to view information about the HSB group bound to DHCP servers.

Example

Display information about the HSB group bound to DHCP servers.

```
<HUAWEI> display hsb-service-type dhcp hsb-group
DHCP HSB Group Information:
-------------------------------------------------------------
   DHCP HSB Group : 0
-------------------------------------------------------------
```

Table 12-30 Description of the **display hsb-service-type dhcp hsb-group** command output

Item	Description
DHCP HSB Group	ID of the HSB group.

12.3.9 hsb enable

Function

The **hsb enable** command enables hot standby (HSB) in an HSB group.

The **undo hsb enable** command disables HSB in an HSB group.

By default, HSB is disabled.

Format

hsb enable

undo hsb enable

Parameters

None.

Views

HSB group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

An HSB group takes effect and notifies the service modules of status changes only after the HSB group is enabled. You need to run the **hsb enable** command to enable HSB in an HSB group after the HSB group configuration is complete.

Precautions

Do not run the **undo hsb enable** command when the master and backup devices are performing batch backup.

The master and backup devices must be the same device type and use the same software version. Otherwise, the HSB function may become unavailable.

Example

Enable HSB in HSB group 0.

```
<HUAWEI> system-view
[HUAWEI] hsb-group 0
[HUAWEI-hsb-group-0] hsb enable
```

12.3.10 hsb-group

Function

The **hsb-group** command creates an HSB group.

The **undo hsb-group** command deletes an HSB group.

By default, no HSB group is created.

Format

hsb-group *group-index*

undo hsb-group *group-index*

Parameters

Parameter	Description	Value
group-index	Specifies the ID of an HSB group.	The value is fixed as 0.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To configure HSB functions, create an HSB group first. An HSB group instructs service modules to perform batch backup, real-time backup, and status synchronization. An HSB group supports status negotiation and event notification functions, implementing service synchronization on master and backup devices.

Precautions

After HSB is enabled for an HSB group, an HSB service cannot be bound to the HSB group.

Example

Create HSB group 0.

```
<HUAWEI> system-view
[HUAWEI] hsb-group 0
[HUAWEI-hsb-group-0]
```

12.3.11 hsb-resource map

Function

The **hsb-resource map** command configures HSB resource mapping information.

The **undo hsb-resource map** command deletes HSB resource mapping information.

By default, no HSB resource mapping is configured.

Format

hsb-resource map interface *interface-type interface-number* **hsb-interface** *hsb-interface-number*

undo hsb-resource map interface *interface-type interface-number* **hsb-interface** *hsb-interface-number*

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Specifies the type and number of an interface: • *interface-type* specifies the interface type. • *interface-number* specifies the interface number.	-
hsb-interface *hsb-interface-number*	Specifies the index of an HSB logical interface.	The value is an integer in the range from 1 to 512.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

If the interface types and numbers on the active and standby devices are different, the standby device cannot back up interface-related entry information of the active device by default. As a result, services are interrupted after an active/standby switchover. To solve this problem, run the **hsb-resource map** command on the active and standby devices to configure mappings between interfaces and HSB logical interfaces. The configuration will map interfaces of the active and standby devices to the same HSB logical interface so that the standby device can back up interface-related entry information of the active device based on the mappings.

Example

Configure mappings between interfaces and a specific HSB logical interface.

```
<HUAWEI> system-view
[HUAWEI] hsb-resource map interface vlanif 10 hsb-interface 1
```

12.3.12 hsb-service

Function

The **hsb-service** command creates an HSB service and displays the HSB service view.

The **undo hsb-service** command deletes an HSB service.

By default, no HSB service is created.

Format

hsb-service *service-index*

undo hsb-service *service-index*

Parameters

Parameter	Description	Value
service-index	Specifies the ID of an HSB service.	The fixed value is 0.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

An HSB service establishes an HSB channel for transmitting packets of other services and maintains the link status by notifying the HSB group of the faulty link. Only after an HSB group is bound to an HSB service, the HSB function can be implemented.

Example

Create HSB service 0.

```
<HUAWEI> system-view
[HUAWEI] hsb-service 0
[HUAWEI-hsb-service-0]
```

12.3.13 hsb-service-type dhcp hsb-group

Function

The **hsb-service-type dhcp hsb-group** command binds DHCP services to an HSB group.

The **undo hsb-service-type dhcp hsb-group** command unbinds DHCP services from an HSB group.

By default, DHCP services are not bound to an HSB group.

Format

hsb-service-type dhcp hsb-group *group-index*

undo hsb-service-type dhcp hsb-group *group-index*

Parameters

Parameter	Description	Value
group-index	Specifies the index of an HSB group.	The value is 0.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In a DHCPv6 prefix delegation (PD) scenario, to ensure reachable routes between the DHCPv6 relay agent and terminals, you need to run the **hsb-service-type dhcp hsb-group** command to bind DHCP services to a specific HSB group. This configuration ensures that prefix routing information on the DHCPv6 relay agent can be backed up by the HSB group.

Prerequisites

An HSB group has been created using the **hsb-group** command.

Precautions

Services can be bound to an HSB group only before the HSB group is enabled.

This command applies only to the DHCPv6 PD scenario and must be configured on the DHCPv6 relay agent.

Example

Bind DHCP services to an HSB group.

```
<HUAWEI> system-view
[HUAWEI] hsb-group 0
[HUAWEI-hsb-group-0] quit
[HUAWEI] hsb-service-type dhcp hsb-group 0
```

12.3.14 key

Function

The **key** command configures the key used by the HSB devices.

The **undo key** command deletes the key used by the HSB devices.

By default, the key used by HSB devices is not configured.

Format

key cipher *key-string*

undo key

Parameters

Parameter	Description	Value
cipher *key-string*	Indicates the key used by the HSB devices.	The value can be a string of 48 characters in cipher text or a string of 8 to 16 characters in plain text.

Views

HSB service view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To ensure security of HSB information negotiation and service backup and prevent the attacks initiated by using bogus packets or modifying packets, run the **key** command to configure the key used by HSB devices. The key provides authentication and verification mechanisms.

Precautions

- Configuring a shared key for HSB devices is not recommended in a secure network environment, as this configuration will degrade the HSB performance.
- The **key** command must be configured before the **service-ip-port** command. Otherwise, the **key** configuration will fail.
- The two HSB devices must be configured with the same shared key. Inconsistent keys on two ends will cause frequent interruption of the HSB channel.

Example

Set the key used by HSB devices to **YsHsjx_202206**.

```
<HUAWEI> system-view
[HUAWEI] hsb-service 0
[HUAWEI-hsb-service-0] key cipher YsHsjx_202206
```


12.3.15 reset hsb statistics hsb-group

Function

The **reset hsb statistics hsb-group** command clears statistics on HSB processes.

Format

reset hsb statistics hsb-group *group-index* **event**

Parameters

Parameter	Description	Value
group-index	Specifies the index of an HSB group.	The value is fixed as 0.
event	Indicates process statistics.	-

Views

User view

Default Level

3: Management level

Usage Guidelines

Before collecting HSB statistics within a certain period, run this command to clear the existing HSB statistics. You can run this command to clear statistics about HSB processes. Two main processes are involved: HSB negotiation process and HSB switching process.

Example

Clear statistics about HSB processes.

```
<HUAWEI> reset hsb statistics hsb-group 0 event
```

12.3.16 reset hsb statistics hsb-service

Function

The **reset hsb statistics hsb-service** command clears statistics on packets or processes of the HSB public mechanism.

Format

reset hsb statistics hsb-service *service-index* { **packet** | **event** }

Parameters

Parameter	Description	Value
service-index	Specifies the index of an HSB service.	The value is fixed as 0.
packet	Indicates packet statistics.	-
event	Indicates process statistics.	-

Views

User view

Default Level

3: Management level

Usage Guidelines

Before collecting HSB statistics within a certain period, run this command to clear the existing HSB statistics. You can run this command to clear statistics on packets or processes of the HSB public mechanism.

Example

Clear statistics on packets of the HSB public mechanism.

```
<HUAWEI> reset hsb statistics hsb-service 0 packet
```

Clear statistics on processes of the HSB public mechanism.

```
<HUAWEI> reset hsb statistics hsb-service 0 event
```

12.3.17 service-ip-port

Function

The **service-ip-port** command configures the IP address and port number of an HSB channel.

The **undo service-ip-port** command deletes the IP address and port number of an HSB channel.

By default, the IP address and port number of an HSB channel are not configured.

Format

service-ip-port local-ip { *local-ipv4-address* | *local-ipv6-address* } **peer-ip** { *peer-ipv4-address* | *peer-ipv6-address* } **local-data-port** *local-port* **peer-data-port** *peer-port*

undo service-ip-port local-ip { *local-ipv4-address* | *local-ipv6-address* } **peer-ip** { *peer-ipv4-address* | *peer-ipv6-address* } **local-data-port** *local-port* **peer-data-port** *peer-port*

Parameters

Parameter	Description	Value
local-ip { *local-ipv4-address* | *local-ipv6-address* }	Specifies the local IPv4 or IPv6 address of the HSB service.	• *local-ipv4-address*: The value is in dotted decimal notation. • *local-ipv6-address*: The value is a 32-digit hexadecimal number, in the format X:X:X:X:X:X:X:X.
peer-ip { *peer-ipv4-address* | *peer-ipv6-address* }	Specifies the peer IPv4 or IPv6 address of the HSB service.	• *peer-ipv4-address*: The value is in dotted decimal notation. • *peer-ipv6-address*: The value is a 32-digit hexadecimal number, in the format X:X:X:X:X:X:X:X.
local-data-port *local-port*	Specifies the local port number of the HSB service.	The value is an integer that ranges from 10240 to 49152.
peer-data-port *peer-port*	Specifies the peer port number of the HSB service.	The value is an integer that ranges from 10240 to 49152.

Views

HSB service view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After you create an HSB service using the **hsb-service** command, run the **service-ip-port** command to configure IP addresses and port numbers for the local and peer devices. When the configuration is complete, the HSB service establishes a Transmission Control Protocol (TCP) channel to transmit packets of other services and notifies service modules of link status changes.

Prerequisites

An HSB service has been created.

Precautions

It is recommended that the HSB channel be configured on an independent and highly reliable physical link.

If the command configuration fails to be restored, you cannot view the unrestored configuration information. In this case, you are advised to check whether the port is occupied by other services.

Example

Configure IP addresses and port numbers for the local and peer devices for the HSB service 0.

```
<HUAWEI> system-view
[HUAWEI] hsb-service 0
[HUAWEI-hsb-service-0] service-ip-port local-ip 192.168.1.1 peer-ip 192.168.1.2 local-data-port 10240 peer-data-port 10240
```

12.3.18 service-keep-alive detect

Function

The **service-keep-alive detect** command sets the retransmission times and interval of HSB packets.

The **undo service-keep-alive** command restores the default retransmission times and interval of HSB packets.

The default retransmission times is 5, and the default retransmission interval is 3 seconds.

Format

service-keep-alive detect retransmit *retransmit-times* **interval** *interval-value*

undo service-keep-alive [**detect retransmit** *retransmit-times* **interval** *interval-value*]

Parameters

Parameter	Description	Value
retransmit *retransmit-times*	Specifies the retransmission times of HSB packets.	The value is an integer that ranges from 1 to 20.
interval *interval-value*	Specifies the retransmission interval of HSB packets.	The value is an integer that ranges from 1 to 10, in seconds.

Views

HSB service view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

An HSB service sends and retransmits HSB packets to prevent long TCP interruption that is not detected by the protocol stack. If a device does not receive an HSB packet from the peer device within the period (value of *retransmit-times* x value of *interval-value*), the local device receives a message indicating the exception and then re-establishes a channel to the peer.

Prerequisites

An HSB service has been configured.

Precautions

It is recommended that the product of the retransmission times of HSB packets multiplied by the retransmission interval of HSB packets be greater than or equal to the value of **Master_Down_Interval**. The value of **Master_Down_Interval** is calculated using the following formula: Master_Down_Interval = 3 x Advertisement_Interval + Skew_time, in seconds. For details, see **vrrp vrid timer advertise** and **vrrp6 vrid timer advertise**. It is recommended that the retransmission times and retransmission interval of HSB packets be set to their default values.

Example

Set the retransmission times of HSB service 0 to 5, and the retransmission interval to 1 second.

```
<HUAWEI> system-view
[HUAWEI] hsb-service 0
[HUAWEI-hsb-service-0] service-keep-alive detect retransmit 5 interval 1
```

12.3.19 track vrrp

Function

The **track vrrp** command binds an IPv4 VRRP group to an HSB group.

The **undo track vrrp** command unbinds an IPv4 VRRP group from an HSB group.

By default, no HSB group is bound to an IPv4 VRRP group.

Format

track vrrp vrid *virtual-router-id* **interface** *interface-type interface-number*

undo track vrrp [**vrid** *virtual-router-id* **interface** *interface-type interface-number*]

Parameters

Parameter	Description	Value
vrid *virtual-router-id*	Specifies the ID of an IPv4 VRRP group bound to an HSB group.	The value is an integer that ranges from 1 to 255.
interface *interface-type interface-number*	Specifies the type and number of the interface in an IPv4 VRRP group. • *interface-type* specifies the interface type. • *interface-number* specifies the interface number.	-

Views

HSB group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can run the **track vrrp** command to bind a VRRP group to an HSB group. The HSB group negotiates the service status based on the VRRP status. By monitoring the changes in the bound HSB channel status and VRRP status, the HSB group instructs service modules to perform batch backup, real-time backup, and status synchronization.

Prerequisites

An HSB group has been configured.

Example

Bind VLANIF100 in IPv4 VRRP group 4 to HSB group 0.

```
<HUAWEI> system-view
[HUAWEI] hsb-group 0
[HUAWEI-hsb-group-0] track vrrp vrid 4 interface vlanif 100
```


12.3.20 track vrrp6

Function

The **track vrrp6** command binds an IPv6 VRRP group to an HSB group.

The **undo track vrrp6** command unbinds the IPv6 VRRP group from the HSB group.

By default, no IPv6 VRRP group is bound to an HSB group.

Format

track vrrp6 vrid *virtual-router-id* **interface** *interface-type interface-number*

undo track vrrp6 [**vrid** *virtual-router-id* **interface** *interface-type interface-number*]

Parameters

Parameter	Description	Value
vrid *virtual-router-id*	Specifies the ID of an IPv6 VRRP group bound to an HSB group.	The value is an integer that ranges from 1 to 255.
interface *interface-type interface-number*	Specifies the type and number of the interface in an IPv6 VRRP group. • *interface-type* specifies the interface type. • *interface-number* specifies the interface number.	-

Views

HSB group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the HSB service is used, you need to run this command to bind a VRRP group to an HSB group. The HSB group negotiates the service status based on the VRRP status. By monitoring the changes in the bound HSB channel status and

VRRP status, the HSB group instructs service modules to perform batch backup, real-time backup, and status synchronization.

Prerequisites

An HSB group has been configured.

Example

Bind IPv6 VRRP group 4 on VLANIF100 to HSB group 0.

```
<HUAWEI> system-view
[HUAWEI] hsb-group 0
[HUAWEI-hsb-group-0] track vrrp6 vrid 4 interface vlanif 100
```

12.4 DLDP Configuration Commands

12.4.1 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.

12.4.2 display dldp

Function

The **display dldp** command displays the DLDP status of an interface or global DLDP status.

Format

display dldp [**interface** *interface-type interface-number*]

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Displays DLDP status of a specified interface. • *interface-type* specifies the interface type. • *interface-number* specifies the interface number.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

You can use the **display dldp** command to view the DLDP status on the device.

Prerequisites

DLDP has been enabled globally using the **dldp enable** command.

DLDP has been enabled in the interface view using the **dldp enable** command.

Precaution

You can run the **display dldp** command to view DLDP status only after enabling DLDP globally using the **dldp enable** command.

Example

Display the DLDP status on the device.

```
<HUAWEI> display dldp
DLDP global status: enable
DLDP interval: 10s
DLDP work-mode: enhance
DLDP authentication-mode: sha, password is ******
DLDP unidirectional-shutdown: auto
DLDP delaydown-timer: 4s
The number of enabled ports is: 1
The number of global neighbors is: 1
The max number of global neighbors is: 512
Interface GigabitEthernet0/0/1
 DLDP port state: advertisement
 DLDP link state: up
 The neighbor number of the port is: 1.
   Neighbor mac address:80fb-0636-792d
   Neighbor port index:49
   Neighbor state:two way
   Neighbor aged time(s):16
```

Display the DLDP status on GE0/0/1.

```
<HUAWEI> display dldp interface gigabitethernet 0/0/1
Interface GigabitEthernet0/0/1
 DLDP port state: advertisement
 DLDP link state: up
 The neighbor number of the port is: 1.
   Neighbor mac address:0001-0001-0001
   Neighbor port index:26
   Neighbor state:two way
   Neighbor aged time(s):206
```


Table 12-31 Description of the display dldp command output

Item	Description
DLDP global status	Global DLDP status. The value can be: ● enable: DLDP is enabled. ● disable: DLDP is disabled. To enable DLDP, use the **dldp enable** command.
DLDP interval	Interval for sending the Advertisement packets, in seconds. To set the interval, use the **dldp interval** command.
DLDP work-mode	Working mode of DLDP. The value can be: ● enhance ● normal To set the working mode of DLDP, use the **dldp work-mode** command.
DLDP authentication-mode	Authentication mode of DLDP packets. The value can be: ● none: DLDP packets are not authenticated. ● simple: DLDP packets are authenticated using plain-text passwords. ● md5: DLDP packets are authenticated using MD5. ● sha: DLDP packets are authenticated using SHA2-256. To set DLDP authentication mode, use the **dldp authentication-mode** command.
DLDP unidirectional-shutdown	Interface shutdown mode. The value can be: ● manual: Interfaces are manually shut down. ● auto: Interfaces are automatically shut down. To set the interface shutdown mode, use the **dldp unidirectional-shutdown** command.

Item	Description
DLDP delaydown-timer	Delay of an interface's response to a Port-Down event, in seconds. To set the delay, use the **dldp delaydown-timer** command.
The number of enabled ports is	Number of interfaces on which DLDP is enabled on a device.
The number of global neighbors is	Number of DLDP neighbors.
The max number of global neighbors is	The max number of global DLDP neighbors.

Item	Description
DLDP port state	Current DLDP status of an interface. The value can be: ● inactive: DLDP is enabled but the link is Down. ● active: DLDP is enabled and the link is Up, or entries of neighbors have been cleared. ● advertisement: All neighbors have established bidirectional connections or have been in Active state for at least 5 seconds. The link in this state is stable. ● probe: The interface receives a packet from an unknown neighbor. The interface then sends a probe packet to check whether the link is a unidirectional link. When an interface enters this state, DLDP starts the probe timer and starts an echo timer for each neighbor to be detected. ● disable: DLDP detects a unidirectional link or a neighbor disappears when DLDP works in enhanced mode. An interface in this state receives and forwards only BPDUs, not user traffic. ● delaydown: When DLDP is in Active, Advertisement, or Probe state, it has not entered the Inactive state when receiving a Port-Down event. An interface in delaydown state retains the DLDP neighbor information and starts the DelayDown timer. ● loop: Indicates that a loop occurs on the interface because the Rx and Tx of an optical module are connected by the same optical fiber.
DLDP link state	Status of the interface. ● up ● down
The neighbor number of the port	Number of neighbors of an interface.
Neighbor mac address	MAC address of a peer device.

Item	Description
Neighbor port index	Index of a peer port.
Neighbor state	Peer status. • unknown • one way • two way
Neighbor aged time(s)	Time period after which a peer ages, in seconds.

12.4.3 display dldp statistics

Function

The **display dldp statistics** command displays the statistics about DLDP packets on an interface.

Format

display dldp statistics [**interface** *interface-type interface-number*]

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Displays the statistics about DLDP packets on a specified DLDP interface. • *interface-type* specifies the interface type. • *interface-number* specifies the interface number. If no interface is specified, the statistics about DLDP packets on all DLDP interfaces are displayed. If an interface is specified, the statistics about DLDP packets on the specified interface are displayed.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

If DLDP negotiation fails, you can use the **display dldp statistics** command to check the statistics about DLDP packets. This command can be used to display the statistics about DLDP packets after the statistics about DLDP packets are cleared using the **reset dldp statistics** command.

Prerequisites

DLDP has been enabled globally and on interfaces using the **dldp enable** command.

Example

Display the statistics about DLDP packets on the device.

```
<HUAWEI> display dldp statistics
Interface : GigabitEthernet0/0/1
 Packets sent: 15
 Packets received: 0
 Invalid packets received: 0
 Loop packets received: 0
 Authentication failed packets received: 0
 Valid packets received: 0
```

Display the statistics about DLDP packets on GE0/0/1.

```
<HUAWEI> display dldp statistics interface gigabitethernet 0/0/1
Interface : GigabitEthernet0/0/1
 Packets sent: 0
 Packets received: 0
 Invalid packets received: 0
 Loop packets received: 0
 Authentication failed packets received: 0
 Valid packets received: 0
```

Table 12-32 Description of the **display dldp statistics** command output

Item	Description
Interface	Name of the port on which DLDP is enabled.
Packets sent	Number of DLDP sent packets.
Packets received	Number of DLDP received packets.
Invalid packets received	Number of DLDP erroneous packets that are received.

Item	Description
Loop packets received	Number of DLDP loop packets that are received.
Authentication failed packets received	Number of DLDP received packets that fail to pass the authentication.
Valid packets received	Number of DLDP valid packets that are received.

12.4.4 dldp authentication-mode

Function

The **dldp authentication-mode** command configures a DLDP authentication mode.

The **undo dldp authentication-mode** command restores the default DLDP authentication mode.

By default, DLDP packets are not authenticated.

Format

dldp authentication-mode { **md5** *md5-password* | **simple** *simple-password* | **sha** *sha-password* | **none** }

undo dldp authentication-mode [**md5** *md5-password* | **simple** *simple-password* | **sha** *sha-password* | **none**]

Parameters

Parameter	Description	Value
md5 *md5-password*	Uses MD5 to authenticate DLDP packets exchanged between the interfaces on the local and neighbor devices. *md5-password* specifies the MD5 authentication password. **NOTE** The password is saved in the configuration file in cipher text for security.	The value is a string of 6 to 16 case-sensitive characters in plain text and consists of at least two of the following: lowercase letters, uppercase letters, digits, and special characters excluding question marks (?) and spaces. **NOTE** Ciphertext passwords with various lengths configured in an earlier version are also supported in the existing version.

Parameter	Description	Value
simple *simple-password*	Uses the plain text to authenticate DLDP packets exchanged between the interfaces on the local and neighbor devices. *simple-password* specifies the plain-text authentication password. **NOTE** The password is saved in the configuration file in cipher text for security.	The value is a string of 6 to 16 case-sensitive characters in plain text and consists of at least two of the following: lowercase letters, uppercase letters, digits, and special characters excluding question marks (?) and spaces. **NOTE** Ciphertext passwords with various lengths configured in an earlier version are also supported in the existing version.
none	Performs no authentication on DLDP packets exchanged between the interfaces on the local and neighbor devices.	-
sha *sha-password*	Uses SHA2-256 mode to authenticate DLDP packets exchanged between the interfaces on the local and neighbor devices. *sha-password* specifies the SHA2-256 authentication password. **NOTE** The password is saved in the configuration file in cipher text for security.	The value is a string of 6 to 16 case-sensitive characters in plain text and consists of at least two of the following: lowercase letters, uppercase letters, digits, and special characters excluding question marks (?) and spaces. **NOTE** Ciphertext passwords with various lengths configured in an earlier version are also supported in the existing version.

NOTE

For security purposes, you are advised to use SHA2-256 as the authentication algorithm of DLDP.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To ensure packet validity on an insecure network, users can configure one of the following authentication modes for DLDP packets:

- None: The sender sets the authentication key of the DLDP packets to all 0s and the authentication type field to 0. The receiver compares the authentication key and authentication type with those set on the local end. If the settings on the two ends are different, the receiver discards the DLDP packets.
- Plain text: The sender sets the authentication key of the DLDP packets to the plain-text password set on the local end and the authentication type field to 1. The receiver compares the authentication key and authentication type with those set on the local end. If the settings on the two ends are different, the receiver discards the DLDP packets.
- MD5: The sender sets the authentication key of the DLDP packets to the summary of the cipher text obtained from the password set on the local end using the MD5 algorithm, and sets the authentication type field to 2. The receiver compares the authentication key and authentication type with the summary of the cipher text obtained on the local end using the MD5 algorithm. If the settings on the two ends are different, the receiver discards the DLDP packets.
- SHA2-256 authentication: The sender sets the authenticator field of the DLDP packets to the digest of the cipher text obtained from the password set on the local end using the SHA2-256 algorithm, and sets the authentication type field to 3. The receiver compares the authenticator and authentication type with the digest of the cipher text obtained on the local end using the SHA2-256 algorithm. If the settings on the two ends are different, the receiver discards the DLDP packets.

When the device that uses MD5 authentication is upgraded from V200R001 or V200R002 to V200R008 or later, to ensure compatibility, upgrade the DLDP authentication mode to MD5-compatible. You can run the **undo dldp authentication-mode md5-compatible** command to cancel MD5-compatible authentication.

Prerequisites

DLDP has been enabled globally using the **dldp enable** command.

Precautions

If the **dldp authentication-mode** command is executed while DLDP is running, the local device deletes information about the DLDP neighbor device and triggers the neighbor device to clear information about the local device. In this way, the negotiation can be re-performed.

If the DLDP authentication mode is set, ensure that the local and neighbor devices are configured with the same DLDP authentication mode and password. If they

use different DLDP authentication modes or passwords, DLDP packets cannot be authenticated. DLDP can work properly only when the two interfaces are authenticated.

Example

Configure simple authentication for DLDP packets exchanged between two devices. Set the SHA2-256 password to YsHsjx_202206.

```
<HUAWEI> system-view
[HUAWEI] dldp authentication-mode sha YsHsjx_202206
```

12.4.5 dldp compatible-mode enable

Function

The **dldp compatible-mode enable** command enables the DLDP compatible mode.

The **undo dldp compatible-mode enable** command disables the DLDP compatible mode.

By default, the DLDP compatible mode is disabled.

Format

dldp compatible-mode enable

undo dldp compatible-mode enable

Parameters

None

Views

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

This configuration is required if the device works with the following Huawei switches to provide the DLDP function:

- S8500
- S7800
- S6500
- S5600 series

- S5100-EI
- S3900 series
- S3500 series
- S3100 series

Prerequisites

DLDP has been enabled globally using the **dldp enable** command.

Precautions

If two devices are connected by two cross-connected links, the DLDP compatible mode must be enabled or disabled on both the two interfaces.

If two devices are Huawei devices (not preceding models), the DLDP compatible mode must be enabled or disabled on both the two interfaces.

Example

Enable the DLDP compatible mode on interfaceGE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] dldp enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] dldp enable
[HUAWEI-GigabitEthernet0/0/1] dldp compatible-mode enable
```

12.4.6 dldp compatible-mode local-mac

Function

The **dldp compatible-mode local-mac** command configures the switch to send DLDP packets containing source MAC addresses in the DLDP compatible mode.

The **undo dldp compatible-mode local-mac** command restores the source MAC addresses of the DLDP packets to the default MAC address.

By default, the MAC address of a DLDP packet is the system MAC address.

Format

dldp compatible-mode local-mac *mac-address*

undo dldp compatible-mode local-mac [*mac-address*]

Parameters

Parameter	Description	Value
mac-address	Specifies the source MAC address of the DLDP packets sent in the DLDP compatible mode.	The value is in H-H-H format. H contains 1 to 4 hexadecimal digits. **NOTE** The source MAC address cannot be a multicast MAC address, a broadcast MAC address, or a reserved address.

Views

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

You can run **dldp compatible-mode local-mac** command to configure the source MAC addresses for DLDP packets sent in DLDP compatible mode. This prevents the DLDP flapping due to discovery of multiple neighbors when the device needs to work with the following Huawei switches:

- S8500
- S7800
- S6500
- S5600 series switches
- S5100-EI
- S3900 series switches
- S3500 series switches
- S3100 series switches

Prerequisites

The DLDP compatible mode has been enabled using the **dldp compatible-mode enable** command.

Precautions

When the configuration is complete, the newly configured MAC address is used as the source MAC addresses of the sent DLDP packets.

Example

Set the source MAC address of the DLDP packets sent by interface GE0/0/1 in DLDP compatible mode to 00e0-fc12-0011.

```
<HUAWEI> system-view
[HUAWEI] dldp enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] dldp enable
[HUAWEI-GigabitEthernet0/0/1] dldp compatible-mode enable
[HUAWEI-GigabitEthernet0/0/1] dldp compatible-mode local-mac 00e0-fc12-0011
```

12.4.7 dldp delaydown-timer

Function

The **dldp delaydown-timer** command sets the timeout value of the DelayDown timer.

The **undo dldp delaydown-timer** command restores the default timeout value of the DelayDown timer.

The default timeout value of the DelayDown timer is 1 second.

Format

dldp delaydown-timer *time*

undo dldp delaydown-timer [*time*]

Parameters

Parameter	Description	Value
time	Specifies the timeout value of the DelayDown timer.	The value is an integer ranging from 1 to 5, in seconds.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If a DLDP interface in Active, Advertisement, or Probe state receives a Port-Down event, the interface enters Inactive state and clears the neighbor information. In some cases, the interface is Down for a short time. For example, failure of the Tx fiber on a port may cause jitter of optical signals on the Rx fiber, which makes the

port Down and then Up again. To prevent the neighbor information from being deleted immediately in this case, the DLDP interface first enters the DelayDown state and starts the DelayDown timer. Before the DelayDown timer times out, the interface retains the neighbor information and responds to only Port-Up events. You can use the **dldp delaydown-timer** command to set the timeout value of the DelayDown timer.

- If the DLDP interface does not receive any Port-Up event when the DelayDown timer times out, the interface deletes the neighbor entry and enters the Inactive state.
- If the DLDP interface receives the Port-Up event before the DelayDown timer times out, the interface returns to the previous state.

Prerequisites

DLDP has been enabled globally using the **dldp enable** command.

Precautions

After the **dldp delaydown-timer** command is executed, the DLDP status is not affected by the Up/Down jitter within the timeout value of the DelayDown timer.

Example

Set the timeout value of the DelayDown timer to 2 seconds.

```
<HUAWEI> system-view
[HUAWEI] dldp enable
[HUAWEI] dldp delaydown-timer 2
```

12.4.8 dldp enable

Function

The **dldp enable** command enables DLDP.

The **undo dldp enable** command disables DLDP.

By default, DLDP is disabled globally and on each interface.

Format

dldp enable

undo dldp enable

Parameters

None

Views

System 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

Sometimes unidirectional links occur on networks. On a unidirectional link, the local device can receive packets from the peer device at the link layer, but the peer device cannot receive packets from the local device. Unidirectional links result in problems such as loops on an STP topology.

DLDP is used to monitor the link status of optical fibers or copper twisted pairs. If a unidirectional link exists, DLDP automatically shuts down the interface or prompts users to manually shut down the interface to prevent network faults.

To enable DLDP, run the **dldp enable** command to globally enable DLDP and then run this command on the interface.

Prerequisites

DLDP takes effect only when the physical link is connected; therefore, securely connect optical fibers or copper twisted pairs before enabling DLDP.

Precautions

- After you enable DLDP using the **dldp enable** command in the system view, run this command again on the interfaces to enable DLDP so that the interfaces can properly transmit and receive DLDP packets.
- If DLDP is disabled in the system view, DLDP is disabled on all interfaces, and all the DLDP configurations are deleted, which cannot be restored.
- Unidirectional links can be detected only for GE optical modules.

Example

Enable DLDP globally.

```
<HUAWEI> system-view
[HUAWEI] dldp enable
```

Enable DLDP on interface GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] dldp enable
```

12.4.9 dldp interval

Function

The **dldp interval** command sets the interval for sending Advertisement packets.

The **undo dldp interval** command restores the default interval for sending Advertisement packets.

The default interval for sending Advertisement packets is 5 seconds.

Format

dldp interval *interval*

undo dldp interval [*interval*]

Parameters

Parameter	Description	Value
interval	Specifies the interval for sending Advertisement packets.	The value is an integer ranging from 1 to 100, in seconds.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Applicable Environment

An interface in Advertisement state sends Advertisement packets. DLDP creates a neighbor entry, starts the entry timer, and transits to the Probe state if the neighbor entry does not exist on the peer interface. DLDP updates the entry timer if the neighbor entry exists.

You can adjust the interval for sending Advertisement packets to allow DLDP to detect unidirectional links on different networks.

The interval for sending Advertisement packets must be smaller than one third of the STP convergence time.

- If the interval is too long, STP loops occur before a unidirectional link is shut down on a DLDP interface, which may lead to forwarding of many error packets.
- If the interval is too short, the traffic volume on the network increases.

Prerequisites

DLDP has been enabled globally using the **dldp enable** command.

Precautions

After the **dldp interval** command is executed, the local device running DLDP deletes information about the peer device and triggers the peer device to clear information about the local device. In this way, the negotiation can be re-performed.

Ensure that the interval for sending Advertisement packets is set to the same value on the local and peer devices connected through optical fibers or copper twisted pairs.

Example

Set the interval for sending Advertisement packets to 20 seconds on all DLDP interfaces.

```
<HUAWEI> system-view
[HUAWEI] dldp enable
[HUAWEI] dldp interval 20
```

12.4.10 dldp reset

Function

The **dldp reset** command resets the DLDP status of an interface so that the interface re-detects unidirectional links.

Format

dldp reset

Parameters

None

Views

System 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

When a unidirectional link is detected, the corresponding interface enters the Disable state. The system prompts you to shut down the interface or automatically sets the interface state to DLDP Down according to the configuration. To enable the interface to detect unidirectional links again, you can reset the DLDP status of the interface as follows:

- If the interface is shut down using the **shutdown (interface view)** command, run the **undo shutdown (interface view)** command to enable the interface to detect unidirectional links again. If the system automatically sets the interface state to DLDP Down, wait the interface to recover using the auto recovery mechanism after the link state becomes bidirectional using the auto recovery mechanism.

- Run the **dldp reset** command to restore the interface. The DLDP status of the interface after recovery depends on the physical status of the port. If the physical status is Down, the DLDP status of the interface changes to Inactive. If the physical status is Up, the DLDP status changes to Active.

You can reset the DLDP status globally or on the interfaces.

- When you run the **dldp reset** command in the interface view, the command takes effect only on this interface.
- When you run the **dldp reset** command in the system view, the command takes effect on all disabled interfaces.

Prerequisites

- If you run this command in the system view, ensure that DLDP has been enabled globally using the **dldp enable** command.
- If you run this command in the interface view, ensure that DLDP has been enabled globally and on the interfaces using the **dldp enable** command.

Example

Reset the DLDP status of all disabled interfaces.

```
<HUAWEI> system-view
[HUAWEI] dldp reset
```

Reset the DLDP status of disabled interfaceGE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] dldp reset
```

12.4.11 dldp unidirectional-shutdown

Function

The **dldp unidirectional-shutdown** command sets the shutdown mode if DLDP detects a unidirectional link on an interface.

The **undo dldp unidirectional-shutdown** command restores the default shutdown mode if DLDP detects a unidirectional link on an interface.

By default, an interface is shut down automatically if DLDP detects a unidirectional link on the interface.

Format

dldp unidirectional-shutdown { **auto** | **manual** }

undo dldp unidirectional-shutdown [**auto** | **manual**]

Parameters

Parameter	Description	Value
auto	Specifies the automatic mode.	-

Parameter	Description	Value
manual	Specifies the manual mode. When the traffic is heavy or CPU usage is high, the manual shutdown mode is recommended.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When DLDP detects a unidirectional link on an interface, run the **dldp unidirectional-shutdown** command to configure the shutdown mode for the interface. The following shutdown modes are available:

- Manual mode: This mode can prevent DLDP from shutting down the port immediately when the network performance is poor. This leads to failure in packet forwarding. It is a compromise mode used to prevent interface shutdown due to incorrect judgment of the system. In this mode, DLDP detects unidirectional links, and the network administrator manually shuts down the interface. When the DLDP state machine detects a unidirectional link, the system sends trap messages to prompt the network administrator to shut down the interface. Then the DLDP state machine changes to the Disable state.
- Automatic mode: It is the default mode. When a unidirectional link is detected, the DLDP state machine changes to the Disable state, records the trap messages, and sets the interface status to Blocking.

Prerequisites

DLDP has been enabled globally using the **dldp enable** command.

Precautions

When the traffic is heavy or CPU usage is high, the manual shutdown mode is recommended.

Example

Configure DLDP to automatically shut down an interface when a unidirectional link is detected.


```
<HUAWEI> system-view
[HUAWEI] dldp enable
[HUAWEI] dldp unidirectional-shutdown auto
```

12.4.12 dldp work-mode

Function

The **dldp work-mode** command sets the working mode of DLDP.

The **undo dldp work-mode** command restores the default working mode of DLDP.

By default, the working mode of DLDP is enhance.

Format

dldp work-mode { **enhance** | **normal** }

undo dldp work-mode [**enhance** | **normal**]

Parameters

Parameter	Description	Value
enhance	Indicates enhance mode of DLDP.	-
normal	Indicates normal mode of DLDP.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A unidirectional link fault may be caused by cross connections of optical fibers or disconnection of one optical fiber. You can use the **dldp work-mode** command to set the working mode of DLDP to detect the preceding two types of unidirectional links.

DLDP can work in either of the following working modes:

- Normal: DLDP does not automatically detect a neighbor when aging out a neighbor entry. In this mode, the system can identify only unidirectional links caused by cross connections of optical fibers. When the aging timer of a

neighbor times out, the local end deletes the entry of the neighbor and sends an Advertisement packet with an RSY tag.

- Enhance: DLDP automatically detects a neighbor when aging out a neighbor entry. In this mode, the system can identify unidirectional links caused by cross connections of optical fibers or disconnection of one optical fiber. In this mode, when the aging timer of a neighbor times out, the local end starts the enhance timer and consecutively sends eight Probe packets to detect the neighbor, at the rate of one packet per second. If the local end does not receive any Echo packet from the neighbor when the Echo timer times out, DLDP enters the Disable state.

Prerequisites

DLDP has been enabled globally using the **dldp enable** command.

Example

Set the working mode of DLDP to enhance.

```
<HUAWEI> system-view
[HUAWEI] dldp enable
[HUAWEI] dldp work-mode enhance
```

12.4.13 reset dldp statistics

Function

The **reset dldp statistics** command deletes the statistics about DLDP packets on an interface.

Format

reset dldp statistics [**interface** *interface-type interface-number*]

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Deletes the statistics about DLDP packets on a specified DLDP interface. • *interface-type* specifies the interface type. • *interface-number* specifies the interface number. If no interface is specified, the statistics about DLDP packets on all DLDP interfaces are deleted. If an interface is specified, the statistics about DLDP packets on the interface are deleted.	-

Views

User view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Before collecting statistics about DLDP packets on an interface in a specified period, you can run the **reset dldp statistics** command to delete the existing DLDP packet statistics on the interface.

Precautions

The **reset dldp statistics** command deletes the statistics about DLDP packets. Exercise caution when running this command.

Example

Delete the statistics about DLDP packets on all DLDP interfaces.

```
<HUAWEI> reset dldp statistics
```


12.5 Smart Link And Monitor Link Configuration Commands

12.5.1 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.

12.5.2 display monitor-link group

Function

The **display monitor-link group** command displays information about a specified Monitor Link group or all Monitor Link groups.

Format

display monitor-link group { **all** | *group-id* }

Parameters

Parameter	Description	Value
all	Displays information about all Monitor Link groups.	-
group-id	Displays information about the specified Monitor Link groups.	The value is an integer that ranges from 1 to 16.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

After creating a Monitor Link group and adding uplink and downlink interfaces to the group, run this command to view the information about the group. The displayed information includes the name and status of each member interface.

Prerequisites

A Monitor Link group has been created using the **monitor-link group** command, and uplink and downlink interfaces have been added to the Monitor Link group using the **port** command.

Example

Display information about Monitor Link group 1.

```
<HUAWEI> display monitor-link group 1
Monitor Link group 1 information :
Recover-timer is 3 sec.
--------------------------------------------------------------------------------
Member                Role     State Last-up-time                 Last-down-time
--------------------------------------------------------------------------------
GigabitEthernet0/0/1  UpLk     DOWN  0000/00/00 00:00:00 UTC+00:00  0000/00/00 00:00:00 UTC
+00:00
GigabitEthernet0/0/2  DwLk[1]  DOWN  0000/00/00 00:00:00 UTC+00:00  0000/00/00 00:00:00 UTC
+00:00
<HUAWEI> display monitor-link group 1
Monitor Link group 1 information :
Recover-timer is 3 sec.
--------------------------------------------------------------------------------
Member                Role     State Last-up-time                 Last-down-time
--------------------------------------------------------------------------------
GigabitEthernet0/0/1  UpLk     DOWN  0000/00/00 00:00:00 UTC+00:00  0000/00/00 00:00:00 UTC
+00:00
GigabitEthernet0/0/2  UpLk     DOWN  0000/00/00 00:00:00 UTC+00:00  0000/00/00 00:00:00 UTC
+00:00
GigabitEthernet0/0/3  DwLk[1]  DOWN  0000/00/00 00:00:00 UTC+00:00  0000/00/00 00:00:00 UTC
+00:00
```

Table 12-33 Description of the display monitor-link group command output

Item	Description
Recover-timer	Wait-to-Restore time of the Monitor Link group, expressed in seconds. Use the **timer recover-time** command to set this parameter.
Member	Member interface of a Monitor Link group.
Role	Role of a member interface. • UpLk: An uplink. • DwLk[1]: A downlink. The number within the square brackets specifies a downlink ID.
State	Physical status of a member interface. • UP: The member interface is in the Up state. • DOWN: The number interface is in the Down state.

Item	Description
Last-up-time	Time when the member interface becomes Up for the last time. The format is YYYY/MM/DD HH:MM:SS UTC+HH:MM. If no record indicates that the interface is switched from Down to Up, the time is displayed as 0000/00/00 00:00:00 UTC +00:00.
Last-down-time	Time when the member interface becomes Down for the last time. The format is YYYY/MM/DD HH:MM:SS UTC+HH:MM. If no record indicates that the interface is switched from Up to Down, the time is displayed as 0000/00/00 00:00:00 UTC +00:00.

12.5.3 display monitor-link protocol-parameter group

Function

The **display monitor-link protocol-parameter group** command displays internal data of all Monitor Link groups or a specified Monitor Link group, including member interface information and Monitor Link configuration.

Format

display monitor-link protocol-parameter group { **all** | *group-id* }

Parameters

Parameter	Description	Value
all	Displays internal data of all Monitor Link groups.	-
group-id	Displays internal data of a specified Monitor Link group.	The value is an integer that ranges from 1 to 16.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

This command displays internal data of Monitor Link groups for diagnosis. You can use this command to check internal status data of a Monitor Link group.

Example

Display the internal data of Monitor Link group 1.

```
<HUAWEI> display monitor-link protocol-parameter group 1
MONITOR-LINK Group 1:
*********************************
 *RecoverTime:        3 sec.
 *TimeCounter:        0 sec.
 *Uplink Info:
  IfIndex:            357(GigabitEthernet4/0/40/0/4)
  PortType:             2(MTLK_PORT_SWITCH)
  LinkStatus:           0(down)
  IFNET_S
   SMLK Group ID:     0
   MTLK Group ID:     1
   Role:              4(uplink)
 *Downlink 1 Info:
  IfIndex:            358(GigabitEthernet4/0/50/0/5)
  LinkStatus:           0(down)
  IsShutdown:           1(shutdown)
<HUAWEI> display monitor-link protocol-parameter group 1
MONITOR-LINK Group 1:
*********************************
 *RecoverTime:        3 sec.
 *TimeCounter:        0 sec.
 *Uplink Info:
  IfIndex:            357(GigabitEthernet4/0/40/0/4)
  PortType:             2(MTLK_PORT_SWITCH)
  LinkStatus:           0(down)
  IFNET_S
   SMLK Group ID:     0
   MTLK Group ID:     1
   Role:              4(uplink)
 *Uplink Info:
  IfIndex:            358(GigabitEthernet4/0/50/0/5)
  PortType:             2(MTLK_PORT_SWITCH)
  LinkStatus:           0(down)
  IFNET_S
   SMLK Group ID:     0
   MTLK Group ID:     1
   Role:              4(uplink)
 *Downlink 1 Info:
  IfIndex:            359(GigabitEthernet4/0/60/0/6)
  LinkStatus:           0(down)
  IsShutdown:           1(shutdown)
```

Table 12-34 Description of the display monitor-link protocol-parameter group command output

Item	Description
MONITOR-LINK Group 1	ID of a Monitor Link group.

Item	Description
RecoverTime	Wait-to-restore (WTR) time of the Monitor Link group The WTR time can be set using the **timer recover-time** command.
TimeCounter	WTR timer counter value.
Uplink Info	Information about the uplink interface in the Monitor Link group.
IfIndex	Interface index.
PortType	Type of the interface. • 0(MTLK_PORT_UNKOWN): invalid interface type • 1(MTLK_PORT_SMLK): Smart Link group • 2(MTLK_PORT_SWITCH): Ethernet or Eth-Trunk interface
LinkStatus	Link status of an interface: • 0(down) • 1(up)
IFNET_S	Mnemonic symbol, indicating information saved on an interface.
SMLK Group ID	ID of a Smart Link group.
MTLK Group ID	ID of a Monitor Link group.
Role	Role of an interface in the Monitor link group.
Ctrl Vlan	Control VLAN.
Password	Password of Flush packets.
Downlink 1 Info	Information about downlink interface 1.
IsShutdown	Whether the downlink interface is shut down.

12.5.4 display smart-link flush

Function

The **display smart-link flush** command displays information about received Flush packets.

Format

display smart-link flush

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

The **display smart-link flush** command displays information about received Flush packets, which helps you learn about link switchover information and identify interface faults. To delete information about received Flush packets, run the **reset smart-link flush** command.

Precautions

The master and slave interfaces of the Smart Link group are both in Down state. When the master interface or slave interface becomes Up, statistics on Flush packets may be inaccurate.

Prerequisites

The downstream device has been enabled to send Flush packets using the **flush send** command and the local device has been enabled to receive Flush packets using the **smart-link flush receive** command.

Follow-up Procedure

If the current information about Flush packets is no longer needed, run the **reset smart-link flush** command to delete the information.

Example

Display information about the received Flush packets.

```
<HUAWEI> display smart-link flush
Receive flush packets count:              1191
Receive last flush interface:             GigabitEthernet0/0/1
Receive last flush packet time:           02:42:37 UTC+03:00 2009/11/27
Receive last flush packet source mac:     00e0-fc00-0140
Receive last flush packet control vlan ID: 311
```

Table 12-35 Description of the display smart-link flush command output

Item	Description
Receive flush packets count	Number of Flush packets received.
Receive last flush interface	Interface that receives the latest Flush packet.

Item	Description
Receive last flush packet time	Time when the latest Flush packet is received, in any of the following formats: • HH:MM:SS YYYY-MM-DD • HH:MM:SS UTC±HH:MM DST YYYY-MM-DD • HH:MM:SS UTC±HH:MM YYYY-MM-DD • HH:MM:SS DST YYYY-MM-DD UTC±HH:MM indicates that a time zone is configured using the **clock timezone** command; DST indicates that the daylight saving time is configured using **clock daylight-saving-time** command.
Receive last flush packet source mac	Source MAC address of the latest Flush packet received.
Receive last flush packet control vlan ID	Control VLAN ID of the latest Flush packet received.

12.5.5 display smart-link group

Function

The **display smart-link group** command displays information about all Smart Link groups or a specified Smart Link group.

Format

display smart-link group { **all** | *group-id* }

Parameters

Parameter	Description	Value
all	Displays information about all Smart Link groups.	-
group-id	Displays information about a specified Smart Link group.	The value is an integer that ranges from 1 to 16.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

The **display smart-link group** command displays information about a Smart Link group, including member interfaces in the Smart Link group and link status. If a Smart Link group fails, you can find the cause of the fault according to the displayed information.

Prerequisites

A Smart Link group has been created by using the **smart-link group** command, and member interfaces have been added to the Smart Link group by using the **port** command.

Example

Display information about Smart Link group 1.

```
<HUAWEI> display smart-link group 1
Smart Link group 1 information :
  Smart Link group was enabled
  Load-Balance Instance: 5 7 9 to 10
  Protected-vlan reference-instance: 4 to 10
  DeviceID: 00e0-fc12-3456  Control-vlan ID: 1011
  Member                Role   InstanceID State    Flush Count Last-Flush-Time
  ------------------------------------------------------------------------------

  GigabitEthernet0/0/1  Master 4         Inactive 0          0000/00/00 00:00:00 UTC+00:00
  GigabitEthernet0/0/1  Master 5         Active   0          0000/00/00 00:00:00 UTC+00:00
  GigabitEthernet0/0/1  Master 6         Inactive 0          0000/00/00 00:00:00 UTC+00:00
  GigabitEthernet0/0/1  Master 7         Active   0          0000/00/00 00:00:00 UTC+00:00
  GigabitEthernet0/0/1  Master 8         Inactive 0          0000/00/00 00:00:00 UTC+00:00
  GigabitEthernet0/0/1  Master 9         Active   0          0000/00/00 00:00:00 UTC+00:00
  GigabitEthernet0/0/1  Master 10        Active   0          0000/00/00 00:00:00 UTC+00:00
  GigabitEthernet0/0/2  Slave  4         Inactive 0          0000/00/00 00:00:00 UTC+00:00
  GigabitEthernet0/0/2  Slave  5         Active   0          0000/00/00 00:00:00 UTC+00:00
  GigabitEthernet0/0/2  Slave  6         Inactive 0          0000/00/00 00:00:00 UTC+00:00
  GigabitEthernet0/0/2  Slave  7         Active   0          0000/00/00 00:00:00 UTC+00:00
  GigabitEthernet0/0/2  Slave  8         Inactive 0          0000/00/00 00:00:00 UTC+00:00
  GigabitEthernet0/0/2  Slave  9         Active   0          0000/00/00 00:00:00 UTC+00:00
  GigabitEthernet0/0/2  Slave  10        Active   0          0000/00/00 00:00:00 UTC+00:00
```

Table 12-36 Description of the display smart-link group command output

Item	Description
Smart Link group	Whether a Smart Link group is enabled. • enabled: The Smart Link group is enabled. • disabled: The Smart Link group is disabled. Run the **smart-link enable** command to modify this parameter.

Item	Description
Wtr-time	WTR time of a Smart Link group. Run the **timer wtr** command to modify this parameter.
Link status	Interface on which the data streams of a Smart Link group are locked. ● lock: Data streams are locked on the master interface. ● force: Data streams are locked on the slave interface. Run the **smart-link** command to modify this parameter.
Load-Balance Instance	ID of the load balancing instance. Run the **load-balance instance** command to modify this parameter.
Protected-vlan reference-instance	ID of the protection VLAN instance. Run the **protected-vlan reference-instance** command to modify this parameter.
DeviceID	MAC address of the local device.
Control-vlan ID	Control VLAN ID of a Smart Link group. Run the **flush send** command to modify this parameter.
Member	Member interfaces added to a Smart Link group. Run the **port** command to modify this parameter.
Role	Role of a member interface in a Smart Link group. ● Master: master interface ● Slave: slave interface Run the **port** command to modify this parameter.
InstanceID	Protection instance ID. Run the **protected-vlan reference-instance** command to modify this parameter. If **protected-vlan reference-instance** is not configured, instance 0 and all instances created by **instance** are displayed.

Item	Description
State	Status of a member interface. • Active: The member interface is forwarding packets. • Inactive: The member interface is blocked. • Unknown: The status of the member interface is unknown (for example, the Smart Link group is disabled or no member interface is added to the group).
Flush Count	Number of Flush packets sent.
Last-Flush-Time	Time when the latest Flush packet is sent. The format is YYYY/MM/DD HH:MM:SS UTC+HH:MM. If no Flush packet has ever been sent, the time is displayed as 0000/00/00 00:00:00 UTC+00:00.

12.5.6 display smart-link protocol-parameter group

Function

The **display smart-link protocol-parameter group** command displays internal data of all Smart Link groups or a specified Smart Link group, including member interface information and Smart Link configuration.

Format

display smart-link protocol-parameter group { **all** | *group-id* }

Parameters

Parameter	Description	Value
all	Displays internal data of all Smart Link groups.	-
group-id	Displays internal data of a specified Smart Link group.	The value is an integer that ranges from 1 to 16.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

This command displays internal data of Smart Link groups for diagnosis. You can use this command to check internal status data of a Smart Link group.

Example

Display the internal data of Smart Link group 1.

```
<HUAWEI> display smart-link protocol-parameter group 1
SMART-LINK Group 1:
*********************************
 *Master Port Info:
  IfIndex:            0()
  PortStatus:         1(unknown)
  LinkStatus:         0(down)
  IFNET_S
   SMLK Group ID:     0
   MTLK Group ID:     0
   Role:              0(invalid)
   Ctrl Vlan:         0
   Password:
 *Slave Port Info:
  IfIndex:            0()
  PortStatus:         1(unknown)
  LinkStatus:         0(down)
  IFNET_S
   SMLK Group ID:     0
   MTLK Group ID:     0
   Role:              0(invalid)
   CTRL Vlan:         0
   Password:
 *FSM Info:
  CurrentState:       0(Idle)
  TransEvent:         0(Invalid)
  TransIfIndex:       0()
 *Other Config:
  Lock|Force:         0(unknown)
  WtrTime:            60 sec.
  RevertEnable:       0(disable)
  GroupActive:        0(inactive)
  MTLK Uplink:        0
  RvtTimeCounter:     0 sec.
 *Flush Send Info:
  CTRL Vlan:          0
  Password:
 *1AG Event Info:
  Event Type:         0
```

Table 12-37 Description of the display smart-link protocol-parameter group command output

Item	Description
SMART-LINK Group 1	ID of a Smart Link group.
Master Port Info	Information about the master interface in the Smart Link group.
IfIndex	Interface index.

Item	Description
PortStatus	Physical status of an interface: • 1(unknown) • 2(active) • 3(inactive)
LinkStatus	Link status of an interface: • 0(down) • 1(up)
IFNET_S	Mnemonic symbol, indicating information saved on an interface.
SMLK Group ID	ID of a Smart Link group.
MTLK Group ID	ID of a Monitor Link group.
Role	Role of a member interface in a Smart Link group: • 0(invalid) • 1(master) • 2(slave)
Ctrl Vlan	Control VLAN. When the device sends Flush packets, run the **flush send** command to specify this parameter. When the device receives Flush packets, run the **smart-link flush receive** command to specify this parameter.
Password	Password of Flush packets. When the device sends Flush packets, run the **flush send** command to specify this parameter. When the device receives Flush packets, run the **smart-link flush receive** command to specify this parameter.
Slave Port Info	Information about a slave interface.
FSM Info	Finite state machine (FSM) information.
CurrentState	Current state of the state machine: • 0(Idle) • 1(Init) • 2(Master) • 3(Slave) • 0(MultiIdle) (used in load balancing scenarios)

Item	Description
TransEvent	Latest state machine transition event.
TransIfIndex	Index of the interface where the latest state machine transition event occurs.
Other Config	Other configuration.
Lock|Force	Interface where data streams are locked. • lock: indicates that data streams are locked on the master interface. • force: indicates that data streams are locked on the slave interface.
WtrTime	Wait-to-restore (WTR) time of a Smart Link group. The WTR time can be changed using the **timer wtr** command.
RevertEnable	Whether revertive switching is enabled. To configure the revertive switching function, run the **restore enable** command.
GroupActive	Whether the current Smart Link group is enabled.
MTLK Uplink	Uplink interface of a Monitor Link group.
RvtTimeCounter	WTR timer counter.
Flush Send Info	Information about Flush packets.
1AG Event Info	802.1ag event information.
Event Type	Type of an 802.1ag event.

12.5.7 flush send

Function

The **flush send** command enables a Smart Link group to send Flush packets.

The **undo flush send** command disables a Smart Link group from sending Flush packets.

By default, a Smart Link group is disabled from sending Flush packets.

Format

flush send control-vlan *vlan-id* [**password** { **simple** | **sha** } *password*]

undo flush send [**control-vlan** *vlan-id* [**password** { **simple** | **sha** } *password*]]

Parameters

Parameter	Description	Value
control-vlan *vlan-id*	Specifies the control VLAN ID of the Flush packets to be sent.	The value is an integer that ranges from 1 to 4094.
password simple	Indicates that the Flush packets sent from the Smart Link group contain a password in plain text. **NOTE** The password is saved in the configuration file in cipher text for security.	-
password sha	Indicates that the Flush packets sent from the Smart Link group contain an SHA2-256-encrypted password. **NOTE** The password is saved in the configuration file in cipher text for security.	-
password	Specifies the password carried in Flush packets.	The value is a string of 8 to 16 case-sensitive characters in plain text and consists of at least two of the following: lowercase letters, uppercase letters, digits, and special characters excluding question marks (?) and spaces.

Views

Smart Link group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When a switchover occurs between the master and slave links in a Smart Link group, the existing forwarding entries do not apply to the new topology. All the

MAC address entries and ARP entries on the network need to be updated. Therefore, the Smart Link group sends Flush packets to request other devices to update their MAC address tables and ARP tables.

The **flush send** command enables a Smart Link group to send Flush packets and sets the encryption mode, control VLAN ID, and password for Flush packets.

Prerequisites

A Smart Link group has been created using the **smart-link group** command.

Follow-up Procedure

Run the **smart-link flush receive** command on the upstream device interface to enable the interface to receive Flush packets. Ensure that the control VLAN ID and password set for the Flush packets received by the upstream device are the same as those set for the Flush packets sent by the local device. That is, the control VLAN ID and password in Flush packets sent by a device must be the same as those in Flush packets received by the device.

Precautions

- The specified control VLAN exists on the device. If it does not exist, the Flush packets fail to send.
- The control VLAN cannot be the VLAN mapped by a VBST dynamic instance.
- The control VLAN must be in the protected instance list configured by the **protected-vlan reference-instance** command.
- The Flush packets mentioned here are used only for communication between Huawei S series switches and CE series switches. Other manufacturers may define the Flush packet format differently. The peer device must be enabled to receive Flush packets.
- The original encryption mode and password are deleted after you run this command to configure the new ones.
- For security purposes, you are advised to use SHA2-256 as the authentication algorithm of Smart Link.
- The original password cannot be retrieved after it is encrypted using the SHA2-256 algorithm. If you forget your password, configure a new password.

Example

Enable Smart Link group 1 to send Flush packets with control VLAN ID 100 and password YsHsjx_202206.

```
<HUAWEI> system-view
[HUAWEI] smart-link group 1
[HUAWEI-smlk-group1] flush send control-vlan 100 password sha YsHsjx_202206
```

12.5.8 load-balance instance

Function

The **load-balance instance** command sets the load-balancing instances for a Smart Link group.

The **undo load-balance instance** command deletes load-balancing instances for a Smart Link group.

Format

load-balance instance { *instance-id1* [**to** *instance-id2*] } &<1-10> **slave**

undo load-balance instance { **all** | { *instance-id1* [**to** *instance-id2*] } &<1-10> [**slave**] }

Parameters

Parameter	Description	Value
instance-id1 [**to** *instance-id2*]	Specifies ID of a Smart Link 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. The value of *instance-id2* is an integer that ranges from 0 to 4094. The value of *instance-id2* must be greater than the value of *instance-id1*. The *instance-id1* and *instance-id2* parameters identify a range of instances. If **to** *instance-id2* is not specified, only one instance specified by *instance-id1* is configured.	-
slave	Indicates that the slave interface sends packets of the specified Smart Link instances.	-
all	Deletes all load-balancing instances of a Smart Link group.	-

Views

Smart Link group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If load balancing is not configured for a Smart Link group, only the active link transmits data traffic and the standby link is idle.

The **load-balance instance** command implements load balancing in a Smart Link group. When both links in the Smart Link group are Up, the standby link transmits the traffic from the VLANs mapping the specified instances.

The instances specified in the command are Multiple Spanning Tree Protocol (MSTP) instances. Each instance maps a range of VLANs. Multiple instances can be bound to the standby link to implement load balancing.

Prerequisites

A Smart Link group has been created using the **smart-link group** command, and VLANs have been mapped to the specified instances using the **instance** command.

Follow-up Procedure

After configuring load balancing in a Smart Link group, you can use the **display smart-link group** command to verify the configuration.

Precautions

- The VLANs mapping the instances in the command cannot be used as the control VLAN ID of Flush packets sent by the local device.
- Before you run the **load-balance instance** command in a Smart Link group, the Smart Link group must be disabled.
- The load balancing instance specified by the **load-balance instance** command must be in the protected instance list by the **protected-vlan reference-instance** command.

Example

Configure load balancing in Smart Link group 3. Configure the standby link to transmit the traffic from the VLANs mapping the instance 1.

```
<HUAWEI> system-view
[HUAWEI] smart-link group 3
[HUAWEI-smlk-group3] load-balance instance 1 slave
```

12.5.9 monitor-link group

Function

The **monitor-link group** command creates a Monitor Link group and displays the Monitor Link group view. If the specified Monitor Link group exists, the command directly displays the Monitor Link group view.

The **undo monitor-link group** command deletes a Monitor Link group.

By default, no Monitor Link group exists.

Format

monitor-link group *group-id*

undo monitor-link group *group-id*

Parameters

Parameter	Description	Value
group-id	Specifies the ID of a Monitor Link group.	The value is an integer that ranges from 1 to 16.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Monitor Link extends link redundancy of Smart Link. It synchronizes the downlink interface status with the uplink interface status so that the downstream device can be notified quickly when the uplink interface fails. The downstream device then triggers a link switchover in the Smart Link group. This prevents packet loss caused by the uplink interface failure. Before using the Monitor Link group, you must create a Monitor Link group and enter the Monitor Link group view.

Follow-up Procedure

Add uplink and downlink interfaces to the created Monitor Link group.

Precautions

Before deleting a Monitor Link group that has member interfaces, run the **undo port** command to delete all the member interfaces.

Example

Create Monitor Link group 1.

```
<HUAWEI> system-view
[HUAWEI] monitor-link group 1
[HUAWEI-mtlk-group1]
```

Delete Monitor Link group 2.

```
<HUAWEI> system-view
[HUAWEI] undo monitor-link group 2
```


12.5.10 port (Monitor Link group view)

Function

The **port** command adds an interface to a Monitor Link group and specifies the link connected to the interface as an uplink or a downlink.

The **undo port** command deletes an uplink or a downlink interface from a Monitor Link group.

By default, a Monitor Link group has no member interface.

Format

port *interface-type interface-number* { **downlink** [*downlink-id*] | **uplink** }

undo port [*interface-type interface-number*] { **downlink** *downlink-id* | **uplink** }

undo port all

Parameters

Parameter	Description	Value
interface-type interface-number	Specifies the type and number of the interface to be added to a Monitor Link group. • *interface-type* specifies the interface type. • *interface-number* specifies the interface number.	-
downlink [*downlink-id*]	Configures the current interface as a downlink interface and specifies the downlink ID.	The value is an integer that ranges from 1 to 512. If the *downlink-id* parameter is not specified, the system allocates an ID to the interface in an ascending order.
uplink	Configures the current interface as an uplink interface.	-
all	Deletes all member interfaces from a Monitor Link group.	-

Views

Monitor Link group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A Monitor Link group consists of an uplink interface or two uplink interfaces and several downlink interfaces. If the uplink interface fails, the Monitor Link group automatically disables all the downlink interfaces. After configuring a Monitor Link group, add uplink and downlink interfaces to the group. The Monitor Link group then can synchronize the downlink interface status with the uplink interface status.

Prerequisites

A Monitor Link group has been created by using the **monitor-link group** command.

Precautions

A Monitor Link group supports a maximum of two uplink interfaces (physical interfaces, Eth-Trunk interfaces, or a combination of them) or one Smart Link group.

The uplink interface status determines the downlink interface status.

- If there is only one uplink interface and the uplink interface is in Up state in the Monitor Link group or the uplink interface changes from the Down state to the Up state in the group, all downlink interfaces go Up. If there are two uplink interfaces and both of them are Down, all downlink interfaces are shut down. If only one uplink interface is Down, the downlink interfaces are Up.
- If there is only one uplink interface and the uplink interface is deleted from the Monitor Link group or the uplink interface changes from the Up state to the Down state in the group, all downlink interfaces are shut down. If there are two uplink interfaces and only one of them is Down, all downlink interfaces are shut down.

If an uplink interface exists in the Monitor Link group, run the **undo port** command to delete this interface before adding a new one.

An interface cannot be added to a Monitor Link group in the following situations:

- The interface has been added to an Eth-Trunk.
- The interface has been added to a Smart Link group.
- The interface has been added to another Monitor Link group.

Example

Add GE0/0/1 to Monitor Link group 1 and specify this interface as the uplink interface.


```
<HUAWEI> system-view
[HUAWEI] monitor-link group 1
[HUAWEI-mtlk-group1] port gigabitethernet 0/0/1 uplink
```

Add GE0/0/2 to a Monitor Link group and specify this interface as the downlink interface and the link ID as 1.

```
<HUAWEI> system-view
[HUAWEI] monitor-link group 1
[HUAWEI-mtlk-group1] port gigabitethernet 0/0/2 downlink 1
```

12.5.11 port (Smart Link group view)

Function

The **port** command adds an interface to a Smart Link group and specifies the interface as the master or slave interface.

The **undo port** command deletes a master or slave interface from a Smart Link group.

By default, a Smart Link group has no member interface.

Format

port *interface-type interface-number* { **master** | **slave** }

undo port *interface-type interface-number* { **master** | **slave** }

undo port { **all** | **master** | **slave** }

Parameters

Parameter	Description	Value
interface-type interface-number	• *interface-type* specifies the interface type. • *interface-number* specifies the interface number.	-
master	Specifies an interface as a master interface.	-
slave	Specifies an interface as a slave interface.	-
all	Deletes all the interfaces in a Smart Link group.	-

Views

Smart Link group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The Smart Link function implements link redundancy and rapid link status transition on a dual-homed network. When a device is connected to upstream devices by two uplink interfaces, one link is blocked and functions as the backup of the other link. When the active link fails, traffic is switched to the other link. To implement the Smart Link function, create a Smart Link group and add two interfaces to the Smart Link group, one as the master interface, and the other as the slave interface. The master interface is in active state; the slave interface is in inactive state.

Prerequisites

A Smart Link group has been created using the **smart-link group** command. The Spanning Tree Protocol (STP) has been disabled on the interfaces to be added to the Smart Link group by using the **stp disable** command.

Follow-up Procedure

Run the **smart-link enable** command to enable the Smart Link group. Run the **flush send** command to enable the Smart Link group to send Flush packets, and run the **smart-link flush receive** command on the upstream device interface to enable the interface to receive Flush packets.

Precautions

If port security is also configured, packets will be discarded when the number of MAC addresses learned by an interface reaches the upper limit. In this case, Smart Link Flush packets may fail to be received. To prevent this, you are advised not to use both Smart Link and port security.

Before adding a new master or slave interface to a Smart Link group, delete the previous one from the Smart Link group.

The slave interface is blocked when the Smart Link group is enabled.

An interface can be added to only one Smart Link group.

If an interface has been added to a Smart Link group, the following configurations cannot be performed on the interface. If any of the following configurations is performed on an interface, the interface cannot be added to a Smart Link group:

- RRPP, SEP, or ERPS
- STP
- Adding an interface to an Eth-Trunk
- Adding an interface to a Monitor Link group
- Adding an interface to another Smart Link group
- Service loopback (for an Eth-Trunk)

Example

Add GE0/0/1 to Smart Link group 1 and specify the interface as the master interface.

```
<HUAWEI> system-view
[HUAWEI] smart-link group 1
[HUAWEI-smlk-group1] port gigabitethernet 0/0/1 master
```

12.5.12 protected-vlan reference-instance

Function

The **protected-vlan reference-instance** command configures the protection instances for a Smart Link group.

The **undo protected-vlan reference-instance** command deletes the protection instances of a Smart Link group.

Format

protected-vlan reference-instance { *instance-id1* [**to** *instance-id2*] }&<1-10>

undo protected-vlan reference-instance { **all** | { *instance-id1* [**to** *instance-id2*] }&<1-10> }

Parameters

Parameter	Description	Value
instance-id1 [**to** *instance-id2*]	Specifies the protection instance ID of a Smart Link group. • *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. The value of *instance-id2* is an integer that ranges from 0 to 4094. The value of *instance-id2* cannot be smaller than the value of *instance-id1*. The *instance-id1* and *instance-id2* parameters identify a range of protection instances. If **to** *instance-id2* is not specified, only the protection instance specified by *instance-id1* is configured.	-
all	Specifies IDs for deleting all protection instances of a Smart Link group.	-

Views

Smart Link group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **protected-vlan reference-instance** command enables Smart Link to transmit or block the data packets from the VLAN mapping the protection instances. The Smart Link function takes effect only on the VLANs mapping the protection

instances. The **protected-vlan reference-instance** command enables users to unbind some VLANs from protection instances. Transmitting the data from these VLANs is not restricted by Smart Link.

Prerequisites

A Smart Link group has been created using the **smart-link group** command, and VLANs have been mapped to the specified instances using the **instance** command.

Precautions

Before you run the **protected-vlan reference-instance** command in a Smart Link group, the Smart Link group must be disabled.

The instances specified in the **protected-vlan reference-instance** command cannot be the VBST dynamic instances.

The Smart Link function takes effect only on the VLANs mapped to the protection instances. Therefore, the users' service data VLANs and VLANs mapped to load-balancing instances must be contained in the VLANs mapped to protection instances.

The VLANs not mapped to protection instances may cause network storms.

Example

Set the protection instance ID of a Smart Link group to 10.

```
<HUAWEI> system-view
[HUAWEI] smart-link group 1
[HUAWEI-smlk-group1] protected-vlan reference-instance 10
```

12.5.13 reset smart-link flush

Function

The **reset smart-link flush** command clears statistics about Flush packets.

Format

reset smart-link flush

Parameters

None

Views

User view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To collect the statistics in a specified period, you can run the **reset smart-link flush** command to clear historical data before collecting the statistics. For example, a Smart Link group sends a large number of Flush packets after a failover occurs. You can view the Flush packet statistics to locate the fault. After locating the fault, you can use the **reset smart-link flush** command to clear the statistics so that you can collect new statistics for fault location when another failover occurs.

Precautions

The cleared statistics cannot be restored. Run the **display smart-link flush** command to view Flush packet statistics before clearing the statistics.

Example

Clear statistics about Flush packets.

```
<HUAWEI> reset smart-link flush
```

12.5.14 restore enable

Function

The **restore enable** command enables the revertive switching of a Smart Link group.

The **undo restore enable** command disables the revertive switching of a Smart Link group.

By default, the revertive switching of a Smart Link group is disabled.

Format

restore enable

undo restore enable

Parameters

None

Views

Smart Link group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the active link in a Smart Link group fails, traffic is switched to the standby link. The original active link remains blocked after recovery. To enable the original

active link to transmit traffic, enable the revertive switching function in the Smart Link group. Traffic is switched back to the original active link when the WTR timer expires.

Prerequisites

A Smart Link group has been created using the **smart-link group** command.

Follow-up Procedure

By default, the WTR timer is 60 seconds. You can run the **timer wtr** command to change the value.

Precautions

- Link switching is performed only when both member interfaces in the Smart Link group are in Up state.
- Do not run the **undo restore enable** command during revertive switching because this will cause a revertive switching failure.

Example

Enable the revertive switching of Smart Link group 1.

```
<HUAWEI> system-view
[HUAWEI] smart-link group 1
[HUAWEI-smlk-group1] restore enable
```

12.5.15 smart-link

Function

The **smart-link** command enables a Smart Link group to lock data streams and specifies the locking interface.

The **undo smart-link** command disables a Smart Link group from locking data streams.

By default, a Smart Link group is disabled from locking data streams.

Format

smart-link { **force** | **lock** }

undo smart-link { **force** | **lock** }

Parameters

Parameter	Description	Value
force	Locks data streams on the slave interface.	-
lock	Locks data streams on the master interface.	-

Views

Smart Link group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Run the **smart-link** command to lock data streams on the master or slave link. During the maintenance, the active link in the Smart Link group needs to be inspected. To prevent the inspection from affecting normal services, configure the data stream policy for the Smart Link group. Then the device forcibly locks data streams to the standby link and switches them back to the active link after the inspection is complete.

Prerequisites

The Smart Link group has been enabled by using the **smart-link enable** command.

Precautions

After data streams are locked on a specified link, traffic cannot be switched to the other link even the specified link fails.

The **lock** and **force** keywords are mutually exclusive and only one of them can be entered each time. The **lock** keyword takes precedence over the **force** keyword. If you specify **force** and then **lock**, data streams are locked on the master interface. If you specify **lock** first, the configuration fails when you specify **force** in the command.

Example

Smart Link group 1 is configured to lock data streams and lock data streams on the slave interface.

```
<HUAWEI> system-view
[HUAWEI] smart-link group 1
[HUAWEI-smlk-group1] smart-link enable
[HUAWEI-smlk-group1] smart-link force
```

12.5.16 smart-link enable

Function

The **smart-link enable** command enables a Smart Link group.

The **undo smart-link enable** command disables a Smart Link group.

By default, a Smart Link group is disabled.

Format

smart-link enable

undo smart-link enable

Parameters

None

Views

Smart Link group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A Smart Link group takes effect and blocks the slave interface only after it is enabled. After the Smart Link group is disabled, the slave interface is unblocked.

After creating a Smart Link group and adding interfaces to the group, you must enable the Smart Link group to make it effective.

Precautions

After a Smart Link group is enabled, the slave interface is blocked only if the master and slave interfaces are both in Up state.

Example

Enable Smart Link group 1.

```
<HUAWEI> system-view
[HUAWEI] smart-link group 1
[HUAWEI-smlk-group1] smart-link enable
```

12.5.17 smart-link flush receive

Function

The **smart-link flush receive** command enables an interface to receive Flush packets and specifies the control VLAN ID and password for Flush packets.

The **undo smart-link flush receive** command disables an interface from receiving Flush packets.

By default, an interface rejects Flush packets.

Format

smart-link flush receive control-vlan { { *vlan-id* } &<1-10> [**password** { **simple** | **sha** } *password*] | **all** }

undo smart-link flush receive [**control-vlan** { *vlan-id* | **all** }] (interface view)

undo smart-link flush receive (port group view)

Parameters

Parameter	Description	Value
control-vlan *vlan-id*	Specifies the control VLAN ID of Flush packets that can be received.	The value is an integer that ranges from 1 to 4094.
password simple	Indicates that the password for sending Flush packets is in plain text. **NOTE** The password is saved in the configuration file in cipher text for security.	-
password sha	Indicates that Flush packets sent from the Smart Link group contain an SHA2-256-encrypted password. **NOTE** The password is saved in the configuration file in cipher text for security.	-
password	Specifies the password carried in Flush packets.	The value is a string of 8 to 16 case-sensitive characters in plain text and consists of at least two of the following: lowercase letters, uppercase letters, digits, and special characters excluding question marks (?) and spaces.
all	Indicates that all control VLANs allow Flush packets.	-

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 and port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When a switchover occurs between the master and slave links in a Smart Link group, the existing forwarding entries do not apply to the new topology. All the MAC address entries and ARP entries on the network need to be updated. The Smart Link group sends Flush packets to notify upstream devices of the topology change. Upstream devices can update their MAC address entries and ARP entries only if they are enabled to receive Flush packets. If a device rejects Flush packets, it cannot forward packets correctly after a link failover occurs in the Smart Link group.

Precautions

- The Flush packets mentioned here are used only for communication between Huawei CE series and S series switches. Other manufacturers may define different Flush packet formats.
- The **smart-link flush receive** command does not add member interfaces of the Smart Link group to the control VLAN. You need to configure the member interfaces to allow the control VLAN. The interface accepts a Flush packet only if the control VLAN ID and password in the packet are the same as those configured on the local interface.
- A maximum of 256 control VLANs used to receive Flush packets can be configured on an interface.
- The original encryption mode and password are deleted after you run this command to configure the new ones. If the control VLAN ID is changed, the password must be reconfigured.
- For security purposes, you are advised to use SHA2-256 as the authentication algorithm of Smart Link.
- If the password is encrypted in the SHA2-256 mode, it cannot be retrieved. Set a new password after the original one is lost.

Example

Enable GE0/0/1 to receive Flush packets with control VLAN ID 100 and password **YsHsjx_202206**.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] smart-link flush receive control-vlan 100 password sha YsHsjx_202206
```

12.5.18 smart-link flush receive password

Function

The **smart-link flush receive password** command specifies an encryption mode and a password for Flush packets on all interfaces.

The **undo smart-link flush receive password** command deletes the encryption mode and a password for Flush packets on all interfaces.

By default, no encryption mode or password is configured for Flush packets on all interfaces.

Format

smart-link flush receive password { **simple** | **sha** } *password*

undo smart-link flush receive password

Parameters

Parameter	Description	Value
simple	Indicates that the password for sending Flush packets is in plain text. **NOTE** The password is saved in the configuration file in cipher text for security.	-
sha	Indicates that the password for sending Flush packets is in SHA2-256 mode. **NOTE** The password is saved in the configuration file in cipher text for security.	-
password	Specifies the password carried in Flush packets.	The value is a string of 8 to 16 case-sensitive characters in plain text and consists of at least two of the following: lowercase letters, uppercase letters, digits, and special characters excluding question marks (?) and spaces.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can run the **smart-link flush receive password** command to specify an encryption mode and a password for Flush packets on all interfaces.

Prerequisites

The downstream device has been enabled to send Flush packets by using the **flush send** command.

Precautions

- The password configured in a control VLAN on an interface that is enabled to receive flush packets takes precedence over the password configured globally. If the password on an interface is not configured, the interface configured globally is used.
- For security purposes, you are advised to use SHA2-256 as the authentication algorithm of Smart Link.

Example

Specify YsHsjx_202206 for Flush packets.

```
<HUAWEI> system-view
[HUAWEI] smart-link flush receive password sha YsHsjx_202206
```

12.5.19 smart-link hold-time

Function

The **smart-link hold-time** command sets the holdtime for reporting the Interface-Up or Interface-Down event in a Smart Link group.

The **undo smart-link hold-time** command deletes the holdtime for reporting the Interface-Up or Interface-Down event in a Smart Link group.

By default, a port-Up or port-Down event is reported immediately.

Format

smart-link hold-time *hold-time*

undo smart-link hold-time [*hold-time*]

Parameters

Parameter	Description	Value
hold-time	Specifies the holdtime for reporting the Interface-Up or Interface-Down event in a Smart Link group.	The value is an integer that ranges from 0 to 60, in 100 ms.

Views

Smart Link group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If services are frequently switched between links in a Smart Link group because of temporary link disconnection, packets may be lost and system performance deteriorates. To prevent frequent switchover caused by temporary link disconnection, run the **smart-link hold-time** command to set the holdtime for reporting an Interface-Up or Interface-Down event. When the member interfaces of the Smart Link group alternate between Up and Down, the Smart Link group waits until the holdtime expires, and then triggers a switchover.

Prerequisites

A Smart Link group has been created using the **smart-link group** command.

Precautions

If you run the **smart-link hold-time** command multiple times in the same Smart Link group view, only the latest configuration takes effect.

Example

Set the holdtime of Smart Link failover in Smart Link group 1 to 300 ms.

```
<HUAWEI> system-view
[HUAWEI] smart-link group 1
[HUAWEI-smlk-group1] smart-link hold-time 3
```

12.5.20 smart-link group

Function

The **smart-link group** command creates a Smart Link group and enters the Smart Link group view. If the Smart Link group already exists, you can enter the Smart Link group view directly.

The **undo smart-link group** command deletes a Smart Link group that already exists.

By default, no Smart Link group is created on the device.

Format

smart-link group *group-id*

undo smart-link group *group-id*

Parameters

Parameter	Description	Value
group-id	Specifies a Smart Link group ID.	The value is an integer that ranges from 1 to 16.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The Smart Link function implements link backup and rapid switchover on a dual-homed network. To use the Smart Link function, you must create a Smart Link group first.

Follow-up Procedure

After creating a Smart Link group, perform the following actions:

1. Configure master and slave interfaces in the Smart Link group.
2. Enable the Smart Link group to send Flush packets.
3. Enable the Smart Link group.

Precautions

Run the **undo port** command to delete all the member interfaces before deleting a Smart Link group that has member interfaces.

Example

Create Smart Link group 1.

```
<HUAWEI> system-view
[HUAWEI] smart-link group 1
[HUAWEI-smlk-group1]
```

12.5.21 smart-link group uplink

Function

The **smart-link group uplink** command adds a Smart Link group to a Monitor Link group as the uplink interface.

The **undo smart-link group uplink** command deletes a Smart Link group from a Monitor Link group.

Format

smart-link group *group-id* **uplink**

undo smart-link group *group-id* **uplink**

Parameters

Parameter	Description	Value
group-id	Specifies a Smart Link group ID.	The value is an integer that ranges from 1 to 16.

Views

Monitor Link group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Cascading of Smart Link and Monitor Link improves link backup reliability. When the uplink interface is a Smart Link group, the uplink interface is considered faulty and the Monitor Link group forcibly disables the downlink interfaces only if both the master and slave interfaces of the Smart Link group are in Inactive or Down state.

Prerequisites

A Smart Link group has been created using the **smart-link group** command.

Precautions

A Smart Link group can be added to only one Monitor Link group.

A Smart Link can function only as the uplink interface in a Monitor Link group.

When the uplink interface fails, all the downlink interfaces in the Monitor Link group are shut down.

Before adding a Smart Link group to a Monitor Link group, delete the previous uplink interface from the Monitor Link group.

Example

Add Smart Link group 1 to Monitor Link group 2 as the uplink interface.

```
<HUAWEI> system-view
[HUAWEI] monitor-link group 2
[HUAWEI-mtlk-group2] smart-link group 1 uplink
```


12.5.22 smart-link link-switch send-broadcast enable

Function

The **smart-link link-switch send-broadcast enable** command enables a device to send broadcast packets to trigger the peer device to re-learn MAC addresses.

The **undo smart-link link-switch send-broadcast enable** command cancels the configuration.

By default, the function of sending broadcast packets to trigger the peer device to re-learn MAC addresses is disabled.

NOTE

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

Format

smart-link link-switch send-broadcast enable

undo smart-link link-switch send-broadcast enable

Parameters

None

Views

Smart Link group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When a Smart Link interface is connected to a non-Huawei device that does not support Smart Link and the active link goes Down, MAC address information on the network cannot be quickly updated. In this case, you can run this command to enable a device to send broadcast packets to trigger the peer device to re-learn MAC addresses.

Prerequisites

This function takes effect only when Smart Link is enabled and the master and slave interfaces are configured.

Example

Enable the function of sending broadcast packets for Smart Link group 1.

```
<HUAWEI> system-view
[HUAWEI] smart-link group 1
```



```
[HUAWEI-smlk-group1] smart-link enable
[HUAWEI-smlk-group1] smart-link link-switch send-broadcast enable
```

12.5.23 smart-link manual switch

Function

The **smart-link manual switch** command enables the device to switch services from the active link to the standby link in a Smart Link group.

Format

smart-link manual switch

Parameters

None

Views

Smart Link group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the active link in a Smart Link group fails, traffic is switched to the standby link. The original active link remains blocked after recovery. Generally, a stable link is used as the active link. Therefore, after the original active link recovers, you can perform the following operations to switch traffic back to this link:

- Enable the revertive switching of a Smart Link group. The system performs switching after the revertive switching timer times out.
- Run the **smart-link manual switch** command to switch traffic back.

However, the minimum revertive switching time is 30s, and the default value is 60s. You can run the **smart-link manual switch** command to manually switch traffic back to the active link.

Prerequisites

To implement an active/standby switchover between links, ensure that:

- The active interface and standby interface exist and are both in Up state.
- Traffic is not blocked on either interface by using the **smart-link** command.

Precautions

Millisecond-level packet loss will occur during the switchover.

Example

Perform an active/standby switchover between links of Smart Link group 1.

```
<HUAWEI> system-view
[HUAWEI] smart-link group 1
[HUAWEI-smlk-group1] smart-link manual switch
```

12.5.24 smart-link { vpls-notify | vll-notify } enable

Function

The **smart-link** { **vpls-notify** | **vll-notify** } **enable** command enables an interface to notify the VPLS/VLL module when the interface receives a Flush packet.

The **undo smart-link** { **vpls-notify** | **vll-notify** } **enable** command cancels the configuration.

By default, an interface does not notify the VPLS/VLL module when receiving a Flush packet.

NOTE

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

Format

smart-link { **vpls-notify** | **vll-notify** } **enable**

undo smart-link { **vpls-notify** | **vll-notify** } **enable**

Parameters

Parameter	Description	Value
vpls-notify	Enables an interface to notify the VPLS module when receiving Flush packets.	-
vll-notify	Enables an interface to notify the VLL module when receiving Flush packets.	-

Views

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

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If a customer edge (CE) device is dual homed to a VPLS or VLL network through VLANIF interfaces or dot1q sub-interfaces of a provider edge (PE) device, associate Smart Link with VPLS on the corresponding physical interfaces of the PE device. If the VLANIF interfaces or dot1q sub-interfaces are bound to VSI or VLL run the **smart-link flush receive** and **smart-link { vpls-notify | vll-notify } enable** commands on the corresponding physical interfaces. Then the physical interfaces can notify the VPLS or VLL module when receiving a Flush packet. The VPLS or VLL module then deletes the MAC addresses learned from the VSI or VLL bound to the VLANIF interfaces or dot1q sub-interfaces, and sends messages to remote devices, instructing them to update MAC address entries.

Prerequisites

The VPLS or VLL configuration has been completed on the backbone network. The Smart Link configuration has been completed on the CE interfaces connected to the PE device. The VLANIF interfaces or dot1q sub-interfaces of the PE device connected to the CE device have been bound to VSI or VLL. The physical interfaces connected to the CE device have been enabled to accept Flush packets by using the **smart-link flush receive** command.

Precautions

You can associate Smart Link with VPLS or VLL only when a CE device is connected to the VPLS or VLL network through VLANIF interfaces or dot1q sub-interfaces of a PE device. Smart Link cannot be associated with VPLS or VLL when the CE device is connected to the VPLS or VLL network through physical interfaces.

Example

Enable XGE0/0/1 to notify the VPLS module when the interface receives a Flush packet.

```
<HUAWEI> system-view
[HUAWEI] interface xgigabitethernet 0/0/1
[HUAWEI-XGigabitEthernet0/0/1] smart-link vpls-notify enable
```

12.5.25 timer recover-time

Function

Using the **timer recover-time** command, you can set the wait to restore (WTR) time of a Monitor Link group.

Using the **undo timer recover-time** command, you can restore the default WTR time of a Monitor Link group.

By default, the WTR time of a Monitor Link group is 3 seconds.

Format

timer recover-time *recover-time*

undo timer recover-time [*recover-time*]

Parameters

Parameter	Description	Value
recover-time	Specifies the WTR time of a Monitor Link group.	The value is an integer that ranges from 3 to 60, in seconds. The default value is 3.

Views

Monitor Link group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If the downlink interface status changes frequently in a Monitor Link group because of temporary uplink disconnection, packets are lost and system performance deteriorates. To prevent frequent failover caused by temporary link disconnection, you can use the **timer recover-time** command to set the WTR time of the Monitor Link group. The Monitor Link group does not restore downlink interfaces immediately after the uplink interface recovers. The downlink interfaces become Up until the WTR time expires.

recover-time indicates the internal switching time of a Monitor Link group. That is, the system starts the interface Up operation after the internal switching time is reached. The actual interface Up time is also affected by the interface Up performance.

Prerequisites

A Monitor Link group has been created by using the **monitor-link group** command.

Example

Set the WTR time to 6 seconds for Monitor Link group 1.

```
<HUAWEI> system-view
[HUAWEI] monitor-link group 1
[HUAWEI-mtlk-group1] timer recover-time 6
```

12.5.26 timer wtr

Function

The **timer wtr** command sets the WTR time of a Smart Link group.

The **undo timer wtr** command restores the default WTR time of a Smart Link group.

By default, the WTR time of a Smart Link group is 60 seconds.

Format

timer wtr *wtr-time*

undo timer wtr [*wtr-time*]

Parameters

Parameter	Description	Value
wtr-time	Specifies the WTR time.	The value is an integer that ranges from 30 to 1200, in seconds. The default WTR time is 60 seconds.

Views

Smart Link group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the active link in a Smart Link group fails, traffic is switched to the standby link. The original active link remains blocked after recovery. To enable the original active link to transmit traffic, enable the revertive switching function in the Smart Link group. Traffic is switched back to the original active link when the WTR timer expires.

Precautions

If the network is unstable or has no requirement for the transmission delay, set a longer WTR time to prevent frequent switching.

Example

Set the WTR time to 120 seconds for Smart Link group 1.

```
<HUAWEI> system-view
[HUAWEI] smart-link group 1
[HUAWEI-smlk-group1] timer wtr 120
```


12.6 MAC Swap Loopback Configuration Commands

12.6.1 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.

12.6.2 display loopback swap-mac information

Function

The **display loopback swap-mac information** command displays the MAC swap loopback configuration.

Format

display loopback swap-mac information

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

To ensure a successful loopback test, use this command to check the loopback configuration before the loopback test. After the loopback test is complete, use this command to view the number of loopback test packets and the number of discarded test packets, and compare them with the number of packets sent from the tester to check network performance.

Pre-configuration Tasks

The local MAC swap loopback function has been configured by using the **loopback local swap-mac** command or the local MAC swap loopback function has been configured by using the **loopback remote swap-mac** command.

Example

Display the MAC swap loopback configuration.

Models excluding 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:

```
<HUAWEI> display loopback swap-mac information
  Loopback type            : local
  Loopback state           : running
  Loopback test time(s)    : 60
  Loopback interface       : GigabitEthernet0/0/1
  Loopback output interface : GigabitEthernet0/0/2
  Loopback source MAC      : 0001-0001-0001
  Loopback destination MAC  : 0002-0002-0002
  Loopback vlan            : 10
  Loopback inner vlan      : 0
  Loopback packets         : 0
  Drop packets             : 3
```

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:

```
<HUAWEI> display loopback swap-mac information
  Loopback type            : remote
  Loopback state           : running
  Loopback test time(s)    : 60
  Loopback interface       : GigabitEthernet0/0/1
  Loopback output interface : GigabitEthernet0/0/2
```

Table 12-38 Description of the display loopback swap-mac information command output

Item	Description
Loopback type	Type of the MAC swap loopback test: • local: local MAC swap loopback test • remote: remote MAC swap loopback test Run the following commands to configure loopback type. **loopback local swap-mac** **loopback remote swap-mac**
Loopback state	Status of the MAC swap loopback function: • running: The MAC swap loopback function is enabled. • stop: The MAC swap loopback function is disabled. Run the following commands to configure loopback state. **loopback swap-mac**
Loopback test time(s)	Timeout period of the loopback test. If the value is none, the loopback test timeout function is disabled.

Item	Description
Loopback interface	Interface where the loopback test is performed.
Loopback output interface	Outbound interface that sends test packets back to the tester.
Loopback source MAC	Source MAC address of test packets.
Loopback destination MAC	Destination MAC address of test packets.
Loopback vlan	VLAN ID of test packets.
Loopback inner vlan	Inner VLAN ID of test packets.
Loopback packets	Number of received loopback packets.
Drop packets	Number of discarded packets. This field is displayed only when a local MAC swap loopback test is performed.

12.6.3 loopback local swap-mac

Function

The **loopback local swap-mac** command enables local MAC swap loopback.

The **undo loopback local swap-mac** command disables local MAC swap loopback.

By default, local MAC swap loopback is disabled on an interface.

NOTE

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

Format

loopback local swap-mac source-mac *source-mac-address* **dest-mac** *dest-mac-address* **vlan** *vlan-id* [**inner-vlan** *inner-vlan-id*] **interface** *interface-type interface-number* [**timeout** { *time-value* | **none** }]

undo loopback local swap-mac

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 the **inner-vlan** *inner-vlan-id* parameter.

Parameters

Parameter	Description	Value
source-mac *source-mac-address*	Specifies the source MAC address of test packets.	The value is in H-H-H format. An H is a hexadecimal number of 1 to 4 digits. The source and destination MAC addresses must be unicast MAC addresses.
dest-mac *dest-mac-address*	Specifies the destination MAC address of test packets.	The value is in H-H-H format. An H is a hexadecimal number of 1 to 4 digits. The source and destination MAC addresses must be unicast MAC addresses.
vlan *vlan-id*	Specifies the VLAN ID of test packets.	The value is an integer that ranges from 1 to 4094.
inner-vlan *inner-vlan-id*	Specifies the inner VLAN ID of test packets.	The value is an integer that ranges from 1 to 4094.
interface *interface-type interface-number*	Specifies the outbound interface that sends loopback packets back to the tester. • *interface-type* specifies the interface type. • *interface-number* specifies the interface number.	-
timeout *time-value*	Specifies the timeout period of a loopback test. If the **loopback swap-mac start** command is run to enable MAC swap loopback, a MAC swap loopback test stops after the timeout period of the loopback test expires.	The value is an integer that ranges from 5 to 300, in seconds. The default value is 60.

Parameter	Description	Value
timeout none	Indicates that the loopback test timeout function is disabled. If the **loopback swap-mac start** command is run to enable MAC swap loopback, a MAC swap loopback test cannot automatically stop after its timeout period expires. Instead, you must run the **loopback swap-mac stop** command to manually stop the MAC swap loopback test.	-

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

Before using the Switch to provide services for users, perform a local MAC swap loopback test on the Switch to check whether the Switch can provide services properly. This test checks connectivity and QoS CAR of the network between the Switch downlink interface and a remote device. The local MAC swap loopback test can also check whether VLAN mapping and VLAN stacking are configured successfully on the downlink interface.

A local MAC swap loopback test checks connectivity and performance of the network between a tester and a tested switch, and performance of the tested switch.

In a local MAC swap loopback test, a tester sends test packets to the Switch. When test packets reach the downlink interface, the Switch swaps the source and destination MAC addresses of test packets and sends the packets back to the tester through a specified outbound interface.

Follow-up Procedure

Run the **loopback swap-mac start** command to enable the MAC swap loopback function.

Precautions

NOTICE

When a local loopback test is performed on an interface, all services on the interface are interrupted.

- An Eth-Trunk interface in LACP mode does not support the local MAC swap loopback function. An Eth-Trunk member interface does not support the MAC swap loopback function.
- Before enabling the local MAC swap loopback function, you need to run the **undo stp enable** command to disable STP on the interface.
- 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.
- If a large number of test packets are sent, test packets occupy bandwidth of other services on the interface that sends test packets.

Example

Configure local MAC swap loopback.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] loopback local swap-mac source-mac 00e0-fc00-0085 dest-mac 00e0-fc00-1004 vlan 100 interface gigabitethernet 0/0/2
```

12.6.4 loopback remote swap-mac

Function

The **loopback remote swap-mac** command enables remote MAC swap loopback.

The **undo loopback remote swap-mac** command disables remote MAC swap loopback.

By default, remote MAC swap loopback is disabled on an interface.

Format

Models excluding the S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S500, S5735-S-I, S5735S-S, and S5735-S:

loopback remote swap-mac source-mac *source-mac-address* **dest-mac** *dest-mac-address* **vlan** *vlan-id* [**inner-vlan** *inner-vlan-id*] [**timeout** { *time-value* | **none** }]

undo loopback remote swap-mac

S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S500, S5735-S-I, S5735S-S, and S5735-S:

loopback remote swap-mac [**timeout** { *time-value* | **none** }]

undo loopback remote swap-mac

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 the **inner-vlan** *inner-vlan-id* parameter.

Parameters

Parameter	Description	Value
source-mac *source-mac-address*	Specifies the source MAC address of test packets.	The value is in H-H-H format. An H is a hexadecimal number of 1 to 4 digits. The source and destination MAC addresses must be unicast MAC addresses.
dest-mac *dest-mac-address*	Specifies the destination MAC address of test packets.	The value is in H-H-H format. An H is a hexadecimal number of 1 to 4 digits. The source and destination MAC addresses must be unicast MAC addresses.
vlan *vlan-id*	Specifies the VLAN ID of test packets.	The value is an integer that ranges from 1 to 4094.
inner-vlan *inner-vlan-id*	Specifies the inner VLAN ID of test packets.	The value is an integer that ranges from 1 to 4094.
timeout *time-value*	Specifies the timeout period of a loopback test. If the **loopback swap-mac start** command is run to enable MAC swap loopback, a MAC swap loopback test stops after the timeout period of the loopback test expires.	The value is an integer that ranges from 5 to 300, in seconds. The default value is 60.

Parameter	Description	Value
timeout none	Indicates that the loopback test timeout function is disabled. If the **loopback swap-mac start** command is run to enable MAC swap loopback, a MAC swap loopback test cannot automatically stop after its timeout period expires. Instead, you must run the **loopback swap-mac stop** command to manually stop the MAC swap loopback test.	-

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

Before using the Switch to provide services for users, perform a remote MAC swap loopback test to check whether the Switch can provide services properly. This test checks connectivity and performance of the network between the Switch uplink interface and a remote device. The remote MAC swap loopback test can also check whether VLAN mapping and VLAN stacking are configured successfully on the uplink interface.

A remote MAC swap loopback test checks connectivity and performance of the network between a tester and a tested switch but does not check performance of the tested switch.

In a remote MAC swap loopback test, a tester sends test packets to the Switch. When test packets reach the uplink interface, the Switch swaps the source and destination MAC addresses of test packets and sends the packets back to the tester through this interface.

Follow-up Procedure

Run the **loopback swap-mac start** command to enable the MAC swap loopback function.

Precautions

- An Eth-Trunk interface supports the MAC swap loopback function but an Eth-Trunk member interface does not.
- 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 **loopback remote swap-mac** and **single-fiber enable** commands cannot be used on the same interface.
- If the switch does not receive any test packet within the timeout period after the remote MAC swap loopback test starts, perform the test again. And then run the **loopback swap-mac start** command.
- If **timeout none** is specified in the command, you can perform a loopback test at any time until the MAC swap loopback function is disabled by using the **loopback swap-mac stop** command.

Example

Configure remote MAC swap loopback.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] loopback remote swap-mac source-mac xxxx-xxxx-xxxx dest-mac xxxx-xxxx-xxxx vlan 100
```

12.6.5 loopback swap-mac

Function

The **loopback swap-mac** command enables or disables the MAC swap loopback function.

By default, the MAC swap loopback function is disabled.

Format

loopback swap-mac { **start** | **stop** }

Parameters

Parameter	Description	Value
start	Enables the MAC swap loopback function.	-
stop	Disables the MAC swap loopback function.	-

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

Both local and remote loopback tests deteriorate network performance. To minimize impact of a loopback test, enable the MAC swap loopback function when the loopback test begins and disable it immediately after the loopback test is complete.

A MAC swap loopback test stops when you disable the MAC swap loopback function or the loopback test times out. To perform the loopback test again, run the **loopback swap-mac start** command.

Pre-configuration Tasks

The local MAC swap loopback function has been configured by using the **loopback local swap-mac** command or the local MAC swap loopback function has been configured by using the **loopback remote swap-mac** command.

Precautions

An Eth-Trunk interface supports the MAC swap loopback function but an Eth-Trunk member interface does not.

An Eth-Trunk interface in LACP mode does not support the local MAC swap loopback function.

To ensure service provisioning on the interface, disable the MAC swap loopback function immediately after the loopback test is complete.

The **loopback swap-mac** command is a one-time command and is not saved in the configuration file.

Example

Enable the MAC swap loopback function.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] loopback swap-mac start
```

12.7 EFM Configuration Commands

12.7.1 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.

12.7.2 clear mgr inactive-configuration slot

Function

The **clear mgr inactive-configuration slot** command deletes the inactive Ethernet OAM configurations from the switch that does not register.

Format

clear mgr inactive-configuration slot *slot-id* [**card** *card-id*]

Parameters

Parameter	Description	Value
slot *slot-id*	Specifies the slot ID of a switch that does not register.	The value is an integer and the value range depends on device model.
card *card-id*	Specifies the offline card ID.	The value is an integer and the value range depends on device model.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

After a subcard has been replaced, using the **clear mgr inactive-configuration slot** command deletes the configurations of the subcard that does not register if these configurations do not need to be saved.

Running the **clear mgr inactive-configuration slot** command can delete the inactive configurations.

Before using this command, note the following points:

- When the device is in the CSS, ensure that the specified card on which configurations are to be deleted does not register.
- Ensure that the specified subcard on which configurations are to be deleted does not register.

Example

Delete the configurations of the card that does not register in slot 1.


```
<HUAWEI> system-view
[HUAWEI] clear mgr inactive-configuration slot 1
Warning: The inactive oam-mgr configuration related to the interfaces of the slot or card will be deleted
and cannot be restored, continue? [Y/N]:y
Info: Operation succeeded.
```

12.7.3 display efm

Function

The **display efm** command displays the EFM configuration on an interface.

Format

display efm { **all** | **interface** *interface-type interface-number* }

Parameters

Parameter	Description	Value
all	Displays the EFM configuration on all the interfaces enabled with EFM.	-
interface-type interface-number	Displays the EFM configuration of a specified interface. • *interface-type* specifies the interface type. • *interface-number* specifies the interface number.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

To view the EFM configuration on the device, run the **display efm** command.

- If **all** is specified, all EFM configuration is displayed.
- If **interface** *interface-type interface-number* is specified, the EFM configuration of a specified interface is displayed.

Prerequisites

EFM has been enabled globally using the **efm enable** command.

Example

Display the EFM configuration on GigabitEthernet0/0/1.


```
<HUAWEI> display efm interface gigabitethernet 0/0/1
  Item                          Value
  ------------------------------------------------------------
  Interface:                    GigabitEthernet0/0/1
  EFM Enable Flag:              enable
  Mode:                         active
  Loopback IgnoreRequest:       no
  OAMPDU MaxSize:               128
  OAMPDU Timeout:               5000
  OAMPDU Interval:              1000
  Parser:                       forward
  Multiplexer:                  forward
  ErrCodeNotification:          disable
  ErrCodePeriod:                1
  ErrCodeThreshold:             1
  ErrFrameNotification:         disable
  ErrFramePeriod:               1
  ErrFrameThreshold:            1
  ErrFrameSecondNotification:   disable
  ErrFrameSecondPeriod:         60
  ErrFrameSecondThreshold:      1
  Hold Up Time:                 10
  ThresholdEvtTriggerErrDown:   enable
  TriggerIfDown:                disable
  TriggerMacRenew:              disable
  Remote MAC:                   --
  Remote EFM Enable Flag:       --
  Remote Mode:                  --
  Remote MaxSize:               --
  Remote Loopback IgnoreRequest: --
  Remote State:                 --
  Remote Parser:                --
  Remote Multiplexer:           --
  ErrFramePeriodNotification:   disable
  ErrFramePeriodPeriod:         200000
  ErrFramePeriodThreshold:      1
  Loopback Remain Time:         1189
```

Table 12-39 Description of the display efm command output

Item	Description
Interface	Interface name.
EFM Enable Flag	Whether EFM is enabled on an interface: ● disable: indicates that EFM is disabled on an interface. ● enable: indicates that EFM is enabled on an interface. To enable or disable EFM on an interface, run the **efm enable** command.
Mode	Operation mode of EFM on an interface: ● active: indicates that EFM works in active mode. ● passive: indicates that EFM works in passive mode. To set the operation mode of EFM on an interface, run the **efm mode** command.

Item	Description
Loopback IgnoreRequest	Whether loopback requests from the remote end are ignored: ● yes: Loopback requests from the remote end are ignored. ● no: Loopback requests from the remote end are processed. To set the parameter, run the **efm loopback ignore-request** command.
OAMPDU MaxSize	Maximum size of an EFM OAMPDU on an interface. The value ranges from 64 to 1518, in bytes. The default value is 128 bytes. To set the maximum size of an EFM OAMPDU on an interface, run the **efm packet max-size** command.
OAMPDU Timeout	Timeout interval at which an interface receives EFM OAMPDUs. The value is an integer that ranges from 3000 to 30000, in milliseconds. It must be an integer multiple of 1000. The default value is 5000 ms. To set the timeout interval at which an interface receives EFM OAMPDUs, run the **efm timeout** command.
OAMPDU Interval	Timeout interval at which an interface sends EFM OAMPDUs. The value is fixed as 1000, in milliseconds.
Parser	Parser: ● forward: device is forwarding non-OAMPDUs to the lower sublayer. ● loopback: device is looping back non-OAMPDUs to lower sublayer. ● discard: device is discarding non-OAMPDUs.
Multiplexer	Multiplexer: ● forward: device is forwarding non-OAMPDUs to higher sublayer. ● discard: device is discarding non-OAMPDUs.

Item	Description
ErrCodeNotification	Whether detection of EFM errored codes is enabled: ● disable: indicates that detection of EFM errored codes is disabled. ● enable: indicates that detection of EFM errored codes is enabled. To enable or disable the detection of EFM errored codes, run the **efm error-code notification enable** command.
ErrCodePeriod	Period for detecting EFM errored codes on an interface. The value ranges from 1 to 60, in seconds. The default value is 1s. To set the period for detecting EFM errored codes on an interface, run the **efm error-code period** command.
ErrCodeThreshold	Threshold for detecting EFM errored codes on an interface. The value ranges from 0 to 65535. The default value is 1. To set the threshold for detecting EFM errored codes on an interface, run the **efm error-code threshold** command.
ErrFrameNotification	Whether detection of EFM errored frames is enabled: ● disable: indicates that detection of EFM errored frames is disabled. ● enable: indicates that detection of EFM errored frames is enabled. To enable or disable the detection of EFM errored frames, run the **efm error-frame notification enable** command.
ErrFramePeriod	Period for detecting EFM errored frames on an interface. The value ranges from 1 to 60, in seconds. The default value is 1s. To set the period for detecting EFM errored frames on an interface, run the **efm error-frame period** command.
ErrFrameThreshold	Threshold for detecting EFM errored frames on an interface. The value ranges from 0 to 65535. The default value is 1. To set the threshold for detecting EFM errored frames on an interface, run the **efm error-frame threshold** command.

Item	Description
ErrFrameSecondNotification	Whether detection of EFM errored frame seconds is enabled: ● disable: indicates that detection of EFM errored frame seconds is disabled. ● enable: indicates that detection of EFM errored frame seconds is enabled. To enable or disable the detection of EFM errored frame seconds, run the **efm error-frame-second notification enable** command.
ErrFrameSecondPeriod	Period for detecting EFM errored frame seconds on an interface. The value ranges from 10 to 900, in seconds. The default value is 60s. To set the period for detecting EFM errored frame seconds on an interface, run the **efm error-frame-second period** command.
ErrFrameSecondThreshold	Threshold for detecting EFM errored frame seconds on an interface. The value ranges from 0 to 900. The default value is 1. To set the threshold for detecting EFM errored frame seconds on an interface, run the **efm error-frame-second threshold** command.
Hold Up Time	Value of the EFM faulty-state holdup timer. The value ranges from 0 to 50, in seconds. The default value is 0. To set the value of the EFM faulty-state holdup timer, run the **efm holdup-timer** command.
ThresholdEvtTriggerErrDown	Whether a threshold crossing event is associated with an interface: ● disable: A threshold crossing event is not associated with an interface. ● enable: A threshold crossing event is associated with an interface. To set the parameter, run the **efm threshold-event trigger error-down** command.

Item	Description
TriggerIfDown	Whether an interface is blocked when the interface detects a fault on the link between the local and peer interfaces: ● disable: The system does not block an interface when detecting a fault on the link between the local and peer interfaces. ● enable: The system blocks an interface when detecting a fault on the link between the local and peer interfaces. To set the parameter, run the **efm trigger if-down** command.
TriggerMacRenew	Whether the MAC address entry on an interface is updated when the interface detects a fault on the link between the local and peer interfaces: ● disable: The system does not update the MAC address entry when detecting a fault on the link between the local and peer interfaces. ● enable: The system updates the MAC address entry when detecting a fault on the link between the local and peer interfaces. To set the parameter, run the **efm trigger mac-renew** command.
Remote MAC	MAC address of the remote interface. The value -- indicates that the system cannot obtain the MAC address of the remote interface.
Remote EFM Enable Flag	Whether EFM is enabled on the remote interface: ● disable: indicates that EFM is disabled on the remote interface. ● enable: indicates that EFM is enabled on the remote interface. ● --: indicates that the system cannot obtain the EFM status on the remote device.
Remote Mode	Operation mode of EFM on the remote interface: ● active: indicates that EFM works in active mode. ● passive: indicates that EFM works in passive mode. ● --: indicates that the system cannot obtain the operation mode of EFM on the remote device.
Remote MaxSize	Maximum size of an OAMPDU on the remote interface, in bytes. The value -- indicates that the system cannot obtain the maximum size of an OAMPDU on the remote interface.

Item	Description
Remote Loopback IgnoreRequest	Whether the remote interface ignores loopback requests from the local end: ● --: The system cannot obtain the mode in which the remote interface processes loopback requests from the local end. ● yes: The remote interface ignores loopback requests from the local end. ● no: The remote interface processes loopback requests from the local end.
Remote State	Active/Standby information of the peer device. The value -- indicates that the system cannot obtain the active/standby information of the peer device.
Remote Parser	Remote parser: ● forward: device is forwarding non-OAMPDUs to the lower sublayer. ● discard: device is discarding non-OAMPDUs.
Remote Multiplexer	Remote Multiplexer: ● forward: device is forwarding non-OAMPDUs to higher sublayer. ● loopback: device is looping back non-OAMPDUs to lower sublayer. ● discard: device is discarding non-OAMPDUs.
ErrFramePeriodNotification	Whether detection of EFM errored frame periods is enabled: ● disable: indicates that detection of EFM errored frame periods is disabled. ● enable: indicates that detection of EFM errored frame periods is enabled.
ErrFramePeriodPeriod	Period for detecting errored frame periods on the interface. The value is an integer that ranges from 20000 to 4294967295. The default value is 200000.
ErrFramePeriodThreshold	Threshold for detecting errored frame periods on the interface. The value is an integer that ranges from 0 to 900. The default value is 1.

Item	Description
Loopback Remain Time	Remaining time of remote loopback: ● --: The interface does not send a remote loopback request. ● Never Timeout: The interface sends a remote loopback request. The value of **timeout** is 0, indicating that the interface is always in remote loopback state. ● Loopback Remain Time: The interface sends a remote loopback request, and the timeout interval of remote loopback is specified.

12.7.4 display efm link-event local

Function

The **display efm link-event local** command displays statistics about local link events.

Format

display efm link-event local { **all** | **interface** *interface-type interface-number* }

Parameters

Parameter	Description	Value
all	Displays statistics about local link events of all interfaces.	-
interface-type interface-number	Displays statistics about local link events of a specified interface. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

After error code detection, error frame detection, or error frame second detection is configured, you can run the **display efm link-event local** command to view statistics about local link events.

Precautions

After the **display efm link-event local** command is run, a hyphen (-) is displayed if error code detection, error frame detection, or error frame second detection is not configured in the interface view.

Example

Displays statistics about local link events on GigabitEthernet0/0/1.

```
<HUAWEI> display efm link-event local interface gigabitethernet 0/0/1
Item                    Value
-------------------------------------------------------
Interface:               GigabitEthernet0/0/1
-------------------------
Errored-code
Errors:                 0
Error Running Total :    0
Event Running Total :    0
-------------------------
Errored-frame
Errors:                 0
Error Running Total :    0
Event Running Total :    0
-------------------------
Errored-frame-period
Errors:                 0
Error Running Total :    0
Event Running Total :    0
-------------------------
Errored-frame-seconds
Errors:                 0
Error Running Total :    0
Event Running Total :    0
```

Table 12-40 Description of the display efm link-event local command output

Item	Description
Interface	Interface enabled with EFM.
Errored-code	Information about error code.
Errored-frame	Information about error frame.
Errored-frame-period	Information about error frame period.
Errored-frame-seconds	Information about error frame second.
Errors	Number of currently detected error codes, error frames, error frame period, or error frame seconds.
Error Running Total	Total number of detected error codes, error frames, error frame period, or error frame seconds.

Item	Description
Event Running Total	Count of detected error codes, error frames, error frame period, or error frame seconds.

12.7.5 display efm session

Function

The **display efm session** command displays information about an EFM session between the specified interface and the peer.

Format

display efm session { **all** | **interface** *interface-type interface-number* }

Parameters

Parameter	Description	Value
all	Displays information about EFM sessions between all interfaces configured with EFM and the peers.	-
interface-type interface-number	Displays information about the EFM session between the specified interface and the peer. • *interface-type* specifies the interface type. • *interface-number* specifies the interface number.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

To check whether an EFM session configured on a device is negotiated successfully, run the **display efm session** command. The command output includes the EFM status and timeout interval of a loopback test.

- If **all** is specified, information about all EFM sessions configured on the device is displayed.
- If **interface** *interface-type interface-number* is specified, information about EFM sessions configured on a specified interface is displayed.

Prerequisites

EFM has been enabled globally using the **efm enable** command.

Example

Display information about EFM sessions between all interfaces and the peers.

```
<HUAWEI> display efm session all
Interface                EFM State                Loopback Timeout
--------------------------------------------------------------------------------
GigabitEthernet0/0/1     discovery                --
```

Table 12-41 Description of the display efm session command output

Item	Description
Interface	Interface name.
EFM State	EFM protocol status on the interface: • disabled: The EFM protocol is disabled on the interface. • discovery: The interface is in OAM discovery state. • detect: The interface is in Detect state. • loopback (control): The interface initiates remote loopback and discards the packets looped back. • loopback (be controlled): The interface responds to remote loopback.
Loopback Timeout	Timeout interval of a loopback test.

12.7.6 display test-packet result

Function

The **display test-packet result** command displays information about sent test packets.

Format

display test-packet result

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After remote loopback is enabled and the **test-packet start** command is used to configure a device to send test packets, the **display test-packet result** command can be used to view information about sent test packets. You can determine link performance based on the information about test packets.

Example

Display information about sent test packets.

```
<HUAWEI> display test-packet result
  TestResult                Value
------------------------------------------------------------
  PacketsSend :              5
  PacketsReceive :           5
  PacketsLost :              0
  BytesSend :                320
  BytesReceive :             320
  BytesLost :                0
  StartTime :                06-13-2012 14:44:13 UTC+03:00
  EndTime :                  06-13-2012 14:44:14 UTC+03:00
```

Table 12-42 Description of the display test-packet result command output

Item	Description
PacketsSend	Number of sent test packets.
PacketsReceive	Number of received test packets.
PacketsLost	Number of discarded test packets.
BytesSend	Total length of sent test packets, in bytes.
BytesReceive	Total length of received test packets, in bytes.
BytesLost	Total length of discarded test packets, in bytes.
StartTime	Start time test packets are sent.
EndTime	End time test packets are sent.

12.7.7 efm enable

Function

The **efm enable** command enables EFM globally or on an interface.

The **undo efm enable** command disables EFM globally or on an interface.

By default, EFM is disabled globally. That is, EFM is disabled on all interfaces.

Format

efm enable

undo efm enable

Parameters

None

Views

System 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

Before using EFM functions, you must enable EFM globally.

After EFM is enabled on an interface, the interface starts to send OAMPDUs to perform point-to-point EFM link detection. EFM link detection can be implemented between two interfaces only after EFM is enabled on the peer interface.

Precautions

When you use the **undo efm enable** command to disable EFM globally, the device deletes all EFM configurations. When the device is implementing remote loopback and sending a great deal of test packets, running the **undo efm enable** command will cause packets to be forwarded.

NOTE

Eth-Trunks do not support EFM.

Example

Enable EFM globally.

```
<HUAWEI> system-view
[HUAWEI] efm enable
Info: Operation succeeded.
```

Enable EFM on Layer 2 interface GigabitEthernet0/0/1.

```
<HUAWEI> system-view
[HUAWEI] efm enable
Info: Operation succeeded.
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] efm enable
Info: Operation succeeded.
```


Enable EFM on Layer 3 interface GigabitEthernet0/0/1.

```
<HUAWEI> system-view
[HUAWEI] efm enable
Info: Operation succeeded.
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] efm enable
Info: Operation succeeded.
```

12.7.8 efm error-code notification enable

Function

The **efm error-code notification enable** command enables an interface to detect EFM errored codes.

The **undo efm error-code notification enable** command disables an interface from detecting EFM errored codes.

By default, an interface is not enabled to detect EFM errored codes.

Format

efm error-code notification enable

undo efm error-code notification enable

Parameters

None

Views

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

Monitoring Ethernet links is difficult if network performance deteriorates while traffic is being transmitted over physical links. Link monitoring is used to detect link layer faults in various environments. After EFM link monitoring is configured, the device queries statistics about the physical layer data of the interface management module to monitor the quality of the link connected to an interface. EFM link monitoring implements the following functions:

- Reports an alarm when the number of errored codes detected during a specified detection interval exceeds the preset threshold.
- Reports an alarm when the number of errored frames detected during a specified detection interval exceeds the preset threshold.

- Reports an alarm when the number of errored frame seconds detected during a specified interval exceeds the preset threshold.

The **efm error-code notification enable** command enables an interface to detect EFM errored codes. The local device considers a link faulty if the number of detected errored codes within the detection interval reaches or exceeds the preset threshold. Then the local device generates an alarm, reports the alarm to the NMS, and sends an OAMPDU to notify the peer device of the link failure.

Prerequisites

EFM has been enabled globally and on an interface using the **efm enable** command.

Example

Enable Layer 2 interface GigabitEthernet0/0/1 to detect errored codes.

```
<HUAWEI> system-view
[HUAWEI] efm enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] efm enable
[HUAWEI-GigabitEthernet0/0/1] efm error-code notification enable
Info: Operation succeeded.
```

Enable Layer 3 interface GigabitEthernet0/0/1 to detect errored codes.

```
<HUAWEI> system-view
[HUAWEI] efm enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] efm enable
[HUAWEI-GigabitEthernet0/0/1] efm error-code notification enable
Info: Operation succeeded.
```

12.7.9 efm error-code period

Function

The **efm error-code period** command sets the period for detecting EFM errored codes on an interface.

The **undo efm error-code period** command restores the default period for detecting EFM errored codes on an interface.

By default, the period for detecting EFM errored codes on an interface is 1s.

Format

efm error-code period *period*

undo efm error-code period

Parameters

Parameter	Description	Value
period	Specifies the period for detecting EFM errored codes.	The value is an integer that ranges from 1 to 60, in seconds. The default value is 1s.

Views

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

After the **efm error-code period** *period* command is run to set the period for detecting EFM errored codes, run the **efm error-code notification enable** command to enable an interface to detect EFM errored codes. When the number of detected errored codes during the period reaches or exceeds a preset threshold, the local device generates an alarm and notifies the peer device of the alarm event.

Prerequisites

EFM has been enabled globally using the **efm enable** command.

Example

Set the period for detecting EFM errored codes on Layer 2 interface GigabitEthernet0/0/1 to 20s.

```
<HUAWEI> system-view
[HUAWEI] efm enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] efm error-code period 20
Info: Operation succeeded.
```

Set the period for detecting EFM errored codes on Layer 3 interface GigabitEthernet0/0/1 to 20s.

```
<HUAWEI> system-view
[HUAWEI] efm enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] efm error-code period 20
Info: Operation succeeded.
```

12.7.10 efm error-code threshold

Function

The **efm error-code threshold** command sets the threshold for detecting EFM errored codes on an interface.

The **undo efm error-code threshold** command restores the default threshold for detecting EFM errored codes on an interface.

By default, the threshold for detecting EFM errored codes on an interface is 1.

Format

efm error-code threshold *threshold*

undo efm error-code threshold

Parameters

Parameter	Description	Value
threshold	Specifies the threshold for detecting EFM errored codes.	The value is an integer that ranges from 0 to 65535. The default value is 1. The value 0 is not recommended.

Views

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

After the **efm error-code period** *period* command is executed to set the period for detecting EFM errored codes, run the **efm error-code threshold** *threshold* command to set the threshold for detecting errored codes. Run the **efm error-code notification enable** command to enable an interface to detect EFM errored codes. When the number of detected errored codes during the period reaches or exceeds the threshold specified by *threshold*, the local device generates an alarm and notifies the peer device of the alarm event.

Prerequisites

EFM has been enabled globally using the **efm enable** command.

Example

Set the threshold for detecting EFM errored codes on Layer 2 interfaceGigabitEthernet0/0/1 to 100.


```
<HUAWEI> system-view
[HUAWEI] efm enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] efm error-code threshold 100
Info: Operation succeeded.
```

Set the threshold for detecting EFM errored codes on Layer 3 interface GigabitEthernet0/0/1 to 100.

```
<HUAWEI> system-view
[HUAWEI] efm enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] efm error-code threshold 100
Info: Operation succeeded.
```

12.7.11 efm error-frame notification enable

Function

The **efm error-frame notification enable** command enables an interface to detect EFM errored frames.

The **undo efm error-frame notification enable** command disables an interface from detecting EFM errored frames.

By default, an interface is not enabled to detect EFM errored frames.

Format

efm error-frame notification enable

undo efm error-frame notification enable

Parameters

None

Views

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

Monitoring Ethernet links is difficult if network performance deteriorates while traffic is being transmitted over physical links. Link monitoring is used to detect link layer faults in various environments. After EFM link monitoring is configured, the device queries statistics about the physical layer data of the interface management module to monitor the quality of the link connected to an interface. EFM link monitoring implements the following functions:

- Reports an alarm when the number of errored codes detected during a specified detection interval exceeds the preset threshold.
- Reports an alarm when the number of errored frames detected during a specified detection interval exceeds the preset threshold.
- Reports an alarm when the number of errored frame seconds detected during a specified interval exceeds the preset threshold.

The **efm error-frame notification enable** command enables an interface to detect EFM errored frames. The local device considers a link faulty if the number of detected errored frames within the detection interval reaches or exceeds the preset threshold. Then the local device generates an alarm, reports the alarm to the NMS, and sends an OAMPDU to notify the peer device of the link failure.

Prerequisites

EFM has been enabled globally and on an interface using the **efm enable** command.

Example

Enable Layer 2 interfaceGigabitEthernet0/0/1 to detect errored frames.

```
<HUAWEI> system-view
[HUAWEI] efm enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] efm enable
[HUAWEI-GigabitEthernet0/0/1] efm error-frame notification enable
Info: Operation succeeded.
```

Enable Layer 3 interface GigabitEthernet0/0/1 to detect errored frames.

```
<HUAWEI> system-view
[HUAWEI] efm enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] efm enable
[HUAWEI-GigabitEthernet0/0/1] efm error-frame notification enable
Info: Operation succeeded.
```

12.7.12 efm error-frame period

Function

The **efm error-frame period** command sets the period for detecting EFM errored frames on an interface.

The **undo efm error-frame period** command restores the default period for detecting EFM errored frames on an interface.

By default, the period for detecting EFM errored frames on an interface is 1s.

Format

efm error-frame period *period*

undo efm error-frame period

Parameters

Parameter	Description	Value
period	Specifies the period for detecting EFM errored frames.	The value is an integer that ranges from 1 to 60, in seconds. The default value is 1s.

Views

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

After the **efm error-code period** *period* command is run to set the period for detecting EFM errored frames on an interface, run the **efm error-frame notification enable** command to enable an interface to detect EFM errored frames. When the number of detected errored frames during the period reaches or exceeds a preset threshold, the local device generates an alarm and notifies the peer device of the alarm event.

Prerequisites

EFM has been enabled globally using the **efm enable** command.

Example

Set the period for detecting EFM errored frames on Layer 2 interface GigabitEthernet0/0/1 to 20 seconds.

```
<HUAWEI> system-view
[HUAWEI] efm enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] efm error-frame period 20
Info: Operation succeeded.
```

Set the period for detecting EFM errored frames on Layer 3 interface GigabitEthernet0/0/1 to 20 seconds.

```
<HUAWEI> system-view
[HUAWEI] efm enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] efm error-frame period 20
Info: Operation succeeded.
```

12.7.13 efm error-frame threshold

Function

The **efm error-frame threshold** command sets the threshold for detecting EFM errored frames on an interface.

The **undo efm error-frame threshold** command restores the default threshold for detecting EFM errored frames on an interface.

By default, the threshold for detecting EFM errored frames on an interface is 1.

Format

efm error-frame threshold *threshold*

undo efm error-frame threshold

Parameters

Parameter	Description	Value
threshold	Specifies the threshold for detecting EFM errored frames.	The value is an integer that ranges from 0 to 65535. The default value is 1. The value 0 is not recommended.

Views

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

After the **efm error-frame period** *period* command is executed to set the period for detecting EFM errored frames on an interface, run the **efm error-frame threshold** *threshold* command to set the threshold for detecting errored frames. Run the **efm error-frame notification enable** command to enable an interface to detect EFM errored frames. When the number of detected errored frames during the period reaches or exceeds the threshold specified by *threshold*, the local device generates an alarm and notifies the peer device of the alarm event.

Prerequisites

EFM has been enabled globally using the **efm enable** command.

Example

Set the threshold for detecting EFM errored frames on interface GigabitEthernet0/0/1 to 100.


```
<HUAWEI> system-view
[HUAWEI] efm enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] efm error-frame threshold 100
Info: Operation succeeded.
```

12.7.14 efm error-frame-second notification enable

Function

The **efm error-frame-second notification enable** command enables an interface to detect EFM errored frame seconds.

The **undo efm error-frame-second notification enable** command disables an interface from detecting EFM errored frame seconds.

By default, an interface is not enabled to detect EFM errored frame seconds.

Format

efm error-frame-second notification enable

undo efm error-frame-second notification enable

Parameters

None

Views

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

Monitoring Ethernet links is difficult if network performance deteriorates while traffic is being transmitted over physical links. Link monitoring is used to detect link layer faults in various environments. After EFM link monitoring is configured, the device queries statistics about the physical layer data of the interface management module to monitor the quality of the link connected to an interface. EFM link monitoring implements the following functions:

- Reports an alarm when the number of errored codes detected during a specified detection interval exceeds the preset threshold.
- Reports an alarm when the number of errored frames detected during a specified detection interval exceeds the preset threshold.
- Reports an alarm when the number of errored frame seconds detected during a specified interval exceeds the preset threshold.

The **efm error-frame-second notification enable** command enables an interface to detect EFM errored frame seconds. The local device considers a link faulty if the number of detected errored frame seconds within the detection interval reaches or exceeds the preset threshold. Then the local device generates an alarm, reports the alarm to the NMS, and sends an OAMPDU to notify the peer device of the link failure.

Prerequisites

EFM has been enabled globally and on an interface using the **efm enable** command.

Example

Enable Layer 2 interface GigabitEthernet0/0/1 to detect errored frame seconds.

```
<HUAWEI> system-view
[HUAWEI] efm enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] efm enable
[HUAWEI-GigabitEthernet0/0/1] efm error-frame-second notification enable
Info: Operation succeeded.
```

Enable Layer 3 interface GigabitEthernet0/0/1 to detect errored frame seconds.

```
<HUAWEI> system-view
[HUAWEI] efm enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] efm enable
[HUAWEI-GigabitEthernet0/0/1] efm error-frame-second notification enable
Info: Operation succeeded.
```

12.7.15 efm error-frame-second period

Function

The **efm error-frame-second period** command sets the period for detecting EFM errored frame seconds on an interface.

The **undo efm error-frame-second period** command restores the default period for detecting EFM errored frame seconds on an interface.

By default, the period for detecting EFM errored frame seconds on an interface is 60s.

Format

efm error-frame-second period *period*

undo efm error-frame-second period

Parameters

Parameter	Description	Value
period	Specifies the period for detecting EFM errored frame seconds.	The value is an integer that ranges from 10 to 900, in seconds. The default value is 60s.

Views

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

After the **efm error-frame-second period** *period* command is run to set the period for detecting EFM errored frame seconds on an interface, run the **efm error-frame-second notification enable** command to enable an interface to detect EFM errored frame seconds. When the number of detected errored frame seconds during the period reaches or exceeds a preset threshold, the local device generates an alarm and notifies the peer device of the alarm event.

Prerequisites

EFM has been enabled globally using the **efm enable** command.

Example

Set the period for detecting EFM errored frame seconds on Layer 2 interface GigabitEthernet0/0/1 to 20s.

```
<HUAWEI> system-view
[HUAWEI] efm enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] efm error-frame-second period 20
Info: Operation succeeded.
```

Set the period for detecting EFM errored frame seconds on Layer 3 interface GigabitEthernet0/0/1 to 20s.

```
<HUAWEI> system-view
[HUAWEI] efm enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] efm error-frame-second period 20
Info: Operation succeeded.
```

12.7.16 efm error-frame-second threshold

Function

The **efm error-frame-second threshold** command sets the threshold for detecting EFM errored frame seconds on an interface.

The **undo efm error-frame-second threshold** command restores the default threshold for detecting EFM errored frame seconds on an interface.

By default, the threshold for detecting EFM errored frame seconds on an interface is 1.

Format

efm error-frame-second threshold *threshold*

undo efm error-frame-second threshold

Parameters

Parameter	Description	Value
threshold	Specifies the threshold for detecting EFM errored frame seconds.	The value is an integer that ranges from 0 to 900. The default value is 1. The value 0 is not recommended.

Views

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

After the **efm error-frame-second period** *period* command is executed to set the threshold for detecting EFM errored frame seconds on an interface, run the **efm error-frame-second threshold** *threshold* command to set the threshold for detecting errored frame seconds. Run the **efm error-frame-second notification enable** command to enable an interface to detect EFM errored frame seconds. When the number of detected errored frame seconds during the period reaches or exceeds the threshold specified by *threshold*, the local device generates an alarm and notifies the peer device of the alarm event.

Prerequisites

EFM has been enabled globally using the **efm enable** command.

Example

Set the threshold for detecting EFM errored frame seconds on Layer 2 interface GigabitEthernet0/0/1 to 10.

```
<HUAWEI> system-view
[HUAWEI] efm enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] efm error-frame-second threshold 10
Info: Operation succeeded.
```

Set the threshold for detecting EFM errored frame seconds on Layer 3 interface GigabitEthernet0/0/1 to 10.

```
<HUAWEI> system-view
[HUAWEI] efm enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] efm error-frame-second threshold 10
Info: Operation succeeded.
```

12.7.17 efm holdup-timer

Function

The **efm holdup-timer** command sets the value of the EFM faulty-state holdup timer on an interface.

The **undo efm holdup-timer** command restores the default value interval of the EFM faulty-state holdup timer on an interface.

By default, the value of the EFM faulty-state holdup timer is 0s.

Format

efm holdup-timer *time*

undo efm holdup-timer

Parameters

Parameter	Description	Value
time	Specifies the value of the EFM faulty-state holdup timer on an interface.	The value is an integer that ranges from 0 to 50, in seconds. The default value is 0.

Views

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

After the **efm trigger if-down** command is used to associate EFM with an interface, run the **efm holdup-timer** command to set the value of the EFM faulty-state holdup timer for connectivity faults detected by EFM. The faulty state remains unchanged within the value of the holdup timer. EFM does not detect whether the connectivity fault is cleared until the faulty-state holdup timer expires.

After the failed link recovers, EFM works as follows:

- If *time* is not specified, EFM immediately changes the link status to Up.
- If *time* is specified, EFM changes the link status to Up only after the time specified by *time* expires. This prevents the link from frequently alternating between Up and Down.

Prerequisites

EFM has been enabled globally and on interfaces using the **efm enable** command.

It is recommended that you run the **efm trigger if-down** command to associate EFM with an interface before running the **efm holdup-timer** command to set the value of EFM faulty-state holdup timer on the interface. Otherwise, the holdup timer does not take effect.

Example

Set the value of EFM faulty-state holdup timer on GigabitEthernet0/0/1 to 10s.

```
<HUAWEI> system-view
[HUAWEI] efm enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] efm enable
[HUAWEI-GigabitEthernet0/0/1] efm trigger if-down
[HUAWEI-GigabitEthernet0/0/1] efm holdup-timer 10
```

12.7.18 efm loopback

Function

The **efm loopback** command configures an interface to initiate or end an EFM remote loopback.

Format

efm loopback { **start** [**timeout** *timeout*] | **stop** }

Parameters

Parameter	Description	Value
start	Initiate an EFM remote loopback.	-
timeout *timeout*	Specifies the timeout interval of an EFM remote loopback.	The value is an integer that ranges from 0 to 1000, in minutes. The default value is 20. The value 0 indicates that no timeout interval is set. That is, the interface remains in remote loopback state.
stop	Ends an EFM remote loopback.	-

Views

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

NOTE

The S6735-S, S6720-EI and S6720S-EI can only initiate EFM OAM remote loopback requests.

Usage Scenario

EFM remote loopback is used to locate link failures and test the link quality. After remote loopback is enabled, configure the local device to send test packets to the peer device. Based on the statistics about sent and received test packets, you can check connectivity and performance of a specified link.

- If **start** is specified, an interface on the local device sends a remote loopback message to the peer device. After receiving the message, the peer device enters the loopback state. In loopback state, the peer sends back all received packets, except EFM OAMPDUs, to the local device through the interface that has received these packets.
- If **stop** is specified, an interface on the local device sends a remote loopback stop message to the peer device. After receiving the message, the peer device exits from the loopback state.
- If remote loopback is left enabled, the remote device keeps looping back service data, causing a service interruption. To prevent this problem, a capability can be configured to disable remote loopback automatically after a specified timeout interval. By default, the timeout interval for remote loopback is 20 minutes. The remote loopback test stops after 20 minutes. You can set the timeout interval to 0 to keep a link in remote loopback state.

NOTE

The link in remote loopback state will not forward service data. Therefore, execute caution when you set the timeout interval to 0.

Prerequisites

- EFM has been enabled and is in detect state.
- The device has been configured to work in active mode using the **efm mode active** command.

Precautions

After remote loopback is enabled, all packets except EFM OAMPDUs are looped back on the remote device. EFM OAM remote loopback must be implemented on the link that does not need to forward service data. Otherwise, service data forwarding is affected.

Remote loopback is implemented successfully only when EFM protocols at the local end and the peer are in handshake state and EFM at the local end works in active mode. You can use the **display efm session** command to check whether EFM OAM protocols on the local interface and the peer are in handshake state.

Example

Configure Layer 2 interface GigabitEthernet0/0/1 to initiate an EFM OAM remote loopback.

```
<HUAWEI> system-view
[HUAWEI] efm enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] efm enable
[HUAWEI-GigabitEthernet0/0/1] efm loopback start
```

Set the timeout interval for an EFM OAM remote loopback on Layer 2 interface GigabitEthernet0/0/1.

```
<HUAWEI> system-view
[HUAWEI] efm enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] efm enable
[HUAWEI-GigabitEthernet0/0/1] efm loopback start timeout 10
```

Configure Layer 2 interface GigabitEthernet0/0/1 to stop an EFM OAM remote loopback.

```
<HUAWEI> system-view
[HUAWEI] efm enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] efm enable
[HUAWEI-GigabitEthernet0/0/1] efm loopback stop
```

Configure Layer 3 interface GigabitEthernet0/0/1 to initiate an EFM OAM remote loopback.

```
<HUAWEI> system-view
[HUAWEI] efm enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] efm enable
[HUAWEI-GigabitEthernet0/0/1] efm loopback start
```


Set the timeout interval for an EFM OAM remote loopback on Layer 3 interface GigabitEthernet0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] efm loopback start timeout 10
```

Configure Layer 3 interface GigabitEthernet0/0/1 to stop an EFM OAM remote loopback.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] efm loopback stop
```

12.7.19 efm loopback ignore-request

Function

The **efm loopback ignore-request** command enables an interface to ignore loopback requests sent by the remote end.

The **undo efm loopback ignore-request** command restores the default setting for the loopback function on an interface.

By default, an interface supports remote loopback. After receiving a loopback request from a remote end, the interface enters the loopback state.

Format

efm loopback ignore-request

undo efm loopback ignore-request

Parameters

None

Views

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

Remote loopback is used to monitor link quality and locate link faults. Periodic loopback detection helps detect network faults in a timely manner.

If an interface is in loopback state, the interface loops back all received traffic, causing service interruption and imposing attacks. To solve this problem, run the

efm loopback ignore-request command to enable the interface to reject the remote Ethernet OAM loopback request carried in a Loopback Control OAMPDU sent by a remote interface.

Prerequisites

EFM has been enabled globally and on an interface using the **efm enable** command and the interface is not in loopback state.

Precautions

After the **efm loopback ignore-request** command is run, the interface will discard an OAMPDU carrying a remote loopback request.

Example

Enable Layer 2 interface GigabitEthernet0/0/1 to ignore loopback requests sent by a specified remote interface.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] efm loopback ignore-request
```

Enable Layer 3 interface GigabitEthernet0/0/1 to ignore loopback requests sent by a specified remote interface.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] efm loopback ignore-request
```

12.7.20 efm mode

Function

The **efm mode** command configures the working mode of EFM on an interface.

The **undo efm mode** command restores the default working mode of EFM on an interface.

By default, EFM on an interface works in active mode.

Format

efm mode { **active** | **passive** }

undo efm mode

Parameters

Parameter	Description	Value
active	Indicates that EFM on an interface works in active mode.	-
passive	Indicates that EFM on an interface works in passive mode.	-

Views

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

EFM supports two connection modes: active and passive. By setting the working mode of EFM OAM, you can configure whether a device can send or receive a specified type of EFM OAMPDU. **Table 12-43** describes the differences between the active and passive modes.

Table 12-43 Capabilities for processing OAMPDUs in active and passive modes

Event	Active Mode	Passive Mode
Initiate a connection request by sending an Information OAMPDU during the discovery process	Supported	Not supported
Respond to a connection request during the discovery process	Supported	Supported
Send Information OAMPDUs	Supported	Supported
Send Event Notification OAMPDUs	Supported	Supported
Send Loopback Control OAMPDUs	Supported	Not supported
Respond to Loopback Control OAMPDUs	Supported (The remote EFM entity must work in active mode.)	Supported

Precautions

- The working mode of EFM can be set on an interface only after EFM is enabled globally and before EFM is enabled on the interface. The working mode of EFM on an interface cannot be changed after EFM is enabled on the interface. Before changing the working mode of EFM on an interface, run the **undo efm enable** command to disable EFM on the interface.

- An EFM connection can only be initiated by an OAM entity working in active mode. An OAM entity working in passive mode waits to receive a connection request from its peer entity.
- Two OAM entities both working in passive mode cannot establish an EFM connection between them.

Example

Configure EFM OAM on Layer 2 interface GigabitEthernet0/0/1 to work in passive mode.

```
<HUAWEI> system-view
[HUAWEI] efm enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] efm mode passive
```

Configure EFM OAM on Layer 3 interface GigabitEthernet0/0/1 to work in passive mode.

```
<HUAWEI> system-view
[HUAWEI] efm enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] efm mode passive
```

12.7.21 efm packet max-size

Function

The **efm packet max-size** command sets the maximum size of an EFM OAMPDU on an interface. All EFM OAMPDUs that exceed the maximum size on an interface are discarded as invalid packets.

The **undo efm packet max-size** command restores the default maximum size of an EFM OAMPDU on an interface.

By default, the maximum size of an EFM OAMPDU on an interface is 128 bytes.

Format

efm packet max-size *size*

undo efm packet max-size

Parameters

Parameter	Description	Value
size	Specifies the maximum size of an EFM OAMPDU. The size contains the length of Layer 2 frame header and the length of the cyclic redundancy check (CRC) field.	The value is an integer that ranges from 64 to 1518, in bytes. The default value is 128 bytes.

Views

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

You can run the **efm packet max-size** command to adjust the maximum size of an EFM OAMPDU so that non-Huawei devices can communicate.

Prerequisites

EFM has been enabled globally using the **efm enable** command.

Precautions

The local device and the peer determine the actual value of the maximum size of an EFM OAMPDU through negotiation. The smaller maximum size of an EFM OAMPDU set on the local interface or the peer is used.

Example

Set the maximum size of an EFM OAMPDU on Layer 2 interface GigabitEthernet0/0/1 to 120 bytes.

```
<HUAWEI> system-view
[HUAWEI] efm enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] efm packet max-size 120
```

Set the maximum size of an EFM OAMPDU on Layer 3 interface GigabitEthernet0/0/1 to 120 bytes.

```
<HUAWEI> system-view
[HUAWEI] efm enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] efm packet max-size 120
```

12.7.22 efm src-mac

Function

The **efm src-mac** command configures an interface or bridge MAC address as the source MAC address in an OAMPDU.

The **undo efm src-mac** command restores the default configuration.

By default, a bridge MAC address is used as the source MAC address in an OAMPDU.

Format

efm src-mac { **port** | **bridge** }

undo efm src-mac

Parameters

Parameter	Description	Value
port	Configures an interface MAC address as the source MAC address in an OAMPDU.	-
bridge	Configures a bridge MAC address as the source MAC address in an OAMPDU.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

OAMPDUs support interface or bridge MAC addresses as source MAC addresses. You can run the **efm src-mac** command to configure an interface or bridge MAC address as the source MAC address in an OAMPDU before enabling EFM globally.

Example

Configure an interface MAC address as the source MAC address in an OAMPDU.

```
<HUAWEI> system-view
[HUAWEI] efm src-mac port
```

12.7.23 efm timeout

Function

The **efm timeout** command sets the timeout interval at which EFM OAMPDUs are received.

The **undo efm timeout** command restores the default timeout interval.

By default, the timeout interval at which EFM OAMPDUs are received is 5000 milliseconds.

Format

efm timeout *timeout-value*

undo efm timeout

Parameters

Parameter	Description	Value
timeout-value	Specifies the timeout interval at which an interface receives EFM OAMPDUs.	The value is an integer that ranges from 3000 to 30000, in milliseconds. The step is 1000 milliseconds. The default value is 5000 milliseconds.

Views

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 setting the timeout interval at which OAMPDUs are received, you can change the time required for connectivity fault detection.

Prerequisites

EFM OAM has been enabled globally but is not enabled on an interface.

Precautions

After the timeout interval expires, the EFM OAM protocol switches back to the discovery state. Ensure that interfaces on both ends of a link use the same timeout interval. Otherwise, EFM session negotiation may fail, or the EFM session may flap.

After EFM OAM is enabled on an interface, the timeout interval cannot be changed.

- A shorter timeout interval indicates a shorter time required for connectivity fault detection.
- A longer timeout interval indicates a longer time required for connectivity fault detection.

Example

Set the timeout interval at which EFM OAMPDUs are received on Layer 2 interface GigabitEthernet0/0/1 to 3000 ms.

```
<HUAWEI> system-view
[HUAWEI] efm enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] efm timeout 3000
```

Set the timeout interval at which EFM OAMPDUs are received on Layer 3 interface GigabitEthernet0/0/1 to 3000 ms.


```
<HUAWEI> system-view
[HUAWEI] efm enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] efm timeout 3000
```

12.7.24 efm threshold-event trigger error-down

Function

The **efm threshold-event trigger error-down** command associates an EFM threshold crossing event with an interface.

The **undo efm threshold-event trigger error-down** command disassociates an EFM threshold crossing event from an interface.

By default, a threshold crossing event is not associated with an interface.

Format

efm threshold-event trigger error-down

undo efm threshold-event trigger error-down

Parameters

None

Views

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

When link monitoring is configured for an interface on a link, the link is considered unavailable, if the number of errored frames, errored codes, or errored frame seconds detected by the interface reaches or exceeds the threshold within a period. In this case, you can run the **efm threshold-event trigger error-down** command to associate a threshold crossing event with an interface so that the system sets the administrative state of the interface to Down. As a result, all services on the interface are interrupted.

Prerequisites

EFM has been enabled on an interface using the **efm enable** command.

Follow-up Procedure

Configure the interface to go administratively Up by using either of the following methods:

- Run the **error-down auto-recovery** command to set the auto-recovery delay before an interface goes administratively Up.
- Run the **shutdown** command and then the **undo shutdown** command to restore the administrative state of the interface to Up.

Example

Associate a threshold crossing event with Layer 2 interface GigabitEthernet0/0/1.

```
<HUAWEI> system-view
[HUAWEI] efm enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] efm enable
[HUAWEI-GigabitEthernet0/0/1] efm threshold-event trigger error-down
```

Associate a threshold crossing event with Layer 3 interface GigabitEthernet0/0/1.

```
<HUAWEI> system-view
[HUAWEI] efm enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] efm enable
[HUAWEI-GigabitEthernet0/0/1] efm threshold-event trigger error-down
```

12.7.25 efm trigger clear-arp vlan

Function

The **efm trigger clear-arp vlan** command clears an ARP entry corresponding to a VLANIF interface.

The **undo efm trigger clear-arp vlan** command cancels the configuration.

By default, an interface does not clear an ARP entry.

Format

efm trigger clear-arp vlan *vlan-id*

undo efm trigger clear-arp vlan *vlan-id*

Parameters

Parameter	Description	Value
vlan-id	Specifies the VLAN ID in an ARP entry.	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, port group view

NOTE

The **efm trigger clear-arp vlan** command takes effect only on Layer 2 Ethernet interfaces.

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When detecting a fault, the EFM module notifies the OAM management module of the fault. The OAM management module searches the EFM fault relationship table based on the interface number and VLAN ID, and then clears the ARP entry that corresponds to the VLANIF interface.

Prerequisites

EFM has been enabled globally and on an interface using the **efm enable** command.

Example

Enable GigabitEthernet0/0/1 in VLAN 10 to clear ARP entries.

```
<HUAWEI> system-view
[HUAWEI] efm enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] efm enable
[HUAWEI-GigabitEthernet0/0/1] efm trigger clear-arp vlan 10
```

12.7.26 efm trigger error-down

Function

The **efm trigger error-down** command associates an error event with an interface.

The **undo efm trigger error-down** command disassociates an error event from an interface.

By default, an error event is not associated with an interface.

Format

efm { **critical-event** | **dying-gasp** | **link-fault** | **timeout** } **trigger error-down**

undo efm { **critical-event** | **dying-gasp** | **link-fault** | **timeout** } **trigger error-down**

Parameters

Parameter	Description	Value
critical-event	Indicates an unspecified critical event. It usually refers to a fault on the interface associated with MGR.	-
dying-gasp	Indicates an unrecoverable failure. It usually refers to device restart or power-off.	-
link-fault	Indicates a physical link fault. It usually refers to a fault on an interface.	-
timeout	Indicates the timeout interval at which EFM OAMPDUs are received.	-

Views

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

When EFM OAM associated with an interface detects a connectivity fault on a link, the protocol status of the interface goes Down. The interface goes Up after the faulty link recovers.

After the **efm trigger error-down** command is used, the administrative status of the interface goes Down when EFM OAM detects remote **critical-event**, **dying-gasp**, or **link-fault** events, or local **timeout** event. Traffic will not be switched back after the faulty link recovers. Check link quality before switching traffic back to the original link.

Prerequisites

EFM OAM has been enabled globally and on an interface using the **efm enable** command.

Follow-up Procedure

When the protocols status of an interface goes Down because error events are associated with the interface. The protocol status of the interface will not go Up even if the faulty link recovers. In this case, perform either of the following operations:

- Run the **restart (interface view)** command to restart the interface.
- Run the **shutdown (interface view)** and **undo shutdown (interface view)** commands to manually restore the interface.

- Run the **undo efm trigger error-down** command to disable association between error events and an interface.

To configure the shutdown interface to go Up automatically, run the **error-down auto-recovery cause efm-remote-failure interval** *interval-value* command in the system view to enable an interface to go Up and set a recovery delay before the interface enters the error-down state. The interface goes Up automatically after the delay.

Precautions

An interface can be associated with various types of error events. For example, if both **efm critical-event trigger error-down** and **efm dying-gasp trigger error-down** are used, the protocol status of the interface becomes Down when the device receives EFM OAM packets indicating **critical-event** or **dying-gasp** faults.

- Dying Gasp fault notification function supports models such as **Table 12-44** shows.

Table 12-44 Models that support Dying Gasp fault notification

Device Series	Model **Unless otherwise specified:** • **The models listed in the table can send Dying Gasp messages to the remote device and send Dying Gasp alarms (EFM_1.3.6.1.4.1.2011.5.25.136.1.6.5_hwDot3ahEfmNonThresholdEvent) to the NMS.** • **All interfaces of the device can send Dying Gasp fault notification.**
S5720-LI	All models support except S5720-16X-PWH-LI-AC, S5720-28P-LI-AC, S5720-28P-PWR-LI-AC, S5720-28X-PWH-LI-AC, S5720-52P-LI-AC, S5720-52P-PWR-LI-AC, S5720-52X-PWR-LI-ACF
S5720S-LI	S5720S-12TP-LI-AC, S5720S-12TP-PWR-LI-AC, S5720S-28TP-PWR-LI-ACL, and S5720S-28X-LI-24S-AC **NOTE** • They can send Dying Gasp messages to the remote device only, but cannot send Dying Gasp alarms to the NMS. • A maximum of 30 interfaces can send Dying Gasp messages.
S5720I-SI	All models
S5735-L	All models
S5735S-L	All models support except S5735S-L48P4S-A and S5735S-L48P4X-A
S5735-L1	S5735-L24P4X-A1, S5735-L24T4X-A1, S5735-L24T4X-D1, S5735-L24T4X-QA1, S5735-L32ST4X-A1, S5735-L32ST4X-D1, S5735-L48T4X-A1, S5735-L8P4X-A1, and S5735-L8T4X-A1 support

Device Series	Model Unless otherwise specified: • The models listed in the table can send Dying Gasp messages to the remote device and send Dying Gasp alarms (EFM_1.3.6.1.4.1.2011.5.25.136.1.6.5_hwDot3ahEfmNonThresholdEvent) to the NMS. • All interfaces of the device can send Dying Gasp fault notification.
S5735S-L1	S5735S-L32ST4X-A1 support
S5735S-L-M	All models
S5735-L-I	All models
S500-32ST4X	S500-32ST4X support

- The **efm critical-event trigger error-down** command is used and the remote interface associated with MGR goes Down. The local device will set the protocol status of the corresponding interface to Down after receiving an EFM OAM packet indicating a **critical-event** fault.
- The **efm dying-gasp trigger error-down** command is used and the board where the remote interface resides is reset or the system restarts. The local device will set the protocol status of the corresponding interface to Down after receiving an EFM OAM packet indicating a **dying-gasp** fault.
- The **efm link-fault trigger error-down** command is used and the physical link of the remote device is faulty. The local device will set the protocol status of the corresponding interface to Down after receiving an EFM OAM packet indicating a **link-fault** fault.
- The **efm timeout trigger error-down** command is used on the local device. The local device will set the protocol status of the corresponding interface to Down if it does not receive packets from the remote device in a specified period of time (5s by default).

NOTE

The **efm trigger if-down** and **efm trigger error-down** commands cannot be used simultaneously, and the **efm trigger mac-renew** and **efm trigger error-down** commands cannot be used simultaneously.

Example

Associate **dying-gasp** faults with Layer 2 interface GigabitEthernet0/0/1.

```
<HUAWEI> system-view
[HUAWEI] efm enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] efm enable
[HUAWEI-GigabitEthernet0/0/1] efm dying-gasp trigger error-down
```

Associate **dying-gasp** faults with Layer 3 interface GigabitEthernet0/0/1.


```
<HUAWEI> system-view
[HUAWEI] efm enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] efm enable
[HUAWEI-GigabitEthernet0/0/1] efm dying-gasp trigger error-down
```

12.7.27 efm trigger if-down

Function

The **efm trigger if-down** command associates EFM with an interface.

The **undo efm trigger if-down** command disassociates EFM from an interface.

By default, EFM OAM is not associated with any interface.

Format

efm trigger if-down

undo efm trigger if-down

Parameters

None

Views

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

EFM can be associated with interfaces. On a scenario with primary and backup links, if EFM detects a fault on the primary link, it will set the protocol status of the associated interface to ETHOAM Down, speeding up routing convergence. Traffic can be fast switched to the backup link.

Prerequisites

EFM has been enabled globally and on an interface, and is in detect state.

Precautions

If EFM is associated with an interface and detects a link fault, the protocol status of the interface becomes ETHOAM Down, and no packet except EFM OAMPDUs can be forwarded by the interface, and all Layer 2 and Layer 3 services are blocked. Therefore, associating EFM with an interface may greatly affect services. When the interface detects link recovery using EFM, the interface can forward all packets and unblocks Layer 2 and Layer 3 services.

If Layer 2 and Layer 3 services are blocked due to a misoperation, run the **undo efm trigger if-down** command in the interface view to restore services.

Example

Associate EFM with Layer 2 interface GigabitEthernet0/0/1.

```
<HUAWEI> system-view
[HUAWEI] efm enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] efm enable
[HUAWEI-GigabitEthernet0/0/1] efm trigger if-down
```

Associate EFM with Layer 3 interface GigabitEthernet0/0/1.

```
<HUAWEI> system-view
[HUAWEI] efm enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] efm enable
[HUAWEI-GigabitEthernet0/0/1] efm trigger if-down
```

12.7.28 efm trigger mac-renew

Function

The **efm trigger mac-renew** command configures the device to clear the MAC address table on a physical interface.

The **undo efm trigger mac-renew** command cancels the configuration.

By default, an interface is not enabled to clear the MAC address table.

Format

efm trigger mac-renew

undo efm trigger mac-renew

Parameters

None

Views

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

NOTE

The **efm trigger mac-renew** command takes effect only on Layer 2 Ethernet interfaces.

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When you need to configure the device to clear the MAC address table on a physical interface, run the **efm trigger mac-renew** command.

Precautions

EFM has been enabled globally and on an interface using the **efm enable** command.

NOTE

The **efm trigger mac-renew** and **efm trigger if-down** commands cannot be used simultaneously on an interface.

Example

Configure GigabitEthernet0/0/1 to delete the corresponding MAC entry after a fault notification is received.

```
<HUAWEI> system-view
[HUAWEI] efm enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] efm enable
[HUAWEI-GigabitEthernet0/0/1] efm trigger mac-renew
```

12.7.29 oam-bind efm interface efm interface

Function

The **oam-bind efm interface efm interface** command enables bidirectional fault notification between EFM modules.

The **undo oam-bind efm interface efm interface** command cancels the configuration.

By default, bidirectional transmission of information about a fault between EFM OAM sessions is not configured.

NOTE

Only the S5720I-SI, S5735-S, S5735S-S, S5735-S-I, S5735S-H, S5736-S, and S6720S-S support this function.

Format

oam-bind efm interface *interface-type interface-number* **efm interface** *interface-type interface-number*

undo oam-bind efm interface *interface-type interface-number* **efm interface** *interface-type interface-number*

Parameters

Parameter	Description	Value
interface-type interface-number	Specifies the type and the number of an interface configured with bidirectional fault notification between EFM modules. • *interface-type* specifies the interface type. • *interface-number* specifies the interface number.	-

Views

OAM management view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If EFM is deployed at both sides of a device, associate EFM modules on the device to ensure reliable service transmission.

Association between EFM and EFM is bidirectional. EFM modules notify each other of faults.

The following commands are used to associate EFM modules:

- **oam-bind efm interface efm interface**
- **oam-bind ingress efm interface egress efm interface**

Choose the preceding commands in different scenarios according to **Table 12-45**.

Table 12-45 Association between EFM modules

Scenario	Configuration Solution 1	Configuration Solution 2
Bidirectional fault notification between EFM modules	Run the **oam-bind efm interface efm interface** command.	Use the following commands: • Run the **oam-bind ingress efm interface egress efm interface** command to configure EFM for the link at one side of the device to notify EFM for the link at the other side of the device of faults. **ingress efm interface** *interface-type interface-number* specifies the EFM-capable interface on the link at one side of the device, and **egress efm interface** *interface-type interface-number* specifies the EFM-capable interface on the link at the other side of the device. • Run the **oam-bind ingress efm interface egress efm interface** command to configure EFM for the link at one side of the device to notify EFM for the link at the other side of the device of faults. **ingress efm interface** *interface-type interface-number* specifies the EFM-capable interface on the link at one side of the device, and **egress efm interface** *interface-type interface-number* specifies the EFM-capable interface on the link at the other side of the device.

Scenario	Configuration Solution 1	Configuration Solution 2
Unidirectional fault notification between EFM sessions	Choose either of the following commands based on the transmission direction: • Run the **oam-bind ingress efm interface egress efm interface** command to configure EFM for the link at one side of the device to notify EFM for the link at the other side of the device of faults. **ingress efm interface** *interface-type interface-number* specifies the EFM-capable interface on the link at one side of the device, and **egress efm interface** *interface-type interface-number* specifies the EFM-capable interface on the link at the other side of the device. • Run the **oam-bind ingress efm interface egress efm interface** command to configure EFM for the link at one side of the device to notify EFM for the link at the other side of the device of faults. **ingress efm interface** *interface-type interface-number* specifies the EFM-capable interface on the link at one side of the device, and **egress efm interface** *interface-type interface-number* specifies the EFM-capable interface on the link at the other side of the device.	None

Prerequisites

The following conditions must be met:

- EFM OAM has been enabled on specified interfaces.
- Two EFM OAM sessions have been associated with each other. When an EFM OAM session is associated with another EFM OAM session, the EFM OAM session cannot be associated with other EFM OAM sessions.

Example

Configure bidirectional fault notification between EFM OAM sessions.

```
<HUAWEI> system-view
[HUAWEI] oam-mgr
[HUAWEI-oam-mgr] oam-bind efm interface gigabitethernet0/0/1 efm interface gigabitethernet0/0/2
```

12.7.30 oam-bind efm interface trigger if-down interface

Function

The **oam-bind efm interface trigger if-down interface** command enables bidirectional fault notification between EFM and an interface.

The **undo oam-bind efm interface trigger if-down interface** command cancels the configuration.

By default, bidirectional transmission of information about a fault between EFM OAM and an interface is not configured.

Format

oam-bind efm interface *interface-type1 interface-number1* **trigger if-down interface** *interface-type2 interface-number2*

undo oam-bind efm interface *interface-type1 interface-number1* **trigger if-down interface** *interface-type2 interface-number2*

Parameters

Parameter	Description	Value
interface-type1 interface-number1	Specifies the type and number of the interface enabled with EFM. ● *interface-type1* specifies the interface type. ● *interface-number1* specifies the interface number.	-
interface-type2 interface-number2	Specifies the type and number of the interface bound to an EFM session. ● *interface-type2* specifies the interface type. ● *interface-number2* specifies the interface number.	-

Views

OAM management view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Association between EFM and an interface in the OAM management view is bidirectional:

- After EFM OAM detects a fault, the OAM module notifies the interface associated with EFM OAM of the fault. Then the interface goes Down. After EFM detects that the fault is rectified, the OAM module notifies the interface associated with EFM OAM. Then the interface goes Up.
- After the interface goes Down, the OAM module notifies EFM OAM of the interface Down event.
- A physical interface associated with EFM cannot be the one that EFM monitors. If EFM is associated with a physical interface that it monitors, the link is locked.

The following commands are used to configure association between EFM and an interface in the OAM management view:

- **oam-bind efm interface trigger if-down interface**
- **oam-bind interface efm interface trigger if-down**
- **oam-bind ingress efm interface trigger if-down egress interface**
- **oam-bind ingress interface egress efm interface trigger if-down**

Table 12-46 describes the implementation of association between EFM and an interface.

Table 12-46 Association between EFM and an EFM-incapable interface

Scenario	Configuration Solution 1	Configuration Solution 2
Bidirectional fault notification between EFM and an interface	Choose either of the following commands (the two commands have the same function): • To specify an EFM OAM session first, run the **oam-bind efm interface trigger if-down interface** command. • To specify an interface first, run the **oam-bind interface efm interface trigger if-down** command. **NOTE** After configuring bidirectional fault notification between EFM and an interface, run the **display current-configuration** command to view the current configuration. The **display current-configuration** command displays **oam-bind ingress interface egress efm interface trigger if-down** and **oam-bind ingress efm interface trigger if-down egress interface** commands, but does not display the **oam-bind efm interface trigger if-down interface** or **oam-bind interface efm interface trigger if-down** command. The displayed commands configure reverse transmission directions of fault information.	Run the following commands at a random order: • **oam-bind ingress efm interface trigger if-down egress interface** • **oam-bind ingress interface egress efm interface trigger if-down**
Unidirectional fault notification between EFM and an interface	Choose either of the following commands based on the transmission direction: • To configure EFM OAM to report faults to an interface, run the **oam-bind ingress efm interface trigger if-down egress interface** command. • To configure an interface to report faults to EFM OAM, run the **oam-bind ingress interface egress efm interface trigger if-down** command.	None

Precautions

When configuring bidirectional fault notification between EFM and an interface, pay attention to the following points:

- EFM has been enabled on the interface specified by **efm interface** *interface-type1 interface-number1*.

- EFM and an interface are associated with each other. After an interface is associated with an EFM session, the interface cannot be associated with other EFM sessions. Similarly, when EFM is bound to an interface, EFM cannot be bound to other interfaces.

Example

Configure bidirectional fault notification between an EFM session and GigabitEthernet0/0/1.

```
<HUAWEI> system-view
[HUAWEI] oam-mgr
[HUAWEI-oam-mgr] oam-bind efm interface gigabitethernet 0/0/1 trigger if-down interface gigabitethernet 0/0/2
```

12.7.31 oam-bind ingress efm interface egress efm interface

Function

The **oam-bind ingress efm interface egress efm interface** command enables an EFM OAM session to report faults to another EFM OAM session.

The **undo oam-bind ingress efm interface egress efm interface** command disables an EFM OAM session from reporting faults to another EFM OAM session.

By default, unidirectional transmission of information about a fault from one EFM OAM session to another EFM OAM session is not configured.

NOTE

Only the S5720I-SI, S5735-S, S5735S-S, S5735-S-I, S5735S-H, S5736-S, and S6720S-S support this function.

Format

oam-bind ingress efm interface *interface-type1 interface-number1* **egress efm interface** *interface-type2 interface-number2*

undo oam-bind ingress efm interface *interface-type1 interface-number1* **egress efm interface** *interface-type2 interface-number2*

Parameters

Parameter	Description	Value
interface-type1 interface-number1	Specifies the type and number of the interface enabled with EFM OAM. • *interface-type1* specifies the interface type. • *interface-number1* specifies the interface number.	-

Parameter	Description	Value
interface-type2 interface-number2	Specifies the type and number of the interface bound to an EFM OAM session. • *interface-type2* specifies the interface type. • *interface-number2* specifies the interface number.	-

Views

OAM management view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If EFM is deployed at both sides of a device, associate EFM modules on the device to ensure reliable service transmission.

Association between EFM and EFM is bidirectional. EFM modules notify each other of faults.

The following commands are used to associate EFM modules:

- **oam-bind efm interface efm interface**
- **oam-bind ingress efm interface egress efm interface**

Choose the preceding commands in different scenarios according to **Table 12-47**.

Table 12-47 Association between EFM modules

Scenario	Configuration Solution 1	Configuration Solution 2
Bidirectional fault notification between EFM modules	Run the **oam-bind efm interface efm interface** command.	Use the following commands: • Run the **oam-bind ingress efm interface egress efm interface** command to configure EFM for the link at one side of the device to notify EFM for the link at the other side of the device of faults. **ingress efm interface** *interface-type interface-number* specifies the EFM-capable interface on the link at one side of the device, and **egress efm interface** *interface-type interface-number* specifies the EFM-capable interface on the link at the other side of the device. • Run the **oam-bind ingress efm interface egress efm interface** command to configure EFM for the link at one side of the device to notify EFM for the link at the other side of the device of faults. **ingress efm interface** *interface-type interface-number* specifies the EFM-capable interface on the link at one side of the device, and **egress efm interface** *interface-type interface-number* specifies the EFM-capable interface on the link at the other side of the device.

Scenario	Configuration Solution 1	Configuration Solution 2
Unidirectional fault notification between EFM sessions	Choose either of the following commands based on the transmission direction: • Run the **oam-bind ingress efm interface egress efm interface** command to configure EFM for the link at one side of the device to notify EFM for the link at the other side of the device of faults. **ingress efm interface** *interface-type interface-number* specifies the EFM-capable interface on the link at one side of the device, and **egress efm interface** *interface-type interface-number* specifies the EFM-capable interface on the link at the other side of the device. • Run the **oam-bind ingress efm interface egress efm interface** command to configure EFM for the link at one side of the device to notify EFM for the link at the other side of the device of faults. **ingress efm interface** *interface-type interface-number* specifies the EFM-capable interface on the link at one side of the device, and **egress efm interface** *interface-type interface-number* specifies the EFM-capable interface on the link at the other side of the device.	None

Precautions

Ingress EFM OAM reports faults to egress EFM OAM.

Example

Configure an EFM OAM session to report faults to another EFM OAM session.

```
<HUAWEI> system-view
[HUAWEI] oam-mgr
```


[HUAWEI-oam-mgr] **oam-bind ingress efm interface gigabitethernet 0/0/1 egress efm interface gigabitethernet 0/0/2**

12.7.32 oam-bind ingress efm interface trigger if-down egress interface

Function

The **oam-bind ingress efm interface trigger if-down egress interface** command enables EFM to report faults to an interface.

The **undo oam-bind ingress efm interface trigger if-down egress interface** command cancels the configuration.

By default, unidirectional transmission of information about a fault from EFM OAM to an interface is not configured.

Format

oam-bind ingress efm interface *interface-type1 interface-number1* **trigger if-down egress interface** *interface-type2 interface-number2*

undo oam-bind ingress efm interface *interface-type1 interface-number1* **trigger if-down egress interface** *interface-type2 interface-number2*

Parameters

Parameter	Description	Value
interface-type1 interface-number1	Specifies the type and number of the interface enabled with EFM. ● *interface-type1* specifies the interface type. ● *interface-number1* specifies the interface number.	-
interface-type2 interface-number2	Specifies the type and number of the interface bound to an EFM session. ● *interface-type2* specifies the interface type. ● *interface-number2* specifies the interface number.	-

Views

OAM management view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Association between EFM and an interface in the OAM management view is bidirectional:

- After EFM OAM detects a fault, the OAM module notifies the interface associated with EFM OAM of the fault. Then the interface goes Down. After EFM detects that the fault is rectified, the OAM module notifies the interface associated with EFM OAM. Then the interface goes Up.
- After the interface goes Down, the OAM module notifies EFM OAM of the interface Down event.
- A physical interface associated with EFM cannot be the one that EFM monitors. If EFM is associated with a physical interface that it monitors, the link is locked.

The following commands are used to configure association between EFM and an interface in the OAM management view:

- **oam-bind efm interface trigger if-down interface**
- **oam-bind interface efm interface trigger if-down**
- **oam-bind ingress efm interface trigger if-down egress interface**
- **oam-bind ingress interface egress efm interface trigger if-down**

Table 12-48 describes the implementation of association between EFM and an interface.

Table 12-48 Association between EFM and an EFM-incapable interface

Scenario	Configuration Solution 1	Configuration Solution 2
Bidirectional fault notification between EFM and an interface	Choose either of the following commands (the two commands have the same function): • To specify an EFM OAM session first, run the **oam-bind efm interface trigger if-down interface** command. • To specify an interface first, run the **oam-bind interface efm interface trigger if-down** command. **NOTE** After configuring bidirectional fault notification between EFM and an interface, run the **display current-configuration** command to view the current configuration. The **display current-configuration** command displays **oam-bind ingress interface egress efm interface trigger if-down** and **oam-bind ingress efm interface trigger if-down egress interface** commands, but does not display the **oam-bind efm interface trigger if-down interface** or **oam-bind interface efm interface trigger if-down** command. The displayed commands configure reverse transmission directions of fault information.	Run the following commands at a random order: • **oam-bind ingress efm interface trigger if-down egress interface** • **oam-bind ingress interface egress efm interface trigger if-down**

Scenario	Configuration Solution 1	Configuration Solution 2
Unidirectional fault notification between EFM and an interface	Choose either of the following commands based on the transmission direction: • To configure EFM OAM to report faults to an interface, run the **oam-bind ingress efm interface trigger if-down egress interface** command. • To configure an interface to report faults to EFM OAM, run the **oam-bind ingress interface egress efm interface trigger if-down** command.	None

Precautions

Before enabling EFM to report faults to an interface, pay attention to the following points:

- EFM has been enabled on the interface specified by **efm interface** *interface-type2 interface-number2*.
- EFM and the interface are associated with each other. After an interface is associated with an EFM session, the interface cannot be associated with other EFM sessions. Similarly, when EFM is bound to an interface, EFM cannot be bound to other interfaces.

Ingress EFM reports faults to the specified interface.

Example

Configure EFM to report a fault to GigabitEthernet0/0/2.

```
<HUAWEI> system-view
[HUAWEI] oam-mgr
[HUAWEI-oam-mgr] oam-bind ingress efm interface gigabitethernet 0/0/1 trigger if-down egress interface gigabitethernet 0/0/2
```

12.7.33 oam-bind ingress interface egress efm interface trigger if-down

Function

The **oam-bind ingress interface egress efm interface trigger if-down** command enables an interface to report faults to EFM OAM.

The **undo oam-bind ingress interface egress efm interface trigger if-down** command cancels the configuration.

By default, unidirectional transmission of information about a fault from an interface to EFM OAM is disabled.

Format

oam-bind ingress interface *interface-type1 interface-number1* **egress efm interface** *interface-type2 interface-number2* **trigger if-down**

undo oam-bind ingress interface *interface-type1 interface-number1* **egress efm interface** *interface-type2 interface-number2* **trigger if-down**

Parameters

Parameter	Description	Value
interface-type1 interface-number1	Specifies the type and number of the interface enabled with EFM. ● *interface-type1* specifies the interface type. ● *interface-number1* specifies the interface number.	-
interface-type2 interface-number2	Specifies the type and number of the interface bound to an EFM OAM session. ● *interface-type2* specifies the interface type. ● *interface-number2* specifies the interface number.	-

Views

OAM management view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If an inward MEP is configured, bidirectional association between EFM and an EFM-incapable interface of a device can be configured in the OAM management view. This ensures that service traffic can be switched to the backup link if the primary link fails.

Association between EFM and an interface in the OAM management view is bidirectional:

- After EFM OAM detects a fault, the OAM module notifies the interface associated with EFM OAM of the fault. Then the interface goes Down. After EFM detects that the fault is rectified, the OAM module notifies the interface associated with EFM OAM. Then the interface goes Up.
- After the interface goes Down, the OAM module notifies EFM OAM of the interface Down event.

The following commands are used to configure association between EFM and an interface in the OAM management view:

- **oam-bind efm interface trigger if-down interface**
- **oam-bind interface efm interface trigger if-down**
- **oam-bind ingress efm interface trigger if-down egress interface**
- **oam-bind ingress interface egress efm interface trigger if-down**

Table 12-49 describes the implementation of association between EFM and an interface.

Table 12-49 Association between EFM and an EFM-incapable interface

Scenario	Configuration Solution 1	Configuration Solution 2
Bidirectional fault notification between EFM and an interface	Choose either of the following commands (the two commands have the same function): • To specify an EFM OAM session first, run the **oam-bind efm interface trigger if-down interface** command. • To specify an interface first, run the **oam-bind interface efm interface trigger if-down** command. **NOTE** After configuring bidirectional fault notification between EFM and an interface, run the **display current-configuration** command to view the current configuration. The **display current-configuration** command displays **oam-bind ingress interface egress efm interface trigger if-down** and **oam-bind ingress efm interface trigger if-down egress interface** commands, but does not display the **oam-bind efm interface trigger if-down interface** or **oam-bind interface efm interface trigger if-down** command. The displayed commands configure reverse transmission directions of fault information.	Run the following commands at a random order: • **oam-bind ingress efm interface trigger if-down egress interface** • **oam-bind ingress interface egress efm interface trigger if-down**
Unidirectional fault notification between EFM and an interface	Choose either of the following commands based on the transmission direction: • To configure EFM OAM to report faults to an interface, run the **oam-bind ingress efm interface trigger if-down egress interface** command. • To configure an interface to report faults to EFM OAM, run the **oam-bind ingress interface egress efm interface trigger if-down** command.	None

Configuration Impact

After an interface goes Down, the status of the associated EFM OAM session does not change. However, the device configured with association sends a message to inform the peer of the fault and triggers the peer to generate an alarm.

Precautions

Before enabling an interface to report faults to EFM OAM, pay attention to the following points:

- EFM has been enabled on the interface specified by **efm interface** *interface-type2 interface-number2*.
- EFM and an interface are associated with each other. After an interface is associated with an EFM session, the interface cannot be associated with other EFM sessions. Similarly, when EFM is bound to an interface, EFM cannot be bound to other interfaces.

The ingress interface reports faults to egress EFM.

Example

Configure GigabitEthernet0/0/1 to report a fault to EFM.

```
<HUAWEI> system-view
[HUAWEI] oam-mgr
[HUAWEI-oam-mgr] oam-bind ingress interface gigabitethernet 0/0/1 egress efm interface gigabitethernet 0/0/2 trigger if-down
```

12.7.34 oam-bind interface efm interface trigger if-down

Function

The **oam-bind interface efm interface trigger if-down** command enables bidirectional transmission of fault messages between an interface and EFM OAM.

The **undo oam-bind interface efm interface trigger if-down** command cancels the configuration.

By default, bidirectional transmission of information about a fault between an interface and EFM OAM is not configured.

Format

oam-bind interface *interface-type1 interface-number1* **efm interface** *interface-type2 interface-number2* **trigger if-down**

undo oam-bind interface *interface-type1 interface-number1* **efm interface** *interface-type2 interface-number2* **trigger if-down**

Parameters

Parameter	Description	Value
interface-type1 interface-number1	Specifies the type and number of the interface enabled with EFM. • *interface-type1* specifies the interface type. • *interface-number1* specifies the interface number.	-
interface-type2 interface-number2	Specifies the type and number of the interface bound to an EFM session. • *interface-type2* specifies the interface type. • *interface-number2* specifies the interface number.	-

Views

OAM management view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If an inward MEP is configured, bidirectional association between EFM and an EFM-incapable interface of a device can be configured in the OAM management view. This ensures that service traffic can be switched to the backup link if the primary link fails.

Association between EFM and an interface in the OAM management view is bidirectional:

- After EFM OAM detects a fault, the OAM module notifies the interface associated with EFM OAM of the fault. Then the interface goes Down. After EFM detects that the fault is rectified, the OAM module notifies the interface associated with EFM OAM. Then the interface goes Up.
- After the interface goes Down, the OAM module notifies EFM OAM of the interface Down event.

The following commands are used to configure association between EFM and an interface in the OAM management view:

- **oam-bind efm interface trigger if-down interface**
- **oam-bind interface efm interface trigger if-down**
- **oam-bind ingress efm interface trigger if-down egress interface**
- **oam-bind ingress interface egress efm interface trigger if-down**

Table 12-50 describes the implementation of association between EFM and an interface.

Table 12-50 Association between EFM and an EFM-incapable interface

Scenario	Configuration Solution 1	Configuration Solution 2
Bidirectional fault notification between EFM and an interface	Choose either of the following commands (the two commands have the same function): • To specify an EFM OAM session first, run the **oam-bind efm interface trigger if-down interface** command. • To specify an interface first, run the **oam-bind interface efm interface trigger if-down** command. **NOTE** After configuring bidirectional fault notification between EFM and an interface, run the **display current-configuration** command to view the current configuration. The **display current-configuration** command displays **oam-bind ingress interface egress efm interface trigger if-down** and **oam-bind ingress efm interface trigger if-down egress interface** commands, but does not display the **oam-bind efm interface trigger if-down interface** or **oam-bind interface efm interface trigger if-down** command. The displayed commands configure reverse transmission directions of fault information.	Run the following commands at a random order: • **oam-bind ingress efm interface trigger if-down egress interface** • **oam-bind ingress interface egress efm interface trigger if-down**
Unidirectional fault notification between EFM and an interface	Choose either of the following commands based on the transmission direction: • To configure EFM OAM to report faults to an interface, run the **oam-bind ingress efm interface trigger if-down egress interface** command. • To configure an interface to report faults to EFM OAM, run the **oam-bind ingress interface egress efm interface trigger if-down** command.	None

Prerequisites

Basic EFM OAM functions have been configured.

Precautions

When configuring bidirectional transmission of fault messages between EFM and an interface, pay attention to the following points:

- EFM has been enabled on the interface specified by **efm interface** *interface-type2 interface-number2*.
- EFM and the interface are associated with each other. After an interface is associated with an EFM session, the interface cannot be associated with other EFM sessions. Similarly, when EFM is bound to an interface, EFM cannot be bound to other interfaces.
- Association between EFM and an EFM-capable interface and association between EFM and an EFM-incapable interface cannot be configured together.
- A physical interface associated with EFM cannot be the one that EFM monitors. If EFM is associated with a physical interface that it monitors, the link is locked.

Example

Configure bidirectional transmission of fault messages between EFM and GigabitEthernet0/0/1.

```
<HUAWEI> system-view
[HUAWEI] oam-mgr
[HUAWEI-oam-mgr] oam-bind interface gigabitethernet 0/0/1 efm interface gigabitethernet 0/0/2 trigger if-down
```

12.7.35 oam-mgr

Function

The **oam-mgr** command displays the OAM management view.

The **undo oam-mgr** command exits from the OAM management view.

Format

oam-mgr

undo oam-mgr

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

CFM can advertise fault information to interfaces or protocol modules. Ethernet OAM fault advertisement is implemented by an OAM manager, application modules, and detection modules. An OAMMGR module associates one module

with another. A detection module monitors link status and network performance. If a detection module detects a fault, it instructs the OAMMGR module to notify an application module or another detection module of the fault. After receiving the notification, the application or detection module takes measures to prevent a communication interruption or service quality deterioration. Run the **oam-mgr** command to display the MGR view before associating the CFM module and other modules.

Example

Enter the OAM management view.

```
<HUAWEI> system-view
[HUAWEI] oam-mgr
[HUAWEI-oam-mgr]
```

12.7.36 test-packet start

Function

The **test-packet start** command configures the device to send test packets.

Format

test-packet start interface *interface-type interface-number* [**-c** *count* | **-s** *size*] *

Parameters

Parameter	Description	Value
interface-type interface-number	Specifies the outbound interface of test packets. • *interface-type* specifies the interface type. • *interface-number* specifies the interface number.	-
-c *count*	Specifies the number of test packets to be sent.	The value is an integer that ranges from 1 to 65535. The default value is 5.
-s *size*	Specifies the length of a test packet.	The value is an integer that ranges from 64 to 1518, in bytes. The default value is 64 bytes.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After remote loopback is enabled on the device, run the **test-packet start** command on an interface in active mode to configure the device to send test packets. Then check link connectivity and performance based on returned test packets.

Press **Ctrl+C** to stop sending test packets. After using this command to send test packets, use the **display test-packet result** command to view the test result.

Precautions

During test packet transmission, parameters of sent test packets cannot be changed.

Example

Send test packets from outbound interface GigabitEthernet0/0/1.
<HUAWEI> **system-view**
[HUAWEI] **test-packet start interface gigabitethernet 0/0/1**

12.8 CFM Configuration Commands

12.8.1 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.

12.8.2 active time

Function

The **active time** command sets the RMEP activation time.

The **undo active time** command deletes the RMEP activation time.

By default, the RMEP activation time is 0 seconds.

Format

active time *time*

undo active time

Parameters

Parameter	Description	Value
time *time*	Specifies the RMEP activation time.	The value ranges from 0 to 600, in seconds.

Views

MA view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After you run the **remote-mep ccm-receive enable** command to enable the local device to receive CCMs from an RMEP in the same MA, the local device generates an RMEP connectivity fault alarm in the following situations:

- A connectivity fault is detected between the local MEP and the RMEP using CC.
- The physical link works normally between the local MEP and the RMEP. The remote device is not configured with a MEP when connectivity check is performed or the MEP configuration is later than connectivity check. In this case, if the local MEP does not receive the CCM from the RMEP in consecutive three intervals for sending CCMs, the local device considers that a connectivity fault occurs between the local MEP and the RMEP.

  The RMEP connectivity fault alarm is generated incorrectly. To solve the problem, set the RMEP activation time.

Precautions

IEEE 802.1ag has two versions: IEEE 802.1ag Draft 7 and IEEE Standard 802.1ag-2007. This command can be used only on the device running IEEE Standard 802.1ag-2007.

If the RMEP activation time is set on the local device that is enabled to receive CCMs from a certain RMEP, the local device can receive CCMs at the configured RMEP activation time. That is, the activation time is the time reserved for configuring the RMEP.

At the RMEP activation time, if the local MEP does not receive any CCMs in three consecutive sending intervals, a connectivity fault occurs between the local MEP and the RMEP. Then the local device generates an alarm about the RMEP connectivity fault.

If the local device uses the default RMEP activation time, the local MEP receives CCMs from the RMEP immediately after the local device is enabled to receive CCMs from the RMEP.

NOTE

The RMEP activation time takes effect only for subsequent RMEPs in an MA, but is invalid for existing RMEPs in the MA.

Example

Set the RMEP activation time to 30s.

```
<HUAWEI> system-view
[HUAWEI] cfm md md1
[HUAWEI-md-md1] ma ma1
[HUAWEI-md-md1-ma-ma1] active time 30
```

12.8.3 alarm finish time

Function

The **alarm finish time** command sets the clear alarm anti-jitter time.

The **undo alarm finish time** command restores the default clear alarm anti-jitter time.

By default, the clear alarm anti-jitter time is 10000 ms.

Format

alarm finish time *time*

undo alarm finish time

Parameters

Parameter	Description	Value
time *time*	Specifies the clear alarm anti-jitter time.	The value ranges from 0 to 30000, in milliseconds. The step is 500, for example, the anti-jitter time can be 500, 1000, or 1500.

Views

MA view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When detecting a link fault or link recovery, CFM will send an alarm to the NMS. If CFM frequently detects a link fault or link recovery, alarm flapping occurs. To

suppress alarm flapping, run the **alarm finish time** command to set the clear alarm anti-jitter time. This prevents the NMS or system from being affected by frequently reported alarms.

Precautions

IEEE 802.1ag has two versions: IEEE 802.1ag Draft 7 and IEEE Standard 802.1ag-2007. This command can be used only on the device running IEEE Standard 802.1ag-2007.

When detecting link recovery, CFM compares the current link recovery time with the last time the fault was generated. CFM sends an alarm to the NMS only when the time difference is not smaller than the clear alarm anti-jitter time.

Example

Set the clear alarm anti-jitter time to 2000 ms.

```
<HUAWEI> system-view
[HUAWEI] cfm md md1
[HUAWEI-md-md1] ma ma1
[HUAWEI-md-md1-ma-ma1] alarm finish time 2000
```

12.8.4 alarm occur time

Function

The **alarm occur time** command sets the alarm anti-jitter time.

The **undo alarm occur time** command restores the default alarm anti-jitter time.

By default, the alarm anti-jitter time is 2500 ms.

Format

alarm occur time *time*

undo alarm occur time

Parameters

Parameter	Description	Value
time *time*	Specifies the alarm anti-jitter time.	The value ranges from 0 to 30000, in milliseconds. The step is 500, for example, the anti-jitter time can be 500, 1000, or 1500.

Views

MA view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When detecting a link fault or link recovery, CFM will send an alarm to the NMS. If CFM frequently detects a link fault or link recovery, alarm flapping occurs. To suppress alarm flapping, run the **alarm occur time** command to set the alarm anti-jitter time. This prevents the NMS or system from being affected by frequently reported alarms.

Precautions

IEEE 802.1ag has two versions: IEEE 802.1ag Draft 7 and IEEE Standard 802.1ag-2007. This command can be used only on the device running IEEE Standard 802.1ag-2007.

When detecting a fault, CFM compares the current fault generation time with the last time the fault was rectified. CFM sends an alarm to the NMS only when the time difference is not smaller than the alarm anti-jitter time.

Example

Set the alarm anti-jitter time to 2000 ms.

```
<HUAWEI> system-view
[HUAWEI] cfm md md1
[HUAWEI-md-md1] ma ma1
[HUAWEI-md-md1-ma-ma1] alarm occur time 2000
```

12.8.5 alarm rdi track-action disable

Function

The **alarm rdi track-action disable** command disables CFM from being triggered when an RDI alarm is generated.

The **undo alarm rdi track-action disable** command enables CFM to be triggered when an RDI alarm is generated.

By default, CFM is triggered when an RDI alarm is generated.

Format

alarm rdi track-action oam-mgr disable

undo alarm rdi track-action oam-mgr disable

Parameters

Parameter	Description	Value
oam-mgr	Indicates that CFM is associated with another feature in the OAM management view.	-

Views

MA view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When CFM is associated with other functions such as EFM and the device receives an RDI alarm, run the **alarm rdi track-action disable** command to disable CFM from being triggered.

Prerequisites

An MD has been created using the **cfm md** *md-name* command, and an MA has been created using the **ma** *ma-name* command.

Example

Disable CFM from being triggered in the OAM MGR view when an RDI alarm is generated.

```
<HUAWEI> system-view
[HUAWEI] cfm md md1
[HUAWEI-md-md1] ma ma1
[HUAWEI-md-md1-ma-ma1] alarm rdi track-action oam-mgr disable
```

12.8.6 alarm suppression track-action oam-mgr enable

Function

The **alarm suppression track-action oam-mgr enable** command configures the function of disabling the MGR module from being notified upon processing of LOC alarms in scenarios where both LOC clear alarms and RDI fault alarms exist.

The **undo alarm suppression track-action oam-mgr enable** command disables this function.

By default, this function is disabled on a device.

Format

alarm suppression track-action oam-mgr enable

undo alarm suppression track-action oam-mgr enable

Parameters

None

Views

MA view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In scenarios where both LOC clear alarms and RDI fault alarms are generated on a device, to prevent link flapping, you can configure the device not to notify the MGR module upon processing of LOC clear alarms. Instead, the device reports LOC clear alarms when processing RDI fault alarms.

Precautions

You are advised to run this command only in scenarios where CFM is associated with an interface bidirectionally. Otherwise, fault recovery performance may be affected.

Example

Disable the MGR module from being notified of LOC clear alarms in scenarios where both LOC clear alarms and RDI fault alarms are generated on a device.

```
<HUAWEI> system-view
[HUAWEI] cfm enable
[HUAWEI] cfm md md1
[HUAWEI-md-md1] ma ma1
[HUAWEI-md-md1-ma-ma1] alarm suppression track-action oam-mgr enable
```

12.8.7 ccm-interval

Function

The **ccm-interval** command sets the interval at which a Maintenance Association End Point (MEP) sends or detects Continuity Check Messages (CCMs) in an MA.

The **undo ccm-interval** command restores the default interval.

By default, a MEP in an MA sends or detects CCMs every 1000 ms.

Format

ccm-interval *interval*

undo ccm-interval

Parameters

Parameter	Description	Value
interval	Specifies the interval at which a MEP sends or detects CCMs.	The value is an integer, in milliseconds. The value is as follows: • S6735-S, S6720-EI and S6720S-EI: 100, 1000, or 10000 • S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S: 3.3, 10, 100, 1000, or 10000 To use the value of 3.3 or 10, first run the **set service-mode** command to configure the device to work in enhanced mode. • 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: 1000 or 10000

Views

MA view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To set the interval at which a MEP in an MA sends or detects CCMs, use this command.

Precautions

All the MEPs in an MA must send or detect CCMs at the same interval.

The interval at which CCMs are sent or detected cannot be changed on the device in an MA if one of the following operations is performed:

- The device is enabled to send CCMs using the **mep ccm-send enable** command.
- The device is enabled to receive CCMs using the **remote-mep ccm-receive enable** command.

The **undo mep ccm-send** or **undo mep ccm-receive** command must be run before the interval is reconfigured.

Example

Set the interval for sending or detecting CCMs to 1000 ms within the MA **ma1** where the device is not enabled to send or receive CCMs.

```
<HUAWEI> system-view
[HUAWEI] cfm enable
[HUAWEI] cfm md md1
[HUAWEI-md-md1] ma ma1
[HUAWEI-md-md1-ma-ma1] ccm-interval 1000
```

Set the interval for sending or detecting CCMs to 1000 ms within the MA **ma1** where the device is enabled to send and receive CCMs.

```
<HUAWEI> system-view
[HUAWEI] cfm enable
[HUAWEI] cfm md md1
[HUAWEI-md-md1] ma ma1
[HUAWEI-md-md1-ma-ma1] undo mep ccm-send enable
[HUAWEI-md-md1-ma-ma1] undo remote-mep ccm-receive enable
[HUAWEI-md-md1-ma-ma1] ccm-interval 1000
```

12.8.8 cfm default md

Function

The **cfm default md** command creates the default MD.

The **undo cfm default md** command deletes the default MD.

By default, the default MD is not created.

Format

cfm default md [**level** *level*]

undo cfm default md

Parameters

Parameter	Description	Value
level *level*	Specifies the level of the default MD.	The value is an integer that ranges from 0 to 7. A larger value indicates a higher MD priority. By default, the level of the default MD is 7 (highest level).

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To identify and locate faults on an MP or a link in an MD, create the default MD.

Precautions

IEEE 802.1ag has two versions: IEEE 802.1ag Draft 7 and IEEE Standard 802.1ag-2007. This command can be used only on the device running IEEE Standard 802.1ag-2007.

The level of the default MD must be higher than that of all MDs to which MEPs configured on the local device belong. In addition, the default MD must be of the same level as the higher-level MD. The default MD transmits higher-level CCMs and creates MIPs to send LTR messages.

On the device configured with the default MD, a MIP can be created based on the default MD in the MA that is not associated with a VLAN. The interface where the default MD is configured generates a MIP based on the MIP creation rule.

To modify the MD level, delete the default MD and reconfigure it.

Prerequisites

CFM has been enabled globally using the **cfm enable (system view)** command.

Example

Create the default MD at level 6.

```
<HUAWEI> system-view
[HUAWEI] cfm enable
[HUAWEI] cfm default md level 6
```

12.8.9 cfm destination-mac

Function

The **cfm destination-mac** command configures the destination MAC address of a CCM.

The **undo cfm destination-mac** command restores the default setting.

As defined in IEEE 802.1ag/Draft 7.0, the default destination MAC address of a CCM is 0180-C2FF-FFF0.

Format

cfm destination-mac *mac-address*

undo cfm destination-mac

Parameters

Parameter	Description	Value
mac-address	Specifies the destination MAC address of a CCM.	The value is in the format of H-H-H. A MAC address must start with 0180-c2 and end with 0, and the last three bytes must be greater than 2F. The default value is 0180-C2FF-FFF0.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

No specific multicast MAC address is defined in IEEE 802.1ag/Draft 7.0, so devices of different vendors may send CCMs with different multicast MAC addresses. To allow devices of different vendors to interconnect, you must use the same multicast MAC address on these devices. Otherwise, CCMs cannot be transmitted between these devices.

Prerequisites

- The **cfm enable** command has been run to enable CFM globally.
- The **cfm version draft7** command has been run to switch the Ethernet CFM version to IEEE 802.1ag Draft 7.

Example

Set the destination MAC address of a CCM to 0180-C210-FFF0.

```
<HUAWEI> system-view
[HUAWEI] cfm enable
[HUAWEI] cfm version draft7
[HUAWEI] cfm destination-mac 0180-c210-fff0
```

12.8.10 cfm enable (system view)

Function

The **cfm enable** command enables Connectivity Fault Management (CFM) globally.

The **undo cfm enable** command disables CFM globally.

By default, CFM is disabled globally.

Format

cfm enable

undo cfm enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To identify and locate faults on links, enable CFM globally.

Precautions

After you use the **undo cfm enable** command to disable CFM globally, the device automatically deletes all the CFM configurations, including the configurations of MDs, MAs, MEPs, MIPs, and RMEPs.

All the configuration commands related to the CFM function are valid only after CFM is enabled globally.

Example

Enable CFM globally.

```
<HUAWEI> system-view
[HUAWEI] cfm enable
```

12.8.11 cfm if-down trigger ccm-send-stop

Function

The **cfm if-down trigger ccm-send-stop** command triggers the MEP on an interface to stop sending CCMs when the interface goes Down.

The **undo cfm if-down trigger ccm-send-stop** command restores the default configuration.

By default, the MEP on an interface is not triggered to stop sending CCMs when the interface goes Down.

Format

cfm if-down trigger ccm-send-stop

undo cfm if-down trigger ccm-send-stop

Parameters

None

Views

Interface view

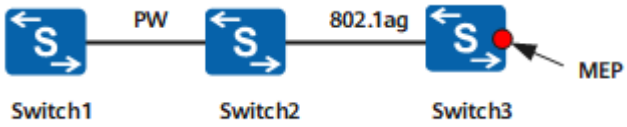
Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Figure 12-1 VLAN stacking scenario with an inward-facing MEP configured



As shown in **Figure 12-1**, in a VLAN stacking scenario with an inward-facing MEP configured, a VLL is configured between Switch1 and Switch2, 802.1ag detection is configured between Switch2 and Switch3, and the MEP on Switch3 is inward-facing. If the interface where the MEP resides goes Down, to prevent the MEP from continuing to send CCMs so that other services can detect the fault information detected by CC, run the **cfm if-down trigger ccm-send-stop** command in the interface view.

Prerequisites

Run the **cfm enable** command to enable CFM globally.

Example

Trigger the MEP on GE 0/0/1 to stop sending CCMs when the interface goes Down.

```
<HUAWEI> system-view
[HUAWEI] cfm enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] cfm if-down trigger ccm-send-stop
```

12.8.12 cfm md

Function

The **cfm md** command creates an MD and displays the MD view, or displays the view of an existing MD.

The **undo cfm md** command deletes an MD.

Format

cfm md *md-name* [**format** { **no-md-name** | **dns** *dns-md-format-name* | **mac-address** *mac-md-format-name* | **string** *string-md-format-name* }] [**level** *level*]

undo cfm md [*md-name*]

Parameters

Parameter	Description	Value
md *md-name*	Specifies the name of an MD.	The value is a string of 1 to 43 case-sensitive characters without spaces, hyphens (-), and question marks (?). The name of an MD on a device must be unique. **NOTE** When double quotation marks are used around the string, spaces are allowed in the string.
no-md-name	Indicates that the MA ID field of a sent packet does not contain an MD name.	-
dns *dns-md-format-name*	Specifies the DNS name used as the MD name carried in packets.	The value is a string of 1 to 43 case-sensitive characters without spaces, hyphens (-), and question marks (?).
mac-address *mac-md-format-name*	Specifies an MD name carried in packets, in the format of H-H-H:U<0-65535>, for example, 0001-0001-0001:1.	The value is a string of 1 to 43 case-sensitive characters without spaces, hyphens (-), and question marks (?).
string *string-md-format-name*	Specifies an ASCII MD name.	The value is a string of 1 to 43 case-sensitive characters without spaces, hyphens (-), and question marks (?).
level *level*	Specifies the level of an MD.	The value is an integer that ranges from 0 to 7. A larger value indicates a higher MD priority. The default value is 0.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To configure CFM to identify and locate faults on links, use this command to create an MD.

Precautions

All the CFM-enabled devices of an ISP can be added to the same MD.

NOTE

When 802.1ag packets in a low-level MD enter a high-level MD, the 802.1ag packets will be discarded. 802.1ag packets in a high-level MD can traverse a low-level MD. 802.1ag packets in an MD cannot traverse the MD of the same level.

Only IEEE Standard 802.1ag-2007 supports **format**, **no-md-name**, **dns** *dns-md-format-name*, **mac-address** *mac-md-format-name*, and **string** *string-md-format-name*.

The MD name format can be specified during the MD configuration, as defined in IEEE Standard 802.1ag-2007. Each MD can be configured with only one name format and one level. You can use the **cfm md** command to enter the view of the existing MD but cannot change the name format and level of the existing MD. To change the name format and level of the existing MD, delete the MD and then use the **cfm md** command to create a new MD.

As defined in IEEE 802.1ag Draft 7, after creating an MD, you cannot use the **cfm md** command to change the level of the MD. To change the level of the MD, you need to delete the MD and then create an MD again.

When an MD is deleted, a device automatically deletes all the configurations of MAs, MEPs, MIPs, and RMEPs within the MD.

The MA, MEP, and RMEP must be created within an MD, so you must create an MD before creating the MA, MEP, and RMEP.

Prerequisites

CFM has been enabled globally using the **cfm enable (system view)** command.

Example

Create an MD named **mdcustomer** at level 4.

```
<HUAWEI> system-view
[HUAWEI] cfm enable
[HUAWEI] cfm md mdcustomer level 4
```

Change the level of **mdcustomer** from 4 to 6.

```
<HUAWEI> system-view
[HUAWEI] undo cfm md mdcustomer
```



```
Warning: Deleting the MD(s) will delete all information about the MA(s). Continue?[Y/N]:y
[HUAWEI] cfm md mdcustomer level 6
```

Create an MD named **mdcustomer** at level 4, with the MD name in **no-md-name** format.

```
<HUAWEI> system-view
[HUAWEI] cfm enable
[HUAWEI] cfm md mdcustomer format no-md-name level 4
```

12.8.13 cfm mip

Function

The **cfm mip level** command creates a MIP on an interface.

The **undo cfm mip** command deletes a MIP on an interface.

By default, no MIP is created.

Format

cfm mip level *level-value*

undo cfm mip

Parameters

Parameter	Description	Value
level *level-value*	Specifies the level of a MIP.	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, MultiGE interface view, Eth-Trunk interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To identify and locate faults on an MP or a link in an MD, create a MIP in the MD.

A MIP is located inside the MD. It can process and respond to CCMs, but cannot send CCMs. When a MIP receives a packet carrying a level higher than its own, the MIP does not process the packet and forwards it along the original path. A MIP forwards only the packet in which the level is lower than or equal to its own.

If a MIP is created and an MP performs LB or LT, the MIP will reply with LBMs or LTMs to identify and locate faults for the MP or link in the MD.

A MIP can be created manually or automatically:

- The **cfm mip level** *level-value* command can be used to manually create a MIP. This configuration is simple, but it is difficult to manage many MIPs and configuration errors may occur.
- The **mip create-type (MD view)** command can be used to define the rule for creating a MIP and enable the device to automatically create a MIP based on the rule. Configuring creation rules is complex, but properly configured rules ensure correct MIP settings.

Prerequisites

CFM has been enabled globally using the **cfm enable (system view)** command.

Precautions

Only IEEE Std 802.1ag-2007 supports the manual MIP configuration.

Example

Create a MIP at level 4.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] cfm mip level 4
```

12.8.14 cfm portid-tlv type

Function

The **cfm portid-tlv type** command sets the portid-tlv type for trace packets.

The **undo cfm portid-tlv type** command restores the default portid-tlv type for trace packets.

By default, the portid-tlv type in trace packets is in character string format.

Format

cfm portid-tlv type { **interface-name** | **local** }

undo cfm portid-tlv type

Parameters

Parameter	Description	Value
interface-name	Indicates that the portid-tlv type is in character string format.	-
local	Indicates that the portid-tlv type is in Huawei proprietary format.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When using the trace function, you need to specify the type of inbound and outbound interface names. You can use the **cfm portid-tlv type** command to set the type of interface names.

Precautions

NOTE

IEEE 802.1ag has two versions: IEEE 802.1ag Draft 7 and IEEE Standard 802.1ag-2007. This command can be used only on the device running IEEE Standard 802.1ag-2007. Before using the **cfm portid-tlv type** command, you must use the **cfm version** command to set the Ethernet CFM version to IEEE Standard 802.1ag-2007.

Vendors may use different TLV types. To implement interworking between Huawei and non-Huawei devices, configure **interface-name** to specify the interface name type in character string format.

If all the devices running on the entire network are Huawei data communications devices, to interwork with devices running different versions, configure **local** to specify the interface name type in Huawei proprietary format.

Example

Configure the portid-tlv type in character string format.

```
<HUAWEI> system-view
[HUAWEI] cfm portid-tlv type interface-name
```

12.8.15 cfm protocol

Function

The **cfm protocol** command configures the EtherType value of a CCM.

The **undo cfm protocol** command restores the default setting.

As defined in IEEE 802.1ag/Draft 7, the default EtherType value of a CCM is 0xBBB0.

Format

cfm protocol *ethertype-value*

undo cfm protocol

Parameters

Parameter	Description	Value
ethertype-value	Specifies the EtherType value of a CCM.	The value is an integer that ranges from 0600 to FFFF. The default value is BBB0.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

No specific protocol type is defined in IEEE 802.1ag/Draft 7, so devices of different vendors may use different protocols to encapsulate CCMs. To allow devices of different vendors to interwork with each other, you must run the **cfm protocol** command to configure the same protocol types on these devices. Otherwise, these devices cannot communicate.

NOTE

You must run the **cfm enable** command to enable CFM globally before configuring the protocol type.

Example

Set the EtherType value of a CCM to 0900.

```
<HUAWEI> system-view
[HUAWEI] cfm protocol 0900
```

12.8.16 cfm trigger if-down

Function

The **cfm trigger if-down** command associates Ethernet CFM with an interface.

The **undo cfm trigger if-down** command disassociates Ethernet CFM from an interface.

By default, an interface is not associated with Ethernet CFM.

Format

cfm md *md-name* **ma** *ma-name* **remote-mep mep-id** *mep-id* **trigger if-down**

undo cfm md *md-name* **ma** *ma-name* **remote-mep mep-id** *mep-id* **trigger if-down**

Parameters

Parameter	Description	Value
md *md-name*	Specifies the name of an MD in an MA.	The value is a string of 1 to 43 case-sensitive characters without spaces, hyphens (-), and question marks (?). **NOTE** When double quotation marks are used around the string, spaces are allowed in the string.
ma *ma-name*	Specifies the name of an MA.	The value is a string of 1 to 43 characters without spaces, hyphens (-), and question marks (?). The total length of the names of the MA and MD must be within 44 characters. **NOTE** When double quotation marks are used around the string, spaces are allowed in the string.
remote-mep mep-id *mep-id*	Specifies ID of an 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, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

CFM can be associated with interfaces. On a scenario with active and standby links, when CFM detects a fault on the active link, the OAM management module shuts down the interface and enables the interface 7 seconds later. This speeds up route convergence. In addition, traffic can be fast switched to the standby link.

Precautions

An interface can be bound to only one RMEP. To modify the association between the interface and the RMEP, delete the current configuration and then configure the new association.

Prerequisites

An outward-facing MEP has been created in the specified MA and the MEP has been created on the interface.

Example

Associate Ethernet CFM with GigabitEthernet0/0/1. The MD name, MA name, and RMEP ID are **md1**, **ma1**, and 2 respectively.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] cfm md md1 ma ma1 remote-mep mep-id 2 trigger if-down
```

12.8.17 cfm trigger clear-arp vlan

Function

The **cfm trigger clear-arp vlan** command clears an ARP entry corresponding to a VLANIF interface.

The **undo cfm trigger clear-arp vlan** command cancels the configuration.

By default, an interface is disabled from clearing an ARP entry.

Format

cfm md *md-name* **ma** *ma-name* **trigger clear-arp vlan** *vlan-id*

undo cfm md *md-name* **ma** *ma-name* **trigger clear-arp vlan** *vlan-id*

Parameters

Parameter	Description	Value
md *md-name*	Specifies the name of an MD in an MA.	The value is a string of 1 to 43 case-sensitive characters without spaces, hyphens (-), and question marks (?). **NOTE** When double quotation marks are used around the string, spaces are allowed in the string.

Parameter	Description	Value
ma *ma-name*	Specifies the name of an MA.	The value is a string of 1 to 43 characters without spaces, hyphens (-), and question marks (?). The total length of the names of the MA and MD must be within 44 characters. **NOTE** When double quotation marks are used around the string, spaces are allowed in the string.
vlan *vlan-id*	Specifies the VLAN ID in an ARP entry.	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, Eth-Trunk interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When detecting a fault, the CM module notifies the OAM management module of the fault. The OAM management module searches the CM fault relationship table based on the interface number and VLAN ID, and then clears the ARP entry that corresponds to the VLANIF interface.

Precautions

Before associating Ethernet CFM with an interface, you must create an outward-facing MEP in the specified MA and ensure that the MEP is on the interface.

Prerequisites

CFM has been enabled globally using the **cfm enable (system view)** command.

Example

Enable GigabitEthernet0/0/1 to clear an ARP entry matching VLANIF 10 after receiving a fault notification.


```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] cfm md md1 ma ma1 trigger clear-arp vlan 10
```

12.8.18 cfm trigger vlan mac-renew

Function

The **cfm trigger vlan mac-renew** command clears MAC address entries of a range of VLANs associated with Ethernet CFM after Ethernet CFM detects a fault.

The **undo cfm trigger vlan mac-renew** command cancels the configuration.

Format

cfm trigger vlan { { *vlan-id* [**to** *vlan-id*] } &<1-10> } **mac-renew**

undo cfm trigger vlan { { *vlan-id* [**to** *vlan-id*] } &<1-10> } **mac-renew**

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
vlan-id	Specifies the ID of a VLAN.	The value is an integer that ranges from 1 to 4094.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the **cfm trigger vlan mac-renew** command is run, CFM deletes MAC address entries of a range of configured VLANs when detecting a fault so that services can be switched between links.

Precautions

A maximum of 10 VLAN ranges can be configured. The VLAN ranges cannot overlap.

When CFM detects a fault in a VLAN associated with the MA in the range specified in this command, the MAC address entries of this VLAN are deleted. If a

fault is detected in a VLAN out of the specified range, the MAC address entries of this VLAN are not deleted.

If the **cfm trigger vlan mac-renew** command is run multiple times, MAC addresses of VLANs specified by the commands are deleted.

Example

Configure the device to clear MAC address entries of VLANs 100 to 200 after CFM detects a fault.

```
<HUAWEI> system-view
[HUAWEI] cfm trigger vlan 100 to 200 mac-renew
```

12.8.19 cfm version

Function

The **cfm version** command switches an Ethernet CFM version between IEEE 802.1ag Draft 7 and IEEE Standard 802.1ag-2007.

The **undo cfm version** command restores the default Ethernet CFM version.

By default, IEEE Standard 802.1ag-2007 is enabled on a device.

Format

cfm version { **draft7** | **standard** }

undo cfm version

Parameters

Parameter	Description	Value
draft7	Indicates IEEE 802.1ag Draft 7.	-
standard	Indicates IEEE Standard 802.1ag-2007.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You need to switch IEEE 802.1ag between the two versions when the device supports both IEEE 802.1ag Draft 7 and IEEE Standard 802.1ag-2007.

Precautions

To ensure that CFM works properly, all devices on the entire network must run IEEE 802.1ag of the same version. During switching between IEEE 802.1ag Draft 7 and IEEE Standard 802.1ag-2007, all 802.1ag functions are unavailable. You can run the **cfm enable (system view)** command to enable CFM globally only after all devices use the same IEEE 802.1ag version.

Example

Switch IEEE Standard 802.1ag-2007 to IEEE 802.1ag Draft 7.

```
<HUAWEI> system-view
[HUAWEI] cfm version draft7
```

12.8.20 display cfm default md

Function

The **display cfm default md** command displays information about the default MD.

Format

display cfm default md

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

You can use the **display cfm default md** command to view information about the level of the default MD, MIP creation rule, Sender ID TLV type, and IDs of VLANs associated with the default MD.

Prerequisites

CFM has been enabled globally using the **cfm enable (system view)** command.

Precautions

IEEE 802.1ag has two versions: IEEE 802.1ag Draft 7 and IEEE Standard 802.1ag-2007. This command can be used only on the device running IEEE Standard 802.1ag-2007.

Example

Display information about the default MD.

```
<HUAWEI> display cfm default md
Level   MIP-Create-type   SenderID TLV-type   VLAN-List
------------------------------------------------------------------------------
7       default           defer             100 to 200 2049
```

Table 12-51 Description of the **display cfm default md** command output

Item	Description
Level	Level of the default MD. The value ranges from 0 to 7. A higher level represents a higher priority of the default MD.
MIP-Create-type	MIP creation rule: • default • explicit • none
SenderID TLV-type	Type of the Sender ID TLV filled in the CCM: • none • chassis • manage • chassisManage • defer
VLAN-List	IDs of VLANs associated with the default MD.

12.8.21 display cfm error-info

Function

The **display cfm error-info** command displays the incorrect configuration of the specified error type.

Format

display cfm error-info error-type unexpected-mep [**md** *md-name* **ma** *ma-name* **mep-id** *mep-id*]

Parameters

Parameter	Description	Value
error-type unexpected-mep	Indicates the error about an unexpected MEP ID.	-

Parameter	Description	Value
md *md-name*	Specifies the name of an MD.	The value is a string of 1 to 43 case-sensitive characters without spaces, hyphens (-), and question marks (?). The name of an MD is unique. **NOTE** When double quotation marks are used around the string, spaces are allowed in the string.
ma *ma-name*	Specifies the name of an MA.	The value is a string of 1 to 43 characters without spaces, hyphens (-), and question marks (?). The total length of the names of the MA and MD must be within 44 characters. **NOTE** When double quotation marks are used around the string, spaces are allowed in the string.
mep-id *mep-id*	Specifies the ID of a MEP. The ID identifies a MEP. The MEP ID must be unique in an MA and in a VLAN.	The value is an integer that ranges from 1 to 8191.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

If CFM cannot work properly, run the **display cfm error-info** command to check received CCMs with unknown MEP IDs. The information helps diagnose a fault.

- If no parameter is configured in the **display cfm error-info** command, the device displays CCMs with unexpected MEP IDs received by all MEPs.

- If an MD name, an MA name, or a MEP ID is specified, the device displays CCMs with unexpected MEP IDs received by a specified MEP.

Prerequisites

CFM has been enabled globally using the **cfm enable (system view)** command.

Precautions

IEEE 802.1ag has two versions: IEEE 802.1ag Draft 7 and IEEE Standard 802.1ag-2007. This command can be used only on the device running IEEE Standard 802.1ag-2007.

Example

Display information about received CCMs with unexpected MEP IDs saved on the device.

```
<HUAWEI> display cfm error-info error-type unexpected-mep
 The total number of unexpected MEPs is : 1
------------------------------------------------------
 MD Name            : md
 Level              : 0
 MA Name            : ma
 MEP ID             : 1
 Unexpected MEP List:
 Unexpected MEP ID  : 2
 MAC Address        : 00e0-fc44-81a4
```

Table 12-52 Description of the **display cfm error-info** command output

Item	Description
MD Name	MD name in CCMs.
Level	Level of an MA.
MA Name	MA name in CCMs.
MEP ID	ID of a MEP in CCMs.
Unexpected MEP List	Unexpected MEP information.
Unexpected MEP ID	Unexpected MEP ID.
MAC Address	MAC address in CCMs.

12.8.22 display cfm ma

Function

The **display cfm ma** command displays detailed information about an MA.

Format

display cfm ma [**md** *md-name* [**ma** *ma-name*]]

Parameters

Parameter	Description	Value
md *md-name*	Displays detailed MA information in a specified MD. *md-name* specifies the name of the MD. If the parameter is not specified, detailed information about all MAs in all MDs is displayed.	The value is a string of 1 to 43 case-sensitive characters without spaces, hyphens (-), and question marks (?). **NOTE** When double quotation marks are used around the string, spaces are allowed in the string.
ma *ma-name*	Displays detailed information about the specified MA. *ma-name* specifies the name of the MA. If *md-name* is specified but this parameter is not specified, detailed information about all the MAs in the specified MD is displayed.	The value is a string of 1 to 43 case-sensitive characters without spaces, hyphens (-), and question marks (?). **NOTE** When double quotation marks are used around the string, spaces are allowed in the string.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

After an MA is configured or CFM cannot work properly, use the **display cfm ma** command to check the MA configuration and the number of MEPs and RMEPs in the MA.

Example

Display detailed information about the MA named **ma1** in the MD named **md1**.

```
<HUAWEI> display cfm ma md md1 ma ma1
 MD Name           : md1
 MD Name Format    : string
 Level             : 0
 MIP Create-type   : none
 SenderID TLV-type : defer
 MA Name           : ma1
 MA Name Format    : string
```



```
Interval          : 1000
Priority          : 7
VLAN ID           : --
VSI Name          : --
L2VC ID           : --
MEP Number        : 1
RMEP Number       : 1
Suppressing Alarms : No
Sending AIS Packet : No
Interface TLV     : disabled
RDI Track-action  : all-enabled
```

Display detailed information about all the MAs in the specified MD.

```
<HUAWEI> display cfm ma md md1
The total number of MAs is : 2
------------------------------------------------------
MD Name           : md1
MD Name Format    : string
Level             : 0
MIP Create-type   : none
SenderID TLV-type  : defer
MA Name           : ma1
MA Name Format    : string
Interval          : 1000
Priority          : 7
VLAN ID           : --
VSI Name          : --
L2VC ID           : --
MEP Number        : 1
RMEP Number       : 1
Suppressing Alarms : No
Sending AIS Packet : No
Interface TLV     : disabled
RDI Track-action  : all-enabled
MD Name           : md1
MD Name Format    : string
Level             : 0
MIP Create-type   : none
SenderID TLV-type  : defer
MA Name           : ma2
MA Name Format    : string
Interval          : 1000
Priority          : 7
VLAN ID           : --
VSI Name          : --
L2VC ID           : --
MEP Number        : 1
RMEP Number       : 1
 Suppressing Alarms : No
Sending AIS Packet : No
Interface TLV     : disabled
RDI Track-action  : all-enabled
```

Display detailed information about all the MAs in the MD named **md** in **no-md-name** format.

```
<HUAWEI> display cfm ma md md
The total number of MAs is : 2
------------------------------------------------------
MD Name           : md
MD Name Format    : string
Level             : 0
MIP Create-type   : none
SenderID TLV-type  : defer
MA Name           : ma
MA Name Format    : no-md-name
Interval          : 1000
Priority          : 7
VLAN ID           : --
```



```
VSI Name          : --
L2VC ID           : --
MEP Number        : 0
RMEP Number       : 1
Suppressing Alarms : No
Sending AIS Packet : No
Interface TLV     : disabled
RDI Track-action  : all-enabled

MD Name           : md
MD Name Format    : string
Level             : 0
MIP Create-type   : none
SenderID TLV-type : defer
MA Name           : ma
MA Name Format    : no-md-name
Interval          : 1000
Priority          : 7
VLAN ID           : --
VSI Name          : --
L2VC ID           : --
MEP Number        : 0
RMEP Number       : 1
Suppressing Alarms : No
Sending AIS Packet : No
Interface TLV     : disabled
RDI Track-action  : all-enabled
```

Table 12-53 Description of the **display cfm ma** command output

Item	Description
MD Name	Name of the MD. To set the name of the MD, run the **cfm md** command.
MD Name Format	Format of the MD name: ● no-md-name ● dns ● mac-address ● string To set the format of the MD name, run the **cfm md** command.
Level	MD level. The value ranges from 0 to 7. To set the MD level, run the **cfm md** command.
MIP Create-type	MIP creation rule: ● default ● explicit ● none To set the MIP creation rule, run the **mip create-type** or **mip create-type** command.

Item	Description
SenderID TLV-type	Type of the Sender ID TLV filled in the CCM: ● none ● chassis ● manage ● chassisManage ● defer To set the type of the Sender ID TLV filled in the CCM, run the **senderid-tlv-type** command.
MA Name	Name of the MA. To set the name of the MA, run the **ma** command.
MA Name Format	Format of the MA name: ● icc-based ● string To set the format of the MA name, run the **ma** command.
Interval	Interval at which CCMs are sent in an MA. To set the interval at which CCMs are sent in an MA, run the **ccm-interval** command.
Priority	802.1p priority of CFM packets in an MA. The value ranges from 0 to 7. A larger value indicates a higher priority. The default value is 7. To set the 802.1p priority of CFM packets in an MA, run the **packet-priority** command.
VLAN ID	ID of the VLAN associated with an MA. To set the ID of the VLAN associated with an MA, run the **map** command.
VSI Name	Name of the VSI associated with an MA.
L2VC ID	ID of the L2VC associated with an MA.
MEP Number	Number of MEPs in an MA.
RMEP Number	Number of RMEPs in an MA.

Item	Description
Suppressing Alarms	Whether the device is enabled to suppress alarms.
Sending AIS Packet	Whether the device is sending AIS PDUs.
Interface TLV	Whether the CCM TLV is enabled: • disabled • enabled
RDI Track-action	Whether the device is RDI Track-action.

12.8.23 display cfm md

Function

The **display cfm md** command displays MD information, including the MD name and level.

Format

display cfm md [*md-name*]

Parameters

Parameter	Description	Value
md *md-name*	Specifies the name of an MD. If *md-name* is not specified, information about all MDs created on the device is displayed.	The value is a string of 1 to 43 case-sensitive characters without spaces, hyphens (-), and question marks (?). **NOTE** 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

You can use the **display cfm md** command to view MD information, including the MD level, MD name format, MIP creation rule in the MD, and Sender ID TLV type. In addition, you can view brief information about MAs in the MD, such as the MA name, interval at which CCMs are sent, ID of the VLAN associated with the MA, and name of the VSI associated with the MA. If *md-name* is not specified, information about all the created MDs is displayed.

Example

Display information about the MD named **mdcustomer** on the device running IEEE Standard 802.1ag-2007.

```
<HUAWEI> display cfm md mdcustomer
 MD Name            : mdcustomer
 MD Name Format     : string
 Level              : 0
 MIP Create-type    : none
 SenderID TLV-type  : defer
 MA list            :
        MA Name           : ma
        MA Name Format    : string
        Interval          : 1000
        VLAN ID           : 100
        VSI Name          : --
        L2VC ID           : --
```

Table 12-54 Description of the **display cfm md** command output

Item	Description
MD Name	Name of the MD. To set the name of the MD, run the **cfm md** command.
MD Name Format	Format of the MD name: ● no-md-name ● dns ● mac-address ● string To set the format of the MD name, run the **cfm md** command.
Level	Level of the MD. The value ranges from 0 to 7. A higher level indicates a higher priority. To set the level of the MD, run the **cfm md** command.

Item	Description
MIP Create-type	MIP creation rule: ● default ● explicit ● none To set the MIP creation rule, run the **mip create-type** command.
SenderID TLV-type	Type of the Sender ID TLV in the CCM: ● none ● chassis ● manage ● chassisManage ● defer To set the type of the Sender ID TLV in the CCM, run the **senderid-tlv-type** command.
MA list	Information about MAs in the MD.
MA Name	Name of the MA. To set the MAs in the MD, run the **ma** command.
MA Name Format	Format of the MA name: ● icc-based ● string To set the format of the MA name, run the **ma** command.
Interval	Interval at which CCMs are sent. To set the interval at which CCMs are sent, run the **ccm-interval** command.
VLAN ID	ID of the VLAN associated with an MA. To set the ID of the VLAN associated with an MA, run the **map** command.
VSI Name	Name of the VSI associated with an MA. The switch does not support this function.
L2VC ID	ID of the L2VC associated with an MA. The switch does not support this function.

12.8.24 display cfm mep

Function

The **display cfm mep** command displays information about a MEP in a specified MD and MA.

Format

display cfm mep [**md** *md-name* [**ma** *ma-name* [**mep-id** *mep-id*]]]

Parameters

Parameter	Description	Value
md *md-name*	Displays information about MEPs in a specified MD. *md-name* specifies the name of the MD. If this parameter is not specified, information about MEPs in all MDs and MAs on the device is displayed.	The value is a string of 1 to 43 case-sensitive characters without spaces, hyphens (-), and question marks (?).
ma *ma-name*	Displays information about MEPs in a specified MA. *ma-name* specifies the name of the MA. If this parameter is not specified, information about MEPs in all the MAs of a specified MD is displayed.	The value is a string of 1 to 43 case-sensitive characters without spaces, hyphens (-), and question marks (?).
mep-id *mep-id*	Displays information about a specified MEP. *mep-id* specifies the ID of the MEP.	The value is an integer that ranges from 1 to 8191.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

After a MEP is configured or CFM cannot work properly, use the **display cfm mep** command to check the MEP configuration.

Example

Display information about the MEP with an ID of 10 in the MA named **ma1** of the MD named **md1**.

```
<HUAWEI> display cfm mep md md1 ma ma1 mep-id 10
```



```
MD Name            : md1
MD Name Format     : string
Level              : 0
MA Name            : ma1
MEP ID             : 2
VLAN ID            : --
VSI Name           : --
L2VC ID            : --
Interface Name     : GigabitEthernet0/0/1
CCM Send           : enabled
Direction          : outward
MAC Address        : 00e0-fc03-0161
MEP Pe-vid         : --
MEP Ce-vid         : --
MEP Vid            : --
Alarm Status       : LOC
Alarm AIS          : enabled
Alarm RDI          : enabled
```

Display information about all MEPs in the MA named **ma1** of the MD named **md1**.

```
<HUAWEI> display cfm mep md md1 ma ma1
The total number of MEPs is : 1
------------------------------------------------------
MD Name            : md1
MD Name Format     : string
Level              : 0
MA Name            : ma1
MEP ID             : 2
VLAN ID            : --
VSI Name           : --
L2VC ID            : --
Interface Name     : GigabitEthernet0/0/1
CCM Send           : enabled
Direction          : outward
MAC Address        : 00e0-fc03-0161
MEP Pe-vid         : --
MEP Ce-vid         : --
MEP Vid            : --
Alarm Status       : LOC
Alarm AIS          : enabled
Alarm RDI          : enabled
```

Display information about all MEPs in the MD named **md1**.

```
<HUAWEI> display cfm mep md md1
The total number of MEPs is : 2
------------------------------------------------------
MD Name            : md1
MD Name Format     : string
Level              : 0
MA Name            : ma1
MEP ID             : 2
VLAN ID            : --
VSI Name           : --
L2VC ID            : --
Interface Name     : GigabitEthernet0/0/1
CCM Send           : enabled
Direction          : outward
MAC Address        : 00e0-fc03-0161
MEP Pe-vid         : --  MEP Ce-vid         : --  MEP Vid            : --  Alarm Status       : LOC  Alarm AIS          :
enabled  Alarm RDI          : enabled
MD Name            : md1
MD Name Format     : string
Level              : 0
MA Name            : ma2
MEP ID             : 4
VLAN ID            : --
VSI Name           : --
```



```
L2VC ID           : --
Interface Name    : GigabitEthernet0/0/2
CCM Send          : enabled
Direction         : outward
MAC Address       : 00e0-fc03-0161
MEP Pe-vid        : --
MEP Ce-vid        : --
MEP Vid           : --
Alarm Status      : LOC
Alarm AIS         : enabled
Alarm RDI         : enabled
```

Table 12-55 Description of the **display cfm mep** command output

Item	Description
MD Name	Name of the MD. To set the name of the MD, run the **cfm md** command.
MD Name Format	Format of the MD name: ● no-md-name ● dns ● mac-address ● string To set the format of the MD name, run the **cfm md** command.
Level	Level of the MD. The value ranges from 0 to 7. A higher level indicates a higher priority of the MD. To set the MD level, run the **cfm md** command. **NOTE** If the level of a MEP on an intermediate node is higher than or equal to that on the source node, run the **cfm md** command to decrease the level of the MEP on the intermediate node to be lower than that on the source node.
MA Name	Name of the MA. To set the name of the MA, run the **ma** command.
MEP ID	ID of the MEP. To set the ID of the MEP, run the **mep mep-id** command.
VLAN ID	ID of the VLAN associated with an MA. To set the ID of the VLAN associated with an MA, run the **map** command.
VSI Name	Name of the VSI associated with an MA.
L2VC ID	ID of the L2VC associated with an MA.

Item	Description
Interface Name	Interface where a MEP is configured. If a MEP is based on VLANIF interfaces, this field is displayed as --.
CCM Send	Whether the MEP is enabled to send CCMs: ● enabled: The MEP is enabled to send CCMs. ● disabled: The MEP is disabled from sending CCMs. To set the parameter, run the **mep ccm-send enable** command.
Direction	Type of the MEP: ● inward: indicates an inward-facing MEP. An inward-facing MEP broadcasts 802.1ag packets in the VLAN associated with the MA, but does not send 802.1ag packets to the interface where the MEP is configured. ● outward: indicates an outward-facing MEP. An outward-facing MEP sends 802.1ag packets through an interface on which the MEP is configured. **NOTE** If the MEP direction is incorrect, run the **mep mep-id** command to configure a correct direction.
MAC Address	MAC address of the MEP.
MEP Pe-vid	Outer VLAN ID of the QinQ interface where the MEP is configured.
MEP Ce-vid	Inner VLAN ID of the QinQ interface where the MEP is configured.
MEP Vid	VLAN ID of the Dot1q interface where the MEP is configured.
Alarm Status	Alarm type: ● unexpectedMEP: The MEP receives CCMs with an unexpected flag. ● mismerge: The MEG ID in received CCMs is different from that configured for the MEP. ● unexpectedPeriod: The interval in the received CCMs is different from the configured interval. ● unexpectedMAC: The MEP MAC address in the received CCM is different from at least one MAC address of the RMEP. ● LOC: At least one session between the MEP and an RMEP is terminated. ● RDI: The MEP receives CCMs with the RDI.

Item	Description
Alarm AIS	Whether the alarm reporting function of a specific alarm indication signal (AIS) is enabled: • enable • disable
Alarm RDI	Whether the alarm reporting function of a specific remote defect indication (RDI) is enabled: • enable • disable

12.8.25 display cfm mip

Function

The **display cfm mip** command displays MIP information.

Format

display cfm mip [**interface** *interface-type interface-number* | **level** *level*]

Parameters

Parameter	Description	Value
level *level*	Displays information about a MIP of a specified level. *level* specifies the level of the MIP.	The value is an integer that ranges from 0 to 7. A larger value indicates a higher level.
interface-type interface-number	Displays MIP information on a specified interface. • *interface-type* specifies the interface type. • *interface-number* specifies the interface number.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

You can use the **display cfm mip** command to check MIPs, interfaces where MIPs are configured, and levels of the MIPs on the device.

Precautions

If **level** *level* and **interface** *interface-type interface-number* are not specified, information about all MIPs on the device is displayed.

Example

Display information about all MIPs.

```
<HUAWEI> display cfm mip
Interface Name              Level     MAC
------------------------------------------------------------
GigabitEthernet0/0/1        0         00e0-fc02-377f
GigabitEthernet0/0/1        0         00e0-fc02-375f
```

Display information about the MIP at level 7.

```
<HUAWEI> display cfm mip level 7
Interface Name              Level     MAC
------------------------------------------------------------
GigabitEthernet0/0/1        7         00e0-fc02-367f
GigabitEthernet0/0/1        7         00e0-fc02-365f
```

Display information about MIPs on GigabitEthernet0/0/1.

```
<HUAWEI> display cfm mip interface gigabitethernet 0/0/1
Interface Name              Level     MAC
------------------------------------------------------------
GigabitEthernet0/0/1        0         00e0-fc02-368f
```

Display information about MIPs on the GigabitEthernet0/0/1.

```
<HUAWEI> display cfm mip interface gigabitethernet 0/0/1
Info: The MIP does not exist.
```

Table 12-56 Description of the **display cfm mip** command output

Item	Description
Interface Name	Name of the interface where a MIP is configured.
Level	Level of the MIP. The value ranges from 0 to 7. A larger value indicates a higher priority. To set the level of the MIP, run the **cfm mip** command.
MAC	MAC address of the MIP.

12.8.26 display cfm mp-info

Function

The **display cfm mp-info** command displays information about CFM objects on a specified interface or in a VLAN.

Format

display cfm mp-info [**interface** *interface-type interface-number*] [**level** *md-level*] [**inward** | **outward**] [**vlan** *vlanid* | **no-associated-vlan**]

Parameters

Parameter	Description	Value
interface-type interface-number	Displays CFM information on a specified interface. • *interface-type* specifies the interface type. • *interface-number* specifies the interface number.	-
level *md-level*	Specifies the level of an MD.	The value is an integer that ranges from 0 to 7. By default, the value is 0.
inward	Indicates the inward-facing MEP. An inward-facing MEP sends 802.1ag packets through all interfaces in a VLAN associated with an MA, except the interface on which the MEP is configured. That is, the inward-facing MEP broadcasts 802.1ag packets in the VLAN associated with the MA.	-
outward	Indicates the outward-facing MEP. An outward-facing MEP sends 802.1ag packets through an interface on which the MEP is configured.	-
vlan *vlanid*	Displays CFM information in a specified VLAN.	The value is an integer that ranges from 1 to 4094.
no-associated-vlan	Indicates the MP that is not associated with a VLAN.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

You can use the **display cfm mp-info** command to view information about CFM objects and the relationship between MPs on the interface so that you can configure MEPs correctly.

Prerequisites

CFM has been enabled globally using the **cfm enable (system view)** command.

Precautions

IEEE 802.1ag has two versions: IEEE 802.1ag Draft 7 and IEEE Standard 802.1ag-2007. This command can be used only on the device running IEEE Standard 802.1ag-2007.

Multiple MEPs can be configured and multiple MIPs can be generated on an interface; however, the levels of MEPs or MIPs must be the same. If the configuration is incorrect, CCM leak occurs or LBR or LTR messages cannot be sent correctly.

Example

Display information about the specified interface, MD level, MEP type, and VLAN.

```
<HUAWEI> display cfm mp-info interface gigabitethernet 0/0/1
The total number of MPs is : 1
The number of MEPs is : 1. The number of MIPs is : 0.
------------------------------------------------------
 MD Name            : md1
 MD Name Format     : string
 Level              : 0
 MA Name            : ma2
 MEP ID             : 4
 VLAN ID            : --
 VSI Name           : --
 L2VC ID            : --
 Interface Name     : GigabitEthernet0/0/1
 CCM Send           : enabled
 Direction          : outward
 MAC Address        : 00e0-fc03-0161
 MEP Pe-vid         : --
 MEP Ce-vid         : --
 MEP Vid            : --
 Alarm Status       : LOC
 Alarm AIS          : enabled
 Alarm RDI          : enabled
```


Table 12-57 Description of the **display cfm mp-info** command output

Item	Description
Interface Name	Name of the interface.
MD Name	Name of the MD. To set the name of the MD, run the **cfm md** command.
MD Name Format	Format of the MD name: ● no-md-name ● dns ● mac-address ● string To set the format of the MD name, run the **cfm md** command.
Level	Level of the MD, MA, or MP. The value ranges from 0 to 7. A higher level indicates a higher priority. To set the MD level, run the **cfm md** command.
MA Name	Name of the MA. To set the name of the MA, run the **ma** command.
MEP ID	ID of the MEP. To set the ID of the MEP, run the **mep mep-id** command.
CCM Send	Whether the MEP is enabled to send CCMs: ● enabled ● disabled To set the parameter, run the **mep ccm-send enable** command.
Direction	Type of the MEP: ● inward ● outward To set the type of the MEP, run the **mep mep-id** command.
VLAN ID	ID of the VLAN associated with an MA. To set the ID of the VLAN associated with an MA, run the **map** command.
VSI Name	Name of the VSI associated with an MA.
L2VC ID	ID of the L2VC associated with an MA.

Item	Description
MAC Address	MAC address of the MEP or MIP. **NOTE** 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.
MEP Pe-vid	VLAN ID in the outer tag of a VLAN frame.
MEP Ce-vid	VLAN ID in the inner tag of a VLAN frame.
MEP Vid	ID of a VLAN.
Alarm Status	Type of alarm: • unexpectedMEGLevel: The MD level carried in a CCM sent by the RMEP was different from that specified on the MEP. • unexpectedMEP: The trap about inconsistency between the MD level carried in a CCM sent by the RMEP and that specified on the MEP was cleared. • mismerge: An MD or MA name carried in a CCM sent by the RMEP was different from that specified on the MEP. • unexpectedPeriod: The CCM interval carried in a CCM sent by the RMEP was different from that specified on the MEP. • unexpectedMAC: The source MAC address carried in a CCM sent by the RMEP was different from the RMEP's MAC address specified on the MEP. • LOC: At least one session between the MEP and an RMEP is terminated. • exceptionalMACstatus: TLV information carried in a CCM sent by the RMEP within a specified interval showed that the interface connecting the RMEP to the MEP became abnormal. • RDI: The RMEP sent a CCM carrying the RDI flag with the value of 1 to the MEP.
Alarm AIS	Whether the alarm reporting function of a specific alarm indication signal (AIS) is enabled: • enable • disable

Item	Description
Alarm RDI	Whether the alarm reporting function of a specific remote defect indication (RDI) is enabled: • enable • disable

12.8.27 display cfm remote-mep

Function

The **display cfm remote-mep** command displays information about RMEPs in a specified MD and MA.

Format

display cfm remote-mep md *md-name* **ma** *ma-name* **mep-id** *mep-id*

display cfm remote-mep [**md** *md-name* [**ma** *ma-name*]] [**cfm-state** { **up** | **down** | **disable** }]

Parameters

Parameter	Description	Value
md *md-name*	Displays information about RMEPs in a specified MD. *md-name* specifies the name of the MD. If this parameter is not specified, information about RMEPs in all MDs and MAs on the device is displayed.	The value is a string of 1 to 43 case-sensitive characters without spaces, hyphen (-), and question mark (?).
ma *ma-name*	Displays information about RMEPs in a specified MA. *ma-name* specifies the name of the MA. If this parameter is not specified, information about RMEPs in all MAs in a specified MD is displayed.	The value is a string of 1 to 43 case-sensitive characters without spaces, hyphen (-), and question mark (?).
mep-id *mep-id*	Displays information about a specified RMEP. *mep-id* specifies the ID of the RMEP.	The value is an integer that ranges from 1 to 8191.
cfm-state	Displays RMEP information based on the CFM status.	-

Parameter	Description	Value
up	Displays information about RMEPs in Up state.	-
down	Displays information about RMEPs in Down state.	-
disable	Displays information about RMEPs in disabled state.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

After an RMEP is configured or CFM cannot work properly, use the **display cfm remote-mep** command to check the RMEP configuration, including:

- Name and level of the MD
- Name of the MA and VLAN associated with the MA
- ID of the RMEP
- MAC address of the RMEP
- Whether the MEP is enabled to receive CCMs from the RMEP
- Alarm status

You can specify **cfm-state** to view RMEP information in the specified CFM state.

Example

Display information about the RMEP with an ID of 50 in the MA named **ma1** within the MD named **md1**.

```
<HUAWEI> display cfm remote-mep md md1 ma ma1 mep-id 50
 MD Name           : md1
 Level             : 0
 MA Name           : ma1
 RMEP ID           : 5
 VLAN ID           : --
 VSI Name          : --
 L2VC ID           : --
 MAC               : --
 CCM Receive       : enabled
 Trigger-If-Down   : enabled
 CFM Status        : down
 Alarm Status      : LOC
 Interface TLV     : --
 Connect Status    : up
```


Display information about all RMEPs in the MA named **ma1** within the MD named **md1**.

```
<HUAWEI> display cfm remote-mep md md1 ma ma1
The total number of RMEPs is : 1
The status of RMEPs : 0 up, 1 down, 0 disable
--------------------------------------------------
 MD Name           : md1
 Level          : 0
 MA Name           : ma1
 RMEP ID         : 5
 VLAN ID         : --
 VSI Name        : --
 L2VC ID         : --
 MAC             : --
 CCM Receive       : enabled
 Trigger-If-Down   : enabled
 CFM Status        : down
 Alarm Status      : LOC
 Interface TLV     : --
 Connect Status    : up
```

Display information about all RMEPs configured on the device.

```
<HUAWEI> display cfm remote-mep
The total number of RMEPs is : 1
The status of RMEPs : 0 up, 0 down, 1 disable
--------------------------------------------------
 MD Name           : md
 Level          : 0
 MA Name           : ma
 RMEP ID         : 1
 VLAN ID         : --
 VSI Name        : --
 L2VC ID         : --
 MAC             : --
 CCM Receive       : disabled
 Trigger-If-Down   : disabled
 CFM Status        : disabled
 Alarm Status      : none
 Interface TLV     : --
 Connect Status    : up
```

Display information about all RMEPs in Down state.

```
<HUAWEI> display cfm remote-mep cfm-state down
The total number of RMEPs is : 2
The status of RMEPs : 0 up, 2 down, 0 disable
--------------------------------------------------
 MD Name           : md
 Level          : 0
 MA Name           : ma
 RMEP ID         : 1111
 VLAN ID         : 1111
 VSI Name        : --
 L2VC ID         : --
 MAC             : --
 CCM Receive       : enabled
 Trigger-If-Down   : disabled
 CFM Status        : down
 Alarm Status      : none
 Interface TLV     : --
 Connect Status    : up

 MD Name           : md1
 Level          : 0
 MA Name           : ma1
 RMEP ID         : 2
 VLAN ID         : 100
 VSI Name        : --
```



```
L2VC ID           : --
MAC               : 00e0-fc41-5410
CCM Receive       : enabled
Trigger-If-Down   : disabled
CFM Status        : down
Alarm Status      : LOC
Interface TLV     : --
Connect Status    : up
```

Table 12-58 Description of the display cfm remote-mep command output

Item	Description
The total number of RMEPs is	Number of RMEPs.
MD Name	Name of the MD.
Level	Level of the MD. The value ranges from 0 to 7. A higher level indicates a higher priority of the MD.
MA Name	Name of the MA.
RMEP ID	ID of the RMEP.
VLAN ID	ID of the VLAN associated with an MA.
VSI Name	Name of the VSI associated with an MA.
L2VC ID	ID of the VC.
MAC	MAC address of the RMEP. **NOTE** An RMEP's MAC address can be a bridge MAC address or the MAC address of the interface where the RMEP is configured. The MAC address depends on the configured MP address model: • If the shared MP address model is configured, an RMEP uses a bridge MAC address as its own MAC address. • If the independent MP address model is configured, an RMEP uses the MAC address of the interface where the RMEP is configured.
CCM Receive	Whether the MEP is enabled to receive CCMs from the RMEP: • disabled: The MEP is disabled from receiving CCMs from the RMEP. • enabled: The MEP is enabled to receive CCMs from the RMEP. To configure the CCM reception function, run the **remote-mep ccm-receive enable** command.

Item	Description
Trigger-If-Down	Whether the block/unblock function is configured on the interface: ● disable: indicates that the block/unblock function is disabled on the interface for the RMEP. ● enable: indicates that the block/unblock function is enabled on the interface for the RMEP. When a MEP detects a connectivity fault between the MEP and the RMEP in the same MA, the system blocks the interface on which the MEP is configured and then unblocks it. To configure the block/unblock function, run the **cfm trigger if-down** command.
CFM Status	CFM status: ● up: indicates that CC works properly. ● down: No MEP is configured on the device or the interface where the MEP is configured is unavailable. The reason why the interface is unavailable is one of the following: The subcard is not installed or has been restarted. The Eth-Trunk has no member interface or all member interfaces are Down. ● disable: indicates that CFM is not configured, that is, the MEP is not enabled to send CCMs and the RMEP is not enabled to receive CCMs.
Alarm Status	CFM alarm status: ● unexpectedPeriod: The interval carried in a CCM sent by the RMEP is different from that configured on the MEP. ● unexpectedMAC: The source MAC address carried in a CCM sent by the RMEP is different from the RMEP's MAC address configured on the MEP. ● LOC: The session is terminated. ● exceptionalMACstatus: TLV information carried in a CCM sent by the RMEP within a specified interval indicates that the interface connecting the RMEP to the MEP is abnormal. ● RDI: The MEP receives CCMs with RDI. ● none: No alarm is generated. **NOTE** If the device is configured with no MEP but an RMEP, the CFM status is Down. However, no alarm is generated. That is, the field is none.

Item	Description
Interface TLV	Status of an interface type-length-value (TLV). The value can be: ● - -: The default value is 0. No TLV status is available on the interface. ● up: The interface status is Up, and the interface can transmit packets. ● down: The interface status is Down, and the interface cannot transmit packets. ● testing: The TLV status of the interface is testing. ● unknown: The interface status is unknown. ● dormant: The interface is blocked and is waiting for an external event. ● notPresent: Information about the interface components is lost. ● lowerLayerDown: The lower layer status of the interface is Down. **NOTE** ● The packets carrying the interface TLV field with the value Up or Down can be sent. ● The received packets carrying the interface TLV field with any value can be parsed.
Connect Status	The connect status of RMEP: ● none: Detection is not started on the RMEP. ● start: The RMEP is configured, but the remote device does not receive valid CCMs within the timeout period. ● up: The physical link is working properly, and the remote device can receive correct CCMs. ● down: The local device cannot receive correct CCMs.

12.8.28 display mip create-type

Function

The **display mip create-type** command displays MIP creation rules globally or on a specified interface.

Format

display mip create-type [**interface** *interface-type interface-number*]

Parameters

Parameter	Description	Value
interface-type interface-number	Displays MIP creation rules on a specified interface. • *interface-type* specifies the interface type. • *interface-number* specifies the interface number. If this parameter is not specified, MIP creation rules on a device are displayed.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

IEEE 802.1ag has two versions: IEEE 802.1ag Draft 7 and IEEE Standard 802.1ag-2007. This command can be used only on the device running IEEE 802.1ag Draft 7.

After MIP creation rules are configured using the **mip create-type (system view)** command or CFM does not work properly, use the **display mip create-type** command to check MIP creation rules.

Example

Display MIP creation rules on GigabitEthernet0/0/1.

```
<HUAWEI> display mip create-type interface gigabitethernet 0/0/1
Interface Name               MIP Create-Type  MIP Create-Type On Interface
------------------------------------------------------------------------------
GigabitEthernet0/0/1         default          --
```

Table 12-59 Description of the **display mip create-type** command output

Item	Description
Interface Name	Name of the interface.
MIP Create-Type	MIP creation rule on the device: • default: A MIP can be created on the interface without a higher-level MEP and a lower-level MIP. • explicit: A MIP can be created on an interface with a lower-level MEP but without a higher-level MEP or a lower-level MIP. • none: No MIP is created automatically.

Item	Description
MIP Create-Type On Interface	MIP creation rule on an interface: • default: A MIP can be created on the interface without a higher-level MEP and a lower-level MIP. • explicit: A MIP can be created on an interface with a lower-level MEP but without a higher-level MEP or a lower-level MIP. • none: No MIP is created automatically. • --: The MIP creation rule on an interface is the same as that on the device.

12.8.29 display oam global configuration

Function

The **display oam global configuration** command displays the global configuration of Ethernet OAM.

Format

display oam global configuration

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

You can use the **display oam global configuration** command to check the global configuration of Ethernet OAM, including:

- Whether Ethernet CFM is enabled globally
- Whether GMAC ping is enabled
- Whether GMAC trace is enabled
- Whether EFM OAM is enabled globally

- Ethernet CFM version information
- MP address model

Precautions

IEEE 802.1ag has two versions: IEEE 802.1ag Draft 7 and IEEE Standard 802.1ag-2007.

NOTE

Run the **cfm version** command to switch Ethernet CFM 802.1ag between IEEE 802.1ag Draft 7 and IEEE Std 802.1ag-2007.

Example

Display the global configuration of Ethernet OAM on the device.

```
<HUAWEI> display oam global configuration
Global Configuration                          Value
------------------------------------------------------------
CFM Status                                 enabled
Ping MAC Status                             disabled
Trace MAC Status                            disabled
CFM MAC-tunnel MIP Trace Status                   disabled
EFM Status                                 enabled
CFM Protocol                               standard
CFM MP-address-model                            bridge
```

Table 12-60 Description of the **display oam global configuration** command output

Item	Description
CFM Status	Whether Ethernet CFM is enabled globally: • disabled: Ethernet CFM is disabled globally. • enabled: Ethernet CFM is enabled globally. To configure the parameter, run the **cfm enable** command.
Ping MAC Status	Whether GMAC ping is enabled: • disabled: GMAC ping is disabled. • enabled: GMAC ping is enabled. To configure the parameter, run the **ping mac enable** command.
Trace MAC Status	Whether GMAC trace is enabled: • disabled: GMAC trace is disabled. • enabled: GMAC trace is enabled. To configure the parameter, run the **trace mac enable** command.

Item	Description
CFM MAC-tunnel MIP Trace Status	Whether the intermediate node in the MAC tunnel is enabled to respond to MAC trace messages: ● disabled: The intermediate node in the MAC tunnel is disabled from responding to MAC trace messages. ● enabled: The intermediate node in the MAC tunnel is enabled to respond to MAC trace messages. **NOTE** The switch does not support this parameter.
EFM Status	Whether EFM OAM is enabled globally: ● disabled: EFM OAM is disabled globally. ● enabled: EFM OAM is enabled globally. To configure the parameter, run the **efm enable** command.
CFM Protocol	Ethernet CFM version. ● standard: IEEE Standard 802.1ag-2007. ● bbb0: IEEE 802.1ag Draft 7. To configure the parameter, run the **cfm version** command.
CFM MP-address-model	MP address model: ● bridge: shared MP address model ● individual: independent MP address model **NOTE** Currently, only the shared MP address model is supported.

12.8.30 ma

Function

The **ma** command creates an MA in an MD and displays the MA view, or directly displays view of an existing MA.

The **undo ma** command deletes an MA.

Format

MD view, MA view:

ma *ma-name* [**format** { **icc-based** *iccbased-ma-format-name* | **string** *ma-format-name* }]

MD view:

undo ma [*ma-name*]

Parameters

Parameter	Description	Value
ma-name	Specifies the name of an MA. The name of an MA in an MD is unique.	The value is a string of 1 to 43 characters without spaces, hyphens (-), and question marks (?). The total length of the names of the MA and MD must be within 44 case-sensitive characters. **NOTE** When double quotation marks are used around the string, spaces are allowed in the string.
icc-based *iccbased-ma-format-name*	Specifies an ICC-based MA name carried in CCMs to be sent. ITU carrier codes (ICCs) are assigned to network operators or service providers and maintained by ITU-T Telecommunication Standardization Bureau (TSB) in compliance with ITU-T M.1400 Recommendation.	The value is a string of 1 to 13 case-sensitive characters without spaces, hyphens (-), and question marks (?).
string *ma-format-name*	Specifies a string-based MA name carried in CCMs to be sent.	The value is a string of 1 to 43 case-sensitive characters without spaces, hyphens (-), and question marks (?).

Views

MD view, MA view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Generally, services are deployed based on VLANs on a network. If CFM is required to monitor link connectivity, run the **ma** *ma-name* command to create an MA. Then CFM can be implemented in the MA.

Prerequisites

An MD has been created using the **cfm md** *md-name* command.

Precautions

- When an MA is deleted, the device automatically deletes all MEPs and RMEPs in the MA, stops CC, and clears MA-related alarms.
- An ICC-based MA can only be configured in the MD with the MD name in **no-md-name** format.

Example

Create an MA named **ma1**.

```
<HUAWEI> system-view
[HUAWEI] cfm enable
[HUAWEI] cfm md md1
[HUAWEI-md-md1] ma ma1
[HUAWEI-md-md1-ma-ma1]
```

12.8.31 map

Function

The **map** command associates a VLAN with an MA.

The **undo map** command disassociates a VLAN from an MA.

By default, an MA is not associated with any VLAN.

Format

map vlan *vlan-id*

undo map vlan

Parameters

Parameter	Description	Value
vlan-id	Specifies the ID of a VLAN.	The value is an integer that ranges from 1 to 4094.

Views

MA view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Ethernet CFM detects connectivity faults in each MA. After an MA is associated with a VLAN, Ethernet CFM can detect connectivity faults in the VLAN.

Precautions

If CFM is used to detect connectivity faults between two directly connected devices, the MA does not need to be associated with a VLAN.

An MA can be associated with only one VLAN.

NOTICE

You can create or delete the association between an MA and a VLAN only when no MEP or RMEP is configured in the MA.

Before changing the VLAN associated with an MA, use the **undo map** command to disassociate the MA from the VLAN.

Example

Associate an MA with VLAN 10. The MA is not associated with any VLAN before the configuration.

```
<HUAWEI> system-view
[HUAWEI] cfm enable
[HUAWEI] cfm md md1
[HUAWEI-md-md1] ma ma1
[HUAWEI-md-md1-ma-ma1] map vlan 10
```

12.8.32 mep mep-id

Function

The **mep mep-id** command creates a MEP.

The **undo mep mep-id** command deletes a MEP.

Format

mep mep-id *mep-id* **interface** *interface-type interface-number* [**pe-vid** *pe-vid* **ce-vid** *ce-vid*] { **inward** | **outward** }

undo mep mep-id *mep-id*

Parameters

Parameter	Description	Value
mep-id *mep-id*	Specifies the ID of a MEP. The ID identifies a MEP. The MEP ID must be unique in an MA and in a VLAN.	The value is an integer that ranges from 1 to 8191.
interface-type interface-number	Specifies the type and number of the interface where a MEP is configured. • *interface-type* specifies the interface type. • *interface-number* specifies the interface number.	-
pe-vid *pe-vid*	Specifies the outer VLAN ID of a PE.	The value is a decimal integer that ranges from 1 to 4094.
ce-vid *ce-vid*	Specifies the inner VLAN ID of a CE.	The value is a decimal integer that ranges from 1 to 4094.
inward	Indicates an inward-facing MEP. An inward-facing MEP sends 802.1ag packets through all interfaces in a VLAN associated with an MA, except the interface on which the MEP is configured. That is, the inward-facing MEP broadcasts 802.1ag packets in the VLAN associated with the MA.	-
outward	Indicates an outward-facing MEP. An outward-facing MEP sends 802.1ag packets through an interface on which the MEP is configured.	-

Views

MA view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To create a MEP, run the **mep mep-id** command.

Precautions

Inward- and outward-facing MEPs are classified based on the scope where 802.1ag packets are sent.

The MEP level of the associated VLAN must be greater than the MEP level of the non-associated VLAN based on the same physical interface or Eth-Trunk member interface. The MEP level is determined by the MD level. You can run the **cfm md** *md-name* command to configure the MD level.

The requirements for the number and type of MEPs created in an MA are as follows:

- The inward- and outward-facing MEPs cannot coexist.
- You can create multiple inward-facing interface-based MEPs but only one outward-facing interface-based MEP. Only one inward-facing interface-based MEP can be created on an interface.

Example

Create an inward-facing MEP on GigabitEthernet0/0/1 in MA **ma1** of MD **md1** and set the MEP ID to 15.

```
<HUAWEI> system-view
[HUAWEI] vlan 100
[HUAWEI-vlan100] port gigabitethernet 0/0/1
[HUAWEI-vlan100] quit
[HUAWEI] cfm enable
[HUAWEI] cfm md md1
[HUAWEI-md-md1] ma ma1
[HUAWEI-md-md1-ma-ma1] map vlan 100
[HUAWEI-md-md1-ma-ma1] mep mep-id 15 interface gigabitethernet 0/0/1 inward
```

12.8.33 mep alarm disable

Function

The **mep alarm disable** command disables a MEP from reporting alarms.

The **undo mep alarm disable** command enables a MEP to report alarms.

By default, a MEP is enabled to report alarms.

Format

mep mep-id *mep-id* **alarm** { **rdi** | **ais** } **disable**

undo mep mep-id *mep-id* **alarm** { **rdi** | **ais** } **disable**

NOTE

Only the S5720I-SI, S5735-S, S500, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6720S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S support **ais**.

Parameters

Parameter	Description	Value
mep-id *mep-id*	Specifies the ID of a MEP. A MEP ID identifies a MEP. Each MEP must have a unique ID in an MA or a VLAN.	The value is an integer that ranges from 1 to 8191.
alarm rdi	Disables a MEP from reporting remote defect indication (RDI) alarms.	-
alarm ais	Disables a MEP from reporting AIS alarms.	-

Views

MA view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When an NMS manages many MEPs on a network, it may receive a large number of RDI and AIS alarms. To reduce such alarms, you can disable the MEPs from reporting alarms. After a MEP is disabled from reporting of RDI or AIS alarms, AIS or RDI alarms of this MEP are no longer sent to the NMS. This reduces the load of the NMS and local device.

Prerequisites

The following operations have been performed:

1. Run the **cfm md** command to create an MD.
2. Run the **ma** command to create an MA.
3. Run the **mep mep-id** command to create a MEP.

Example

Disable MEP 1 in the MA **ma1** of the MD **md1** from reporting RDI alarms.

```
<HUAWEI> system-view
[HUAWEI] cfm enable
[HUAWEI] cfm md md1
[HUAWEI-md-md1] ma ma1
[HUAWEI-md-md1-ma-ma1] map vlan 100
[HUAWEI-md-md1-ma-ma1] mep mep-id 1 alarm rdi disable
```

12.8.34 mep ccm-send enable

Function

The **mep ccm-send enable** command enables a MEP in an MA to send CCMs.

The **undo mep ccm-send enable** command disables a MEP in an MA from sending CCMs.

By default, a MEP is disabled from sending CCMs.

Format

mep ccm-send [**mep-id** *mep-id*] **enable**

undo mep ccm-send [**mep-id** *mep-id*] **enable**

Parameters

Parameter	Description	Value
mep-id *mep-id*	Specifies the ID of a MEP. If this parameter is not specified, all the MEPs in the MA are enabled to send CCMs or disabled from sending CCMs.	The value of *mep-id* is an integer that ranges from 1 to 8191.

Views

MA view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After you use the **mep mep-id** command to configure a MEP, use this command to enable the MEP to send CCMs.

Precautions

The interval at which CCMs are sent or received cannot be modified on the device in an MA if one of the following operations is performed:

- The **mep ccm-send enable** command is run to enable a MEP in an MA to send CCMs.
- The **remote mep ccm-receive enable** command is run to enable a MEP in an MA to receive CCMs.

The **undo mep ccm-send enable** or **remote mep ccm-receive enable** command must be run before the interval is reconfigured.

Example

Enable MEP 10 in the MA named **ma1** to send CCMs.


```
<HUAWEI> system-view
[HUAWEI] cfm md md1
[HUAWEI-md-md1] ma ma1
[HUAWEI-md-md1-ma-ma1] mep ccm-send mep-id 10 enable
```

12.8.35 mip create-type (MD view)

Function

The **mip create-type** command configures a MIP creation rule in an MD or the default MD.

The **undo mip create-type** command restores the default MIP creation rule in an MD or the default MD.

By default, the MIP creation rule in an MD or the default MD is **none**. That is, MIPs are not created.

Format

mip create-type { **default** | **explicit** | **none** }

undo mip create-type

Parameters

Parameter	Description	Value
default	Indicates that a MIP can be created on the interface without a higher-level MEP and a lower-level MIP. In this mode, MIPs can be created when no MEP is configured on the interface.	-
explicit	Indicates that a MIP can be created on an interface with a lower-level MEP but without a higher-level MEP or a lower-level MIP. In this mode, a MIP can be created on an interface only when a lower-level MEP has been configured on this interface.	-
none	Indicates that the MIP creation rule on an interface is none, that is, a MIP is not created automatically.	-

Views

MD view, default MD view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When all devices in an MD are enabled to send CCMs, MEPs send CCMs periodically. If a MEP receives no CCMs from an RMEP within three consecutive intervals for sending CCMs, a connectivity fault between the MEP and RMEP occurs. A MIP needs to be used to locate the fault.

Precautions

IEEE 802.1ag has two versions: IEEE 802.1ag Draft 7 and IEEE Standard 802.1ag-2007. This command can be used only on the device running IEEE Standard 802.1ag-2007.

After the MIP creation rule is set in an MD or the default MD, all interfaces in the MD or default MD use this rule to create a MIP.

If the MIP creation rule is **default** or **explicit**, the device creates a MIP automatically according to the rule.

NOTE

The **mip create-type** command can be used only on the Layer 2 interfaces to which the MD or default MD belongs.

Example

Set the MIP creation rule to **none** in the MD named **customer**.

```
<HUAWEI> system-view
[HUAWEI] cfm md customer level 1
[HUAWEI-md-customer] mip create-type none
```

Set the MIP creation rule to **default** in the default MD.

```
<HUAWEI> system-view
[HUAWEI] cfm default md
[HUAWEI-default-md] mip create-type default
```

12.8.36 mip create-type (system view)

Function

The **mip create-type** command configures a MIP creation rule on the device or a specified interface.

The **undo mip create-type** command restores the default MIP creation rule on a specified interface.

By default, the MIP creation rule on the device is **none** and all the interfaces use this rule to generate MIPs.

Format

mip create-type { **default** | **explicit** | **none** } [**interface** *interface-type interface-number*]

undo mip create-type [[**default** | **explicit** | **none**] **interface** *interface-type interface-number*]

Parameters

Parameter	Description	Value
default	Indicates that the MIP creation rule on an interface is **default**. That is, a MIP can be created on the interface without a higher-level MEP and a lower-level MIP. In this mode, MIPs can be created when no MEP is configured on the interface.	-
explicit	Indicates that the MIP creation rule on an interface is **explicit**. That is, a MIP can be created on an interface with a lower-level MEP but without a higher-level MEP or a lower-level MIP. In this mode, a MIP can be created on an interface only when a lower-level MEP has been configured on this interface.	-
none	Indicates that the MIP creation rule on an interface is **none**. That is, a MIP is not created automatically.	-
interface-type interface-number	Specifies the type and number of an interface where a MIP creation rule is configured. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number. If this parameter is not specified, the MIP creation rule takes effect globally.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To configure a MIP creation rule on the device, run the **mip create-type** command.

Precautions

NOTE

The command is only applicable to IEEE 802.1ag Draft 7.

If the MIP creation rule is **default** or **explicit**, the device creates a MIP automatically according to the rule.

Generally, you need to configure MIP nodes only when the 802.1ag MAC ping or trace operation is performed on a non-MEP node in an MA.

Prerequisites

CFM has been enabled globally using the **cfm enable (system view)** command.

Example

Set the MIP creation rule to **default** on GigabitEthernet0/0/1.

```
<HUAWEI> system-view
[HUAWEI] cfm enable
[HUAWEI] mip create-type default interface gigabitethernet 0/0/1
```

12.8.37 oam-bind cfm md ma efm interface

Function

The **oam-bind cfm md ma efm interface** command configures EFM and Ethernet CFM to report faults to each other.

The **undo oam-bind cfm md ma efm interface** command cancels the configuration.

By default, EFM OAM and Ethernet CFM are not configured to report faults to each other.

Format

oam-bind cfm md *md-name* **ma** *ma-name* **efm interface** *interface-type interface-number*

undo oam-bind cfm md *md-name* **ma** *ma-name* **efm interface** *interface-type interface-number*

NOTE

This command is not supported by only the SS1720GW-E, and S1720GWR-E.

Parameters

Parameter	Description	Value
md-name	Specifies the name of an MD.	The value is a string of 1 to 43 case-sensitive characters without spaces, hyphens (-), and question marks (?). **NOTE** When double quotation marks are used around the string, spaces are allowed in the string.

Parameter	Description	Value
ma-name	Specifies the name of an MA.	The value is a string of 1 to 43 case-sensitive characters without spaces, hyphens (-), and question marks (?). The total length of the names of the MA and MD must be within 44 characters. **NOTE** When double quotation marks are used around the string, spaces are allowed in the string.
interface-type interface-number	Specifies the type and number of an Ethernet interface. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number. The interface must have been enabled with EFM OAM.	-

Views

OAM management view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If EFM is deployed at one side and CFM is deployed at another side of a device, associate EFM with CFM on the device so that EFM and CFM can report faults to each other.

Association between EFM and CFM is bidirectional:

- When EFM detects a link fault, it will notify CFM of the fault.
- When CFM detects a link fault, it will notify EFM of the fault.

The following commands are used to associate EFM with CFM:

- **oam-bind cfm md ma efm interface**
- **oam-bind ingress cfm md ma egress efm interface**
- **oam-bind ingress efm interface egress cfm md ma**

Select the preceding commands in different scenarios according to **Table 12-61**.

Table 12-61 Association between EFM and CFM

Scenario	Configuration Solution 1	Configuration Solution 2
Bidirectional fault notification between EFM and CFM	The **oam-bind cfm md ma efm interface** command is used to configure EFM and CFM to report faults to each other.	Run the following commands at a random order (each command configures fault transmission in a single direction): • The **oam-bind ingress efm interface egress cfm md ma** command is used to configure EFM to report faults to CFM. • The **oam-bind ingress cfm md ma egress efm interface** command is used to configure CFM to report faults to EFM.
Unidirectional fault notification between EFM and CFM	Select either of the following commands based on the transmission direction: • Run the **oam-bind ingress efm interface egress cfm md ma** command to configure EFM to report faults to CFM. • Run the **oam-bind ingress cfm md ma egress efm interface** command to configure CFM to report faults to EFM.	None

Prerequisites

The MD and MA have been created and EFM has been enabled on the specified interface.

Precautions

The binding between an Ethernet CFM module and an interface is one-to-one. That is, when an Ethernet CFM module is bound to an interface, the Ethernet CFM module cannot be bound to other interfaces.

Example

Configure EFM and CFM to report faults to each other through the GigabitEthernet0/0/1.


```
<HUAWEI> system-view
[HUAWEI] oam-mgr
[HUAWEI-oam-mgr] oam-bind cfm md mdcustomer ma customer efm interface gigabitethernet 0/0/1
```

12.8.38 oam-bind cfm md ma trigger if-down interface

Function

The **oam-bind cfm md ma trigger if-down interface** command enables Ethernet CFM and an interface to report faults to each other.

The **undo oam-bind cfm md ma trigger if-down interface** command cancels the configuration.

By default, Ethernet CFM and an interface are not configured to report faults to each other.

Format

oam-bind cfm md *md-name* **ma** *ma-name* **trigger if-down interface** *interface-type interface-number*

undo oam-bind cfm md *md-name* **ma** *ma-name* **trigger if-down interface** *interface-type interface-number*

Parameters

Parameter	Description	Value
md *md-name*	Specifies the name of an MD.	The value is a string of 1 to 43 case-sensitive characters without spaces, hyphens (-), and question marks (?). **NOTE** When double quotation marks are used around the string, spaces are allowed in the string.
ma *ma-name*	Specifies the name of an MA.	The value is a string of 1 to 43 case-sensitive characters without spaces, hyphens (-), and question marks (?). The total length of the names of the MA and MD must be within 44 characters. **NOTE** When double quotation marks are used around the string, spaces are allowed in the string.
if-down	Indicates that an interface goes Down when Ethernet CFM on the interface detects a fault.	-

Parameter	Description	Value
interface-type interface-number	Specifies the type and number of the interface bound to CFM. • *interface-type* specifies the interface type. • *interface-number* specifies the interface number.	-

Views

OAM management view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To associate CFM with an interface, run the **oam-bind cfm md ma trigger if-down interface** command.

Precautions

Before configuring CFM and an interface to report faults to each other, pay attention to the following points:

- The MD and MA related to the Ethernet CFM module must have been created.
- The binding between an Ethernet CFM module and an interface is one-to-one. That is, when an Ethernet CFM module is bound to an interface, the Ethernet CFM module cannot be bound to other interfaces.
- A physical interface associated with CFM cannot be monitored by CFM. If CFM is associated with a physical interface monitored by itself, the link is locked.

Configure unidirectional or bidirectional transmission of fault information between Ethernet CFM and an interface. You may use the following commands when associating Ethernet CFM with an interface:

- **oam-bind cfm md ma trigger if-down interface**
- **oam-bind interface cfm md ma trigger if-down**
- **oam-bind ingress cfm md ma egress interface**
- **oam-bind ingress interface egress cfm md ma trigger if-down**

Select the preceding commands in different scenarios according to **Table 12-62**.

Table 12-62 Association between Ethernet CFM and an interface

Scenario	Configuration Solution 1	Configuration Solution 2
Faults need to be transmitted bidirectionally between Ethernet CFM and an interface.	Select either of the following commands (the two commands have the same function): • If you prefer to specify the MD and MA before the interface, use the **oam-bind cfm md ma trigger if-down interface** command. • If you prefer to specify the interface before the MD and MA, use the **oam-bind interface cfm md ma trigger if-down** command. **NOTE** After configuring Ethernet CFM and an interface to report faults to each other, run the **display current-configuration** command to check the configuration. The command output displays the **oam-bind ingress cfm md ma egress interface** and **oam-bind ingress interface egress cfm md ma trigger if-down** commands, but does not display the **oam-bind cfm md ma trigger if-down interface** or **oam-bind interface cfm md ma trigger if-down** command. The displayed commands configure reverse directions of fault transmission.	Run the following commands at a random order (each command configures fault transmission in a single direction): • **oam-bind ingress cfm md ma egress interface** • **oam-bind ingress interface egress cfm md ma trigger if-down**
Faults need to be transmitted unidirectionally between Ethernet CFM and an interface.	Select either of the following commands based on the transmission direction: • To configure Ethernet CFM to report faults to an interface, use the **oam-bind ingress cfm md ma egress interface** command. • To configure an interface to report faults to Ethernet CFM, use the **oam-bind ingress interface egress cfm md ma trigger if-down** command.	None

Example

Configure Ethernet CFM to report faults to the GigabitEthernet0/0/1.


```
<HUAWEI> system-view
[HUAWEI] oam-mgr
[HUAWEI-oam-mgr] oam-bind cfm md md1 ma ma1 trigger if-down interface gigabitethernet 0/0/1
```

12.8.39 oam-bind ingress cfm md ma egress interface

Function

The **oam-bind ingress cfm md ma egress interface** command configures Ethernet CFM to report faults to an interface.

The **undo oam-bind ingress cfm md ma egress interface** command cancels the configuration.

By default, Ethernet CFM is not configured to report faults to an interface.

Format

oam-bind ingress cfm md *md-name* **ma** *ma-name* **trigger if-down egress interface** *interface-type interface-number*

undo oam-bind ingress cfm md *md-name* **ma** *ma-name* **trigger if-down egress interface** *interface-type interface-number*

Parameters

Parameter	Description	Value
md *md-name*	Specifies the name of an MD.	The value is a string of 1 to 43 case-sensitive characters without spaces, hyphens (-), and question marks (?). **NOTE** When double quotation marks are used around the string, spaces are allowed in the string.
ma *ma-name*	Specifies the name of an MA.	The value is a string of 1 to 43 case-sensitive characters without spaces, hyphens (-), and question marks (?). The total length of the names of the MA and MD must be within 44 characters. **NOTE** When double quotation marks are used around the string, spaces are allowed in the string.
if-down	Indicates that an interface goes Down when Ethernet CFM on the interface detects a fault.	-

Parameter	Description	Value
interface-type interface-number	Specifies the type and number of the interface bound to CFM. • *interface-type* specifies the interface type. • *interface-number* specifies the interface number.	-

Views

OAM management view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To associate CFM with an interface, run the **oam-bind ingress cfm md ma egress interface** command.

Precautions

Before configuring CFM and an interface to report faults to each other, pay attention to the following points:

- Fault messages are transmitted from the ingress to the egress.
- The MD and MA related to the Ethernet CFM module must have been created.
- The binding between an Ethernet CFM module and an interface is one-to-one. That is, when an Ethernet CFM module is bound to an interface, the Ethernet CFM module cannot be bound to other interfaces.
- A physical interface associated with CFM cannot be monitored by CFM. If CFM is associated with a physical interface monitored by itself, the link is locked.

Configure unidirectional or bidirectional transmission of fault information between Ethernet CFM and an interface. You may use the following commands when associating Ethernet CFM with an interface:

- **oam-bind cfm md ma trigger if-down interface**
- **oam-bind interface cfm md ma trigger if-down**
- **oam-bind ingress cfm md ma egress interface**
- **oam-bind ingress interface egress cfm md ma trigger if-down**

Select the preceding commands in different scenarios according to **Table 12-63**.

Table 12-63 Association between Ethernet CFM and an interface

Scenario	Configuration Solution 1	Configuration Solution 2
Faults need to be transmitted bidirectionally between Ethernet CFM and an interface.	Select either of the following commands (the two commands have the same function): • If you prefer to specify the MD and MA before the interface, use the **oam-bind cfm md ma trigger if-down interface** command. • If you prefer to specify the interface before the MD and MA, use the **oam-bind interface cfm md ma trigger if-down** command. **NOTE** After configuring Ethernet CFM and an interface to report faults to each other, run the **display current-configuration** command to check the configuration. The command output displays the **oam-bind ingress cfm md ma egress interface** and **oam-bind ingress interface egress cfm md ma trigger if-down** commands, but does not display the **oam-bind cfm md ma trigger if-down interface** or **oam-bind interface cfm md ma trigger if-down** command. The displayed commands configure reverse directions of fault transmission.	Run the following commands at a random order (each command configures fault transmission in a single direction): • **oam-bind ingress cfm md ma egress interface** • **oam-bind ingress interface egress cfm md ma trigger if-down**
Faults need to be transmitted unidirectionally between Ethernet CFM and an interface.	Select either of the following commands based on the transmission direction: • To configure Ethernet CFM to report faults to an interface, use the **oam-bind ingress cfm md ma egress interface** command. • To configure an interface to report faults to Ethernet CFM, use the **oam-bind ingress interface egress cfm md ma trigger if-down** command.	None

Example

Configure CFM to report faults to the GigabitEthernet0/0/1.


```
<HUAWEI> system-view
[HUAWEI] oam-mgr
[HUAWEI-oam-mgr] oam-bind ingress cfm md md1 ma ma1 trigger if-down egress interface
gigabitethernet 0/0/1
```

12.8.40 oam-bind ingress cfm md ma egress sep segment

Function

The **oam-bind ingress cfm md ma egress sep segment** command configures CFM to report faults to a SEP segment.

The **undo oam-bind ingress cfm md ma egress sep segment** command cancels the configuration.

By default, CFM is not configured to report faults to a SEP segment.

Format

oam-bind ingress cfm md *md-name* **ma** *ma-name* **egress sep segment** *segment-id* **interface** *interface-type interface-number*

undo oam-bind ingress cfm md *md-name* **ma** *ma-name* **egress sep segment** *segment-id* **interface** *interface-type interface-number*

Parameters

Parameter	Description	Value
ingress egress	Configures CFM to report faults to a SEP segment.	-
md *md-name*	Specifies the name of an MD.	The value is a string of 1 to 43 case-sensitive characters without spaces, hyphens (-), and question marks (?). **NOTE** When double quotation marks are used around the string, spaces are allowed in the string.
ma *ma-name*	Specifies the name of an MA.	The value is a string of 1 to 43 case-sensitive characters without spaces, hyphens (-), and question marks (?). The total length of the names of the MA and MD must be within 44 characters. **NOTE** When double quotation marks are used around the string, spaces are allowed in the string.
segment *segment-id*	Specifies the ID of a SEP segment.	The value is an integer that ranges from 1 to 1024.

Parameter	Description	Value
interface-type interface-number	Specifies the type and number of an Ethernet interface. • *interface-type* specifies the interface type. • *interface-number* specifies the interface number. The Ethernet interface must have been added to the SEP segment.	-

Views

OAM management view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To associate CFM with SEP, run the **oam-bind ingress cfm md ma egress sep segment** command.

Precautions

When a device running SEP at the access layer connects to the aggregation layer, pay attention to the following points:

- When a fault occurs at the access layer, configure topology change notification so that the aggregation layer can detect the fault at the access layer. Devices in the SEP segment can update their MAC address tables and ARP tables in a timely manner.
- If a fault occurs at the aggregation layer, associate SEP with Ethernet CFM on the device between the access layer and aggregation layer so that the access layer can detect the fault at the aggregation layer. Devices at the access layer can update their MAC address tables and ARP tables.

Prerequisites

This command can take effect only when the following configurations are completed:

- Run the **cfm enable (system view)** command to enable CFM globally.
- Run the **cfm md** command in the system view to create an MD.
- Run the **ma** command in the MD view to create an MA.
- Run the **mep mep-id** command in the MA view to create a MEP.

- Run the **remote-mep** command in the MA view to create an RMEP.
- Run the **mep ccm-send enable** command in the MA view to enable the local MEP in the MA to send CCMs.
- Run the **remote-mep ccm-receive enable** command in the MA view to enable the MEP to receive CCMs from the RMEP in the same MA.
- The interface specified in this command has been added to the SEP segment.

Example

Configure CFM to report faults to SEP segment 10.

```
<HUAWEI> system-view
[HUAWEI] oam-mgr
[HUAWEI-oam-mgr] oam-bind ingress cfm md md1 ma ma1 egress sep segment 10 interface
gigabitethernet 0/0/1
```

12.8.41 oam-bind ingress cfm md ma egress efm interface

Function

The **oam-bind ingress cfm md ma egress efm interface** command configures Ethernet CFM to report faults to EFM OAM.

The **undo oam-bind ingress cfm md ma egress efm interface** command cancels the configuration.

By default, Ethernet CFM is not configured to report faults to EFM OAM.

Format

oam-bind ingress cfm md *md-name* **ma** *ma-name* **egress efm interface** *interface-type interface-number*

undo oam-bind ingress cfm md *md-name* **ma** *ma-name* **egress efm interface** *interface-type interface-number*

NOTE

This command is not supported by only the SS1720GW-E, and S1720GWR-E.

Parameters

Parameter	Description	Value
md-name	Specifies the name of an MD.	The value is a string of 1 to 43 case-sensitive characters without spaces, hyphens (-), and question marks (?).

Parameter	Description	Value
ma-name	Specifies the name of an MA.	The value is a string of 1 to 43 case-sensitive characters without spaces, hyphens (-), and question marks (?). The total length of the names of the MA and MD must be within 44 characters.
interface-type interface-number	Specifies the type and number of an Ethernet interface. • *interface-type* specifies the interface type. • *interface-number* specifies the interface number. The interface must have been enabled with EFM OAM.	-

Views

OAM management view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If EFM is deployed at one side and CFM is deployed at another side of a device, associate EFM with CFM on the device so that EFM and CFM can report faults to each other.

Association between EFM and CFM is bidirectional:

- When EFM detects a link fault, it will notify CFM of the fault.
- When CFM detects a link fault, it will notify EFM of the fault.

The following commands are used to associate EFM with CFM:

- **oam-bind cfm md ma efm interface**
- **oam-bind ingress cfm md ma egress efm interface**
- **oam-bind ingress efm interface egress cfm md ma**

Select the preceding commands in different scenarios according to **Table 12-64**.

Table 12-64 Association between EFM and CFM

Scenario	Configuration Solution 1	Configuration Solution 2
Bidirectional fault notification between EFM and CFM	The **oam-bind cfm md ma efm interface** command is used to configure EFM and CFM to report faults to each other.	Run the following commands at a random order (each command configures fault transmission in a single direction): • The **oam-bind ingress efm interface egress cfm md ma** command is used to configure EFM to report faults to CFM. • The **oam-bind ingress cfm md ma egress efm interface** command is used to configure CFM to report faults to EFM.
Unidirectional fault notification between EFM and CFM	Select either of the following commands based on the transmission direction: • Run the **oam-bind ingress efm interface egress cfm md ma** command to configure EFM to report faults to CFM. • Run the **oam-bind ingress cfm md ma egress efm interface** command to configure CFM to report faults to EFM.	None

Prerequisites

The MD and MA have been created and EFM has been enabled on the specified interface.

Example

Configure Ethernet CFM to report faults to EFM through the GigabitEthernet0/0/1.

```
<HUAWEI> system-view
[HUAWEI] oam-mgr
[HUAWEI-oam-mgr] oam-bind ingress cfm md mdcustomer ma customer egress efm interface gigabitethernet 0/0/1
```

12.8.42 oam-bind ingress efm interface egress cfm md ma

Function

The **oam-bind ingress efm interface egress cfm md ma** command configures EFM OAM to report faults to Ethernet CFM.

The **undo oam-bind ingress efm interface egress cfm md ma** command cancels the configuration.

By default, EFM OAM is not configured to report faults to Ethernet CFM.

Format

oam-bind ingress efm interface *interface-type interface-number* **egress cfm md** *md-name* **ma** *ma-name*

undo oam-bind ingress efm interface *interface-type interface-number* **egress cfm md** *md-name* **ma** *ma-name*

NOTE

This command is not supported by only the SS1720GW-E, and S1720GWR-E.

Parameters

Parameter	Description	Value
md-name	Specifies the name of an MD.	The value is a string of 1 to 43 case-sensitive characters without spaces, hyphens (-), and question marks (?). **NOTE** When double quotation marks are used around the string, spaces are allowed in the string.
ma-name	Specifies the name of an MA.	The value is a string of 1 to 43 case-sensitive characters without spaces, hyphens (-), and question marks (?). The total length of the names of the MA and MD must be within 44 characters. **NOTE** When double quotation marks are used around the string, spaces are allowed in the string.

Parameter	Description	Value
interface-type interface-number	Specifies the type and number of an Ethernet interface. • *interface-type* specifies the interface type. • *interface-number* specifies the interface number. The interface must have been enabled with EFM OAM.	-

Views

OAM management view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If EFM is deployed at one side and CFM is deployed at another side of a device, associate EFM with CFM on the device so that EFM and CFM can report faults to each other.

Association between EFM and CFM is bidirectional:

- When EFM detects a link fault, it will notify CFM of the fault.
- When CFM detects a link fault, it will notify EFM of the fault.

The following commands are used to associate EFM with CFM:

- **oam-bind cfm md ma efm interface**
- **oam-bind ingress cfm md ma egress efm interface**
- **oam-bind ingress efm interface egress cfm md ma**

Select the preceding commands in different scenarios according to **Table 12-65**.

Table 12-65 Association between EFM and CFM

Scenario	Configuration Solution 1	Configuration Solution 2
Bidirectional fault notification between EFM and CFM	The **oam-bind cfm md ma efm interface** command is used to configure EFM and CFM to report faults to each other.	Run the following commands at a random order (each command configures fault transmission in a single direction): • The **oam-bind ingress efm interface egress cfm md ma** command is used to configure EFM to report faults to CFM. • The **oam-bind ingress cfm md ma egress efm interface** command is used to configure CFM to report faults to EFM.
Unidirectional fault notification between EFM and CFM	Select either of the following commands based on the transmission direction: • Run the **oam-bind ingress efm interface egress cfm md ma** command to configure EFM to report faults to CFM. • Run the **oam-bind ingress cfm md ma egress efm interface** command to configure CFM to report faults to EFM.	None

Prerequisites

The MD and MA have been created and EFM has been enabled on the specified interface.

Example

Configure EFM to report faults to CFM through the GigabitEthernet0/0/1.

```
<HUAWEI> system-view
[HUAWEI] oam-mgr
[HUAWEI-oam-mgr] oam-bind ingress efm interface gigabitethernet 0/0/1 egress cfm md mdcustomer ma customer
```

12.8.43 oam-bind ingress interface egress cfm md ma trigger if-down

Function

The **oam-bind ingress interface egress cfm md ma trigger if-down** command configures an interface to report faults to Ethernet CFM.

The **undo oam-bind ingress interface egress cfm md ma trigger if-down** command cancels the configuration.

By default, an interface is not configured to report faults to Ethernet CFM.

Format

oam-bind ingress interface *interface-type interface-number* **egress cfm md** *md-name* **ma** *ma-name* **trigger if-down**

undo oam-bind ingress interface *interface-type interface-number* **egress cfm md** *md-name* **ma** *ma-name* **trigger if-down**

Parameters

Parameter	Description	Value
interface-type interface-number	Specifies the type and number of an interface. • *interface-type* specifies the interface type. • *interface-number* specifies the interface number.	-
md *md-name*	Specifies the name of an MD.	The value is a string of 1 to 43 case-sensitive characters without spaces, hyphens (-), and question marks (?). **NOTE** When double quotation marks are used around the string, spaces are allowed in the string.
ma *ma-name*	Specifies the name of an MA.	The value is a string of 1 to 43 case-sensitive characters without spaces, hyphens (-), and question marks (?). The total length of the names of the MA and MD must be within 44 characters. **NOTE** When double quotation marks are used around the string, spaces are allowed in the string.

Parameter	Description	Value
if-down	Indicates that the OAM management module notifies Ethernet CFM of the fault and Ethernet CFM notifies the remote end of the fault when an interface goes Down.	-

Views

OAM management view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To associate an interface with CFM, run the **oam-bind ingress interface egress cfm md ma trigger if-down** command.

Precautions

If CFM is associated with an interface on a device and a device interface goes Down, the OAM management module notifies Ethernet CFM of the fault and Ethernet CFM notifies the remote end of the fault.

Prerequisites

Unidirectional fault transmission from an interface to Ethernet CFM can be configured only when the following requirements are met:

- The MD and MA related to the Ethernet CFM module must have been created.
- The binding between an Ethernet CFM module and an interface is one-to-one. That is, when an Ethernet CFM module is bound to an interface, the Ethernet CFM module cannot be bound to other interfaces.
- A physical interface associated with CFM cannot be the one that CFM monitors. If CFM is associated with a physical interface that it monitors, the link is locked.

Configure unidirectional or bidirectional fault transmission between Ethernet CFM and an interface. You may use the following commands when associating Ethernet CFM with an interface:

- **oam-bind cfm md ma trigger if-down interface**
- **oam-bind interface cfm md ma trigger if-down**
- **oam-bind ingress cfm md ma egress interface**
- **oam-bind ingress interface egress cfm md ma trigger if-down**

Select the preceding commands in different scenarios according to **Table 12-66**.

Table 12-66 Association between Ethernet CFM and an interface

Scenario	Configuration Solution 1	Configuration Solution 2
Faults need to be transmitted bidirectionally between Ethernet CFM and an interface.	Select either of the following commands (the two commands have the same function): • If you prefer to specify the MD and MA before the interface, use the **oam-bind cfm md ma trigger if-down interface** command. • If you prefer to specify the interface before the MD and MA, use the **oam-bind interface cfm md ma trigger if-down** command. **NOTE** After configuring Ethernet CFM and an interface to report faults to each other, run the **display current-configuration** command to check the configuration. The command output displays the **oam-bind ingress cfm md ma egress interface** and **oam-bind ingress interface egress cfm md ma trigger if-down** commands, but does not display the **oam-bind cfm md ma trigger if-down interface** or **oam-bind interface cfm md ma trigger if-down** command. The displayed commands configure reverse transmission directions of fault information.	Run the following commands at a random order (each command configures fault transmission in a single direction): • **oam-bind ingress cfm md ma egress interface** • **oam-bind ingress interface egress cfm md ma trigger if-down**
Faults need to be transmitted unidirectionally between Ethernet CFM and an interface.	Select either of the following commands based on the transmission direction: • To configure Ethernet CFM to report faults to an interface, use the **oam-bind ingress cfm md ma egress interface** command. • To configure an interface to report faults to Ethernet CFM, use the **oam-bind ingress interface egress cfm md ma trigger if-down** command.	None

Example

Configure Ethernet CFM to report faults to the GigabitEthernet0/0/1.

```
<HUAWEI> system-view
[HUAWEI] oam-mgr
[HUAWEI-oam-mgr] oam-bind ingress interface gigabitethernet 0/0/1 egress cfm md md1 ma ma1
trigger if-down
```

12.8.44 oam-bind interface cfm md ma trigger if-down

Function

The **oam-bind interface cfm md ma trigger if-down** command configures an interface and Ethernet CFM to report faults to each other.

The **undo oam-bind interface cfm md ma trigger if-down** command cancels the configuration.

By default, an interface and Ethernet CFM are not configured to report faults to each other.

Format

oam-bind interface *interface-type interface-number* **cfm md** *md-name* **ma** *ma-name* **trigger if-down**

undo oam-bind interface *interface-type interface-number* **cfm md** *md-name* **ma** *ma-name* **trigger if-down**

Parameters

Parameter	Description	Value
interface-type interface-number	Specifies the type and number of an interface. • *interface-type* specifies the interface type. • *interface-number* specifies the interface number.	-
md *md-name*	Specifies the name of an MD.	The value is a string of 1 to 43 case-sensitive characters without spaces, hyphens (-), and question marks (?). **NOTE** When double quotation marks are used around the string, spaces are allowed in the string.

Parameter	Description	Value
ma *ma-name*	Specifies the name of an MA.	The value is a string of 1 to 43 case-sensitive characters without spaces, hyphens (-), and question marks (?). The total length of the names of the MA and MD must be within 44 characters. **NOTE** When double quotation marks are used around the string, spaces are allowed in the string.
if-down	Indicates that the OAM management module notifies Ethernet CFM of the fault and Ethernet CFM notifies the remote end of the fault when an interface goes Down.	-

Views

OAM management view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To associate an interface with CFM, run the **oam-bind interface cfm md ma trigger if-down** command.

Precautions

Before configuring CFM and an interface to report faults to each other, pay attention to the following points:

- The MD and MA related to the Ethernet CFM module must have been created.
- The binding between an Ethernet CFM module and an interface is one-to-one. That is, when an Ethernet CFM module is bound to an interface, the Ethernet CFM module cannot be bound to other interfaces.
- A physical interface associated with CFM cannot be monitored by CFM. If CFM is associated with a physical interface monitored by itself, the link is locked.

Configure unidirectional or bidirectional fault transmission between Ethernet CFM and an interface. You may use the following commands when associating Ethernet CFM with an interface:

- **oam-bind cfm md ma trigger if-down interface**
- **oam-bind interface cfm md ma trigger if-down**
- **oam-bind ingress cfm md ma egress interface**
- **oam-bind ingress interface egress cfm md ma trigger if-down**

Select the preceding commands in different scenarios according to **Table 12-67**.

Table 12-67 Association between Ethernet CFM and an interface

Scenario	Configuration Solution 1	Configuration Solution 2
Faults need to be transmitted bidirectionally between Ethernet CFM and an interface.	Select either of the following commands (the two commands have the same function): • If you prefer to specify the MD and MA before the interface, use the **oam-bind cfm md ma trigger if-down interface** command. • If you prefer to specify the interface before the MD and MA, use the **oam-bind interface cfm md ma trigger if-down** command. **NOTE** After configuring Ethernet CFM and an interface to report faults to each other, run the **display current-configuration** command to check the configuration. The command output displays the **oam-bind ingress cfm md ma egress interface** and **oam-bind ingress interface egress cfm md ma trigger if-down** commands, but does not display the **oam-bind cfm md ma trigger if-down interface** or **oam-bind interface cfm md ma trigger if-down** command. The displayed commands configure reverse directions of fault transmission.	Run the following commands at a random order (each command configures fault transmission in a single direction): • **oam-bind ingress cfm md ma egress interface** • **oam-bind ingress interface egress cfm md ma trigger if-down**

Scenario	Configuration Solution 1	Configuration Solution 2
Faults need to be transmitted unidirectionally between Ethernet CFM and an interface.	Select either of the following commands based on the transmission direction: • To configure Ethernet CFM to report faults to an interface, use the **oam-bind ingress cfm md ma egress interface** command. • To configure an interface to report faults to Ethernet CFM, use the **oam-bind ingress interface egress cfm md ma trigger if-down** command.	None

Example

Enable the GigabitEthernet0/0/1 to report faults to Ethernet CFM.

```
<HUAWEI> system-view
[HUAWEI] oam-mgr
[HUAWEI-oam-mgr] oam-bind interface gigabitethernet 0/0/1 cfm md md1 ma ma1 trigger if-down
```

12.8.45 oam-mgr

Function

The **oam-mgr** command displays the OAM management view.

The **undo oam-mgr** command exits from the OAM management view.

Format

oam-mgr

undo oam-mgr

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

CFM can advertise fault information to interfaces or protocol modules. Ethernet OAM fault advertisement is implemented by an OAM manager, application modules, and detection modules. An OAMMGR module associates one module with another. A detection module monitors link status and network performance. If a detection module detects a fault, it instructs the OAMMGR module to notify an application module or another detection module of the fault. After receiving the notification, the application or detection module takes measures to prevent a communication interruption or service quality deterioration. Run the **oam-mgr** command to display the MGR view before associating the CFM module and other modules.

Example

Enter the OAM management view.

```
<HUAWEI> system-view
[HUAWEI] oam-mgr
[HUAWEI-oam-mgr]
```

12.8.46 packet-priority

Function

The **packet-priority** command sets the 802.1p priority of 802.1ag packets in an MA.

The **undo packet-priority** command restores the default 802.1p priority of 802.1ag packets in an MA.

Format

packet-priority *priority*

undo packet-priority

Parameters

Parameter	Description	Value
priority	Specifies the 802.1p priority of 802.1ag packets.	The value is an integer that ranges from 0 to 7. The default value is 7. A larger value indicates a higher priority.

Views

MA view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The 802.1ag packets are the Continuity Check Message (CCM), Loopback Message (LBM), Loopback Reply (LBR), Linktrace Message (LTM), and Linktrace Reply (LTR).

The 802.1ag packets with different 802.1p priorities are transmitted differently on networks. You can use this command to change the transmission quality of 802.1ag packets on networks.

Example

Set the 802.1p priority of 802.1ag packets in an MA to 3.

```
<HUAWEI> system-view
[HUAWEI] cfm enable
[HUAWEI] cfm md md1
[HUAWEI-md-md1] ma ma1
[HUAWEI-md-md1-ma-ma1] packet-priority 3
```

12.8.47 ping mac-8021ag

Function

The **ping mac-8021ag** command enables 802.1ag MAC ping to detect connectivity faults between a MEP and an RMEP or a MIP in an MA.

Format

All views except the MA view:

ping mac-8021ag mep mep-id *mep-id* **md** *md-name* **ma** *ma-name* { **mac** *mac-address* | **remote-mep mep-id** *mep-id* } [**-c** *count* | **interface** *interface-type interface-number* | **-s** *packetsize* | **-t** *timeout* | **-p** *priority-value*] *

MA view

ping mac-8021ag mep mep-id *mep-id* { **md** *md-name* **ma** *ma-name* { **mac** *mac-address* | **remote-mep mep-id** *mep-id* } | **mac** *mac-address* | **remote-mep mep-id** *mep-id* } [**-c** *count* | **interface** *interface-type interface-number* | **-s** *packetsize* | **-t** *timeout* | **-p** *priority-value*] *

Parameters

Parameter	Description	Value
mep mep-id *mep-id*	Specifies the ID of a MEP. The MEP must have been created using the **mep mep-id** command.	The value is an integer that ranges from 1 to 8191.

Parameter	Description	Value
md *md-name*	Specifies the name of an MD.	The value is a string of 1 to 43 case-sensitive characters without spaces, hyphens (-), and question marks (?).
ma *ma-name*	Specifies the name of an MA.	The value is a string of 1 to 43 case-sensitive characters without spaces, hyphens (-), and question marks (?). The total length of the names of the MA and MD must be within 44 characters.
mac *mac-address*	Specifies the MAC address of the destination node. The destination node can be a MEP or MIP. *mac-address* specifies the MP's MAC address. **NOTE** 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.
remote-mep mep-id *mep-id*	Specifies the ID of an RMEP.	The value is an integer that ranges from 1 to 8191.
-c *count*	Specifies the number of ping attempts.	The value is an integer that ranges from 1 to 4294967295. The default value is 5.

Parameter	Description	Value
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.	-
-s *packetsize*	Specifies 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 the same as the 802.1p priority of 802.1ag packets specified in the MA view.

Views

All views

Default Level

0: Visit level

Usage Guidelines

Usage Scenario

Similar to ping, 802.1ag MAC ping enables the local device to send test packets and wait for a response to check whether the destination device is reachable. In addition, the ping operation time can be calculated at the transmit end for network performance analysis.

A device is usually configured with multiple MDs and MAs. To accurately detect connectivity of a link between two or more devices, perform either of the following operations:

- Run the **ping mac-8021ag** command in the MA view.
  - Run the **ping mac-8021ag** command without **md** *md-name* **ma** *ma-name* specified to check connectivity of links in a specified MA.
  - Run the **ping mac-8021ag** command with **md** *md-name* and **ma** *ma-name* specified to check connectivity of links based on the configured MA and MD.
- Run the **ping mac-8021ag** command in all views except the MA view to check connectivity of links based on the configured MA and MD.

Prerequisites

- The MA has been associated with a VLAN.
- The MEP has been configured in the MA.

Precautions

802.1ag MAC ping is initiated by the local MEP in the MA and destined for a MEP or a MIP of the same level on other devices. The source node and the destination node can be located in different MAs.

If the outbound interface is specified, it cannot be configured with an inward-facing MEP.

Example

Ping the MIP with a bridge MAC address of 00e0-fc00-0204 twice on the MEP in **ma1** and set the size of ping packets to 112 bytes.

```
<HUAWEI> system-view
[HUAWEI] cfm enable
[HUAWEI] cfm md md1
[HUAWEI-md-md1] ma ma1
[HUAWEI-md-md1-ma-ma1] ping mac-8021ag mep mep-id 1 mac 00e0-fc00-0204 -c 2 -s 112
Pinging 00e0-fc00-0204 with 112 bytes of data:
Reply from 00e0-fc00-0204: bytes = 112 time = 9ms
Reply from 00e0-fc00-0204: bytes = 112 time = 11ms
Packets: Sent = 2, Received = 2, Lost = 0  <0% Lost >
Minimum = 9ms, Maximum = 11ms, Average = 10ms
```

Table 12-68 Description of the **ping mac-8021ag** command output

Item	Description
Reply from 00e0-fc00-0204: bytes = 112 time = 9ms	Size and response time of ping packets sent by the destination device. When the response time is less than 1 ms, "time < 1ms" is displayed.
Packets: Sent = 2, Received = 2, Lost = 0 <0% Lost >	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.

12.8.48 remote-mep

Function

The **remote-mep** command configures an RMEP in an MA.

The **undo remote-mep** command deletes an RMEP from an MA.

Format

remote-mep mep-id *mep-id* [**mac** *mac-address*]

undo remote-mep mep-id *mep-id*

Parameters

Parameter	Description	Value
mep-id *mep-id*	Specifies the ID of an RMEP.	The value is an integer that ranges from 1 to 8191.
mac *mac-address*	Specifies the MAC address of an RMEP.	The value is in H-H-H format. An H is a hexadecimal number of 1 to 4 digits.

Views

MA view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To configure an RMEP, use this command.

Precautions

To detect CFM connectivity faults between a device and an RMEP in an MA, complete the following tasks:

- Run the **remote-mep** command to configure an RMEP in an MA.
- Run the **remote-mep ccm-receive enable** command to enable the MEP to receive CCMs from the RMEP.

To modify the bridge MAC address of the RMEP, you must delete the RMEP from an MA and then reconfigure the RMEP.

The RMEP ID must be different from the MEP ID configured on a local interface.

NOTICE

- If multiple MEPs exist in an MA, the configured RMEP corresponds to multiple MEPs.
- If one MEP exists in an MA, one or more configured RMEPs correspond to one MEP.

Example

Configure RMEP 10 in **ma1** on the device with the bridge MAC address of 00e0-fc00-0204.

```
<HUAWEI> system-view
[HUAWEI] cfm enable
[HUAWEI] cfm md md1
[HUAWEI-md-md1] ma ma1
[HUAWEI-md-md1-ma-ma1] remote-mep mep-id 10 mac 00e0-fc00-0204
```

12.8.49 remote-mep ccm-receive enable

Function

The **remote-mep ccm-receive enable** command enables a MEP on the device to receive CCMs from an RMEP in the same MA or MAC tunnel.

The **undo remote-mep ccm-receive enable** command cancels the configuration.

By default, a MEP does not receive CCMs from an RMEP.

Format

remote-mep ccm-receive [**mep-id** *mep-id*] **enable**

undo remote-mep ccm-receive [**mep-id** *mep-id*] **enable**

Parameters

Parameter	Description	Value
mep-id *mep-id*	Enables a MEP to receive CCMs from the specified RMEP. If this parameter is not specified, a MEP can receive CCMs from all RMEPs in the same MA.	The value is an integer that ranges from 1 to 8191.

Views

MA view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **remote-mep ccm-receive enable** command enables a MEP on the device to receive CCMs from an RMEP in the same MA or MAC tunnel.

Precautions

The interval at which CCMs are sent or detected cannot be changed on the device in an MA if one of the following operations is performed:

- The device is enabled to send CCMs using the **mep ccm-send enable** command.
- The device is enabled to receive CCMs using the **remote-mep ccm-receive enable** command.

The **undo mep ccm-send enable** or **undo remote mep ccm-receive enable** command must be run before the interval is reconfigured.

Prerequisites

A MEP and an RMEP have been created in the MA.

Example

Enable the device to receive CCMs from RMEP 10 in **ma1**.

```
<HUAWEI> system-view
[HUAWEI] cfm enable
[HUAWEI] cfm md md1
[HUAWEI-md-md1] ma ma1
[HUAWEI-md-md1-ma-ma1] remote-mep mep-id 10 mac 00e0-fc00-0204
[HUAWEI-md-md1-ma-ma1] remote-mep ccm-receive mep-id 10 enable
```

12.8.50 senderid-tlv-type

Function

The **senderid-tlv-type** command sets the type of the Sender ID TLV in CFM packets.

The **undo senderid-tlv-type** command restores the default type of the Sender ID TLV in CFM packets.

By default, the type of the Sender ID TLV is **defer**.

Format

senderid-tlv-type { **none** | **chassis** | **manage** | **chassis-manage** | **defer** }

undo senderid-tlv-type

Parameters

Parameter	Description	Value
none	Indicates that a sent CFM packet does not contain the Sender ID TLV.	-
chassis	Indicates that a sent CFM packet contains the chassis ID.	-
manage	Indicates that a sent CFM packet contains the management address.	-
chassis-manage	Indicates that a sent CFM packet contains the chassis ID and management address.	-
defer	Indicates that the content of the Sender ID TLV is determined by the MD object.	-

Views

MD view, default MD view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can use the **senderid-tlv-type** command to configure the type of the Sender ID TLV in CFM packets in the MD view or default MD view.

Example

Set the type of the Sender ID TLV to **manage**.

```
<HUAWEI> system-view
[HUAWEI] cfm enable
[HUAWEI] cfm default md
[HUAWEI-default-md] senderid-tlv-type manage
```

12.8.51 trace mac-8021ag

Function

The **trace mac-8021ag** command enables 802.1ag MAC trace to detect connectivity faults between a MEP and an RMEP or a MIP in an MA.

Format

All views except the MA view:

trace mac-8021ag mep mep-id *mep-id* **md** *md-name* **ma** *ma-name* { **mac** *mac-address* | **remote-mep mep-id** *mep-id* } [**interface** *interface-type interface-number* | **-t** *timeout* | **ttl** *ttl*] *

MA view:

trace mac-8021ag mep mep-id *mep-id* { **md** *md-name* **ma** *ma-name* { **mac** *mac-address* | **remote-mep mep-id** *mep-id* } | **mac** *mac-address* | **remote-mep mep-id** *mep-id* } [**interface** *interface-type interface-number* | **-t** *timeout* | **ttl** *ttl*] *

Parameters

Parameter	Description	Value
mep mep-id *mep-id*	Specifies the ID of a MEP. The MEP must have been created using the **mep mep-id** command.	The value is an integer that ranges from 1 to 8191.
md *md-name*	Specifies the name of an MD.	The value is a string of 1 to 43 case-sensitive characters without spaces, hyphens (-), and question marks (?). **NOTE** When double quotation marks are used around the string, spaces are allowed in the string.
ma *ma-name*	Specifies the name of an MA.	The value is a string of 1 to 43 case-sensitive characters without spaces, hyphens (-), and question marks (?). The total length of the names of the MA and MD must be within 44 characters. **NOTE** When double quotation marks are used around the string, spaces are allowed in the string.

Parameter	Description	Value
mac *mac-address*	Specifies the MAC address of the destination node. The destination node can be a MEP or MIP. *mac-address* specifies the MP's MAC address. 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. **NOTE** 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.	-
remote-mep mep-id *mep-id*	Specifies the ID of an RMEP.	The value is an integer that ranges from 1 to 8191.

Parameter	Description	Value
interface-type interface-number	Specifies the outbound interface on the local device for sending LTMs. • *interface-type* specifies the interface type. • *interface-number* specifies the interface number. This parameter must be specified if the forwarding entry of the destination node does not exist in the MAC address table or there is more than one interface in a VLAN.	-
-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.
ttl *ttl*	Specifies the maximum hop of LTMs.	The value is an integer that ranges from 1 to 255. The default value is 64.

Views

All views

Default Level

0: Visit level

Usage Guidelines

Usage Scenario

Similar to traceroute (tracert for short), 802.1ag MAC trace tests the path between the local device and the destination device or locates failure points by sending test packets and receiving reply packets.

A device is usually configured with multiple MDs and MAs. To locate failure points or detect connectivity of a link between one MEP to another MEP or a MIP in the same MA, perform either of the following operations:

- Run the **trace mac-8021ag** command in the MA view.

  - Run the **trace mac-8021ag** command without **md** *md-name* and **ma** *ma-name* specified to test the actual forwarding patch and locate failure points in a specified MA.
  - Run the **md** *md-name* **ma** *ma-name* command with **md** *md-name* and **ma** *ma-name* specified to test the actual forwarding patch and locate failure points based on the configured MA and MD.
- Run the **trace mac-8021ag md** *md-name* **ma** *ma-name* command in all views except the MA view to test the actual forwarding patch and locate failure points based on the configured MA and MD.

Prerequisites

- The MA has been associated with a VLAN.
- The MEP has been configured in the MA.

Precautions

A MEP initiates an 802.1ag MAC trace test to monitor reachability of the MEP's or MIP's destination address. These nodes have the same level and can be located in the same MA or different MAs.

If the outbound interface is specified, it cannot be configured with an inward-facing MEP.

Example

Trace the MEP with the MAC address of aa99-6600-5600 from the MEP in the MA **macustomer**, with the TTL of 64.

```
<HUAWEI> system-view
[HUAWEI] cfm enable
[HUAWEI] cfm md mdcustomer
[HUAWEI-md-mdcustomer] ma macustomer
[HUAWEI-md-mdcustomer-ma-macustomer] trace mac-8021ag mep mep-id 1 mac aa99-6600-5600 ttl 64
Tracing the route to aa99-6600-5600 over a maximum of 64 hops:
-------------------------------------------------------------------------------
 Hops  Ingress Mac       Ingress Port            Ingress Action      Relay Action
       Egress Mac        Egress Port             Egress Action       Ismep
-------------------------------------------------------------------------------
1      00e0-fc01-3302     Vlanif0/0/1     IngOK               RlyFDB
       00e0-fce2-36db     Vlanif0/0/1     EgrOK               NoMep
```

Table 12-69 Description of the **trace mac-8021ag** command output

Item	Description
Hops	Number of hops.
Ingress Mac	MAC address of the inbound interface for receiving LTMs on the intermediate node or destination node.
Ingress Port	Inbound interface for receiving LTMs on the intermediate node or destination node.

Item	Description
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.
Reply 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 Mac	MAC address of the outbound interface for forwarding LTMs on the intermediate node.
Egress Port	Outbound interface for forwarding LTMs on the intermediate node.
Egress Action	Action taken by the outbound interface to process LTMs: • EgrOK: The outbound interface forwards LTMs successfully. • If this field is empty, the outbound interface does not or fails to forward LTMs.
Ismep	Whether the mode of the outbound interface is a MEP: • NoMep: no • IsMep: yes

12.8.52 vlan (default MD view)

Function

The **vlan** command creates a VLAN in the default MD.

The **undo vlan** command deletes a VLAN from the default MD.

Format

vlan { *vlan-id1* [**to** *vlan-id2*] }&<1-10>

undo vlan { *vlan-id1* [**to** *vlan-id2*] }&<1-10>

Parameters

Parameter	Description	Value
vlan-id1	Specifies the start VLAN ID.	The value is an integer that ranges from 1 to 4094.
vlan-id2	Specifies the end VLAN ID.	The value 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

Default MD view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After you run the **vlan** command in the default MD view, all the interfaces in the specified VLAN can generate MIPs based on the configured MIP creation rule in the default MD.

Precautions

IEEE 802.1ag has two versions: IEEE 802.1ag Draft 7 and IEEE Standard 802.1ag-2007. This command can be used only on the device running IEEE Standard 802.1ag-2007.

If the **vlan** command is run multiple times, all configurations take effect.

NOTE

The specified VLAN cannot be associated with any MA.

Example

Associate VLAN 100 to VLAN 200 with the default MD.

```
<HUAWEI> system-view
[HUAWEI] cfm default md
[HUAWEI-default-md] vlan 100 to 200
```

12.9 Y.1731 Configuration Commands

12.9.1 Command Support

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

12.9.2 ais enable

Function

The **ais enable** command enables alarm indication signal (AIS) in an MA.

The **undo ais enable** command disables AIS in an MA.

By default, AIS is disabled.

NOTE

Only the S6730-S, S6730S-S, S6730-H, S6730S-H, S6720S-S, S6720-EI, S6720S-EI, S6735-S, S5731-S, S5731S-H, S5731S-S, S5732-H, S5731-H, S5735S-H, S5736-S, S5735-S-I, S5735S-S, S500, S5720I-SI and S5735-S support this command.

Format

ais enable

undo ais enable

Parameters

None

Views

MD view, MA view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In MD nesting scenarios, if a MEP in a low-level MD detects a fault, the MEP sends a trap to the NMS. After a certain period, a MEP in the MD of a higher level also detects the fault and sends the same trap to the NMS. Enable the AIS function in low-level and high-level MDs to suppress the MEP of the high-level MD from sending traps to the NMS.

Precautions

The **ais enable** command can be used on only the device running IEEE Standard 802.1ag-2007.

When the device processes many AIS packets, the CPU usage will become high. When the device is enabled with AIS, it is recommended that nestling layers in an

MD should be reduced and the number of interfaces associated with VLANs in an MA should be reduced.

Prerequisites

An MD has been created using the **cfm md** command and an MA has been created using the **ma** command.

Example

Create an MD named **md1**, create an MA named **ma1** in the MD, and enable the AIS function in **ma1**.

```
<HUAWEI> system-view
[HUAWEI] cfm md md1
[HUAWEI-md-md1] ma ma1
[HUAWEI-md-md1-ma-ma1] ais enable
```

12.9.3 ais interval

Function

The **ais interval** command sets the interval at which a MEP in an MA sends AIS PDUs to a MEP in a high-level MA.

The **undo ais interval** command restores the default interval.

By default, the interval at which AIS PDUs are sent is 1s.

NOTE

Only the S6730-S, S6730S-S, S6730-H, S6730S-H, S6720S-S, S6720-EI, S6720S-EI, S6735-S, S5731-S, S5731S-H, S5731S-S, S5732-H, S5731-H, S5735S-H, S5736-S, S5735-S-I, S5735S-S, S500, S5720I-SI and S5735-S support this command.

Format

ais interval *interval-value*

undo ais interval

Parameters

Parameter	Description	Value
interval-value	Specifies the interval at which AIS PDUs are sent.	The value is an integer that ranges from 1 to 60, in seconds.

Views

MA view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In MD nesting scenarios, if a MEP in a low-level MD detects a fault, the MEP sends a trap to the NMS. After a certain period, a MEP in the MD of a higher level also detects the fault and sends the same trap to the NMS. You can enable the AIS function in low-level and high-level MDs to suppress the MEP of the high-level MD from sending traps to the NMS. After AIS is enabled, set the interval at which AIS PDUs are sent according to the networking.

Precautions

The **ais interval** command can be used on only the device running IEEE Standard 802.1ag-2007.

Prerequisites

An MD has been created using the **cfm md** command, an MA has been created using the **ma** command, and AIS has been enabled using the **ais enable** command.

Example

Create an MD named **md1**, create an MA named **ma1** in the MD, and set the interval at which AIS PDUs are sent in **ma1** to 60s.

```
<HUAWEI> system-view
[HUAWEI] cfm md md1
[HUAWEI-md-md1] ma ma1
[HUAWEI-md-md1-ma-ma1] ais interval 60
```

12.9.4 ais level

Function

The **ais level** command sets the level of AIS PDUs to be sent by a MEP in an MA.

The **undo ais level** command deletes the level of AIS PDUs to be sent by a MEP in an MA.

NOTE

Only the S6730-S, S6730S-S, S6730-H, S6730S-H, S6720S-S, S6720-EI, S6720S-EI, S6735-S, S5731-S, S5731S-H, S5731S-S, S5732-H, S5731-H, S5735S-H, S5736-S, S5735-S-I, S5735S-S, S500, S5720I-SI and S5735-S support this command.

Format

ais level *level-value*

undo ais level

Parameters

Parameter	Description	Value
level-value	Specifies the level of AIS PDUs to be sent.	The value is an integer that ranges from 0 to 7.

Views

MA view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In MD nesting scenarios, if a MEP in a low-level MD detects a fault, the MEP sends a trap to the NMS. After a certain period, a MEP in the MD of a higher level also detects the fault and sends the same trap to the NMS. You can enable the AIS function in low-level and high-level MDs to suppress the MEP of the high-level MD from sending traps to the NMS. After AIS is enabled, set the level of AIS PDUs to be sent according to the networking.

Precautions

The **ais level** command can be used on only the device running IEEE Standard 802.1ag-2007.

Prerequisites

An MD has been created using the **cfm md** command, an MA has been created using the **ma** command, and AIS has been enabled using the **ais enable** command.

Example

Create an MD named **md1**, create an MA named **ma1** in the MD, and set the level of AIS PDUs to be sent to 2 in **ma1**.

```
<HUAWEI> system-view
[HUAWEI] cfm md md1
[HUAWEI-md-md1] ma ma1
[HUAWEI-md-md1-ma-ma1] ais level 2
```

12.9.5 ais link-status

Function

The **ais link-status** command configures AIS to monitor interfaces.

The **undo ais link-status** command cancels the configuration.

By default, AIS does not monitor any interface.

NOTE

Only the S6730-S, S6730S-S, S6730-H, S6730S-H, S6720S-S, S6720-EI, S6720S-EI, S6735-S, S5731-S, S5731S-H, S5731S-S, S5732-H, S5731-H, S5735S-H, S5736-S, S5735-S-I, S5735S-S, S500, S5720I-SI and S5735-S support this command.

Format

ais link-status interface *interface-type interface-number*

undo ais link-status interface *interface-type interface-number*

Parameters

Parameter	Description	Value
interface-type interface-number	Specifies the interface to be monitored by AIS. • *interface-type* specifies the interface type. • *interface-number* specifies the interface number.	-

Views

MA view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In MD nesting scenarios, if a MEP in a low-level MD detects a fault, the MEP sends a trap to the NMS. After a certain period, a MEP in the MD of a higher level also detects the fault and sends the same trap to the NMS. You can enable the AIS function in low-level and high-level MDs to suppress the MEP of the high-level MD from sending traps to the NMS. To speed up AIS PDU transmission, run the **ais link-status** command to configure AIS to monitor interfaces. In this manner, a MEP sends an AIS PDU immediately after the monitored interface goes Down. The MEP does not need to wait for the timeout of CCMs. In addition, the MEP in a high-level MD is suppressed from sending the same trap to the NMS.

NOTE

Both inward- and outward-facing MEPs can receive AIS PDUs in MD scenarios.

Precautions

The **ais link-status** command can be used on only the device running IEEE Standard 802.1ag-2007.

Prerequisites

An MD has been created using the **cfm md** command, an MA has been created using the **ma** command, and AIS has been enabled using the **ais enable** command.

Example

Create an MD named **md1**, create an MA named **ma1** in the MD, and configure AIS to monitor an interface in **ma1**.

```
<HUAWEI> system-view
[HUAWEI] cfm md md1
[HUAWEI-md-md1] ma ma1
[HUAWEI-md-md1-ma-ma1] ais link-status interface gigabitethernet 0/0/1
```

12.9.6 ais suppress-alarm

Function

The **ais suppress-alarm** command enables alarm suppression on the device.

The **undo ais suppress-alarm** command disables alarm suppression on the device.

By default, alarm suppression is disabled on the device.

NOTE

Only the S6730-S, S6730S-S, S6730-H, S6730S-H, S6720S-S, S6720-EI, S6720S-EI, S6735-S, S5731-S, S5731S-H, S5731S-S, S5732-H, S5731-H, S5735S-H, S5736-S, S5735-S-I, S5735S-S, S500, S5720I-SI and S5735-S support this command.

Format

ais suppress-alarm

undo ais suppress-alarm

Parameters

None

Views

MA view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In MD nesting scenarios, after a MEP in a high-level MD receives an AIS PDU, the MEP does not send an alarm to the NMS. If the MEP does not receive any AIS PDU within the period 3.5 times as long as the interval at which AIS PDUs are sent, the alarm suppression function is disabled automatically on the local device.

- If a MEP detects a link fault and sends an alarm to the NMS before receiving an AIS PDU, run the **ais suppress-alarm** command to enable the alarm suppression function. The MEP sends only an alarm indicating that the link fault is rectified if the MEP detects that the link fault is rectified.
- If a MEP does not detect a link fault before receiving an AIS PDU, after the **ais suppress-alarm** command is used to enable the alarm suppression function, the MEP does not send an alarm to the NMS if the MEP detects a link fault.

Precautions

The **ais suppress-alarm** command can be used on only the device running IEEE Standard 802.1ag-2007.

Prerequisites

An MD has been created using the **cfm md** command, an MA has been created using the **ma** command, and AIS has been enabled using the **ais enable** command.

Example

Create an MD named **md1**, create an MA named **ma1** in the MD, and enable alarm suppression in **ma1**.

```
<HUAWEI> system-view
[HUAWEI] cfm md md1
[HUAWEI-md-md1] ma ma1
[HUAWEI-md-md1-ma-ma1] ais suppress-alarm
```

12.9.7 ais vlan

Function

The **ais vlan** command sets the range of VLANs to which the MEP of an MA sends AIS PDUs.

The **undo ais vlan** command cancels the configuration.

NOTE

Only the S6730-S, S6730S-S, S6730-H, S6730S-H, S6720S-S, S6720-EI, S6720S-EI, S6735-S, S5731-S, S5731S-H, S5731S-S, S5732-H, S5731-H, S5735S-H, S5736-S, S5735-S-I, S5735S-S, S500, S5720I-SI and S5735-S support this command.

Format

ais vlan vid { *low-vid* [**to** *high-vid*] } &<1-10> **mep** *mep-id*

ais vlan pe-vid *pe-vid* **ce-vid** { *low-ce-vid* [**to** *high-ce-vid*] } &<1-10> **mep** *mep-id*

undo ais vlan vid { *low-vid* [**to** *high-vid*] } &<1-10> **mep** *mep-id*

undo ais vlan pe-vid *pe-vid* **ce-vid** { *low-ce-vid* [**to** *high-ce-vid*] } &<1-10> **mep** *mep-id*

undo ais vlan [**vid** | **pe-vid** *pe-vid*] **mep** *mep-id*

Parameters

Parameter	Description	Value
pe-vid *pe-vid*	Specifies the VLAN ID in the outer tag of a VLAN frame.	The value is an integer that ranges from 1 to 4094.
ce-vid *low-ce-vid*	Specifies the lower limit of the VLAN ID in the inner tag of a VLAN frame.	The value is an integer that ranges from 1 to 4094.
high-ce-vid	Specifies the upper limit of the VLAN ID in the inner tag of a VLAN frame.	The value is an integer that ranges from 1 to 4094.
vid *low-vid*	Specifies the lower limit of the VLAN ID in an AIS PDU.	The value is an integer that ranges from 1 to 4094.
high-vid	Specifies the upper limit of the VLAN ID in an AIS PDU.	The value is an integer that ranges from 1 to 4094.
mep *mep-id*	Specifies the ID of a MEP. The ID identifies a MEP. The MEP ID must be unique in an MA and in a VLAN.	The value is an integer that ranges from 1 to 8191.

Views

MA view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can run the **ais vlan** command to set the range of VLANs to which the AIS PDUs to be sent. This prevents the MEP from sending AIS PDUs to all VLANs and reduces the load of the system.

Precautions

The **ais vlan** command can be used on only the device running IEEE Standard 802.1ag-2007.

If the **ais vlan** command is run more than once, all configurations take effect.

Prerequisites

An MD has been created using the **cfm md** command, an MA has been created using the **ma** command, and AIS has been enabled using the **ais enable** command.

Example

Create an MD named **md1**, create an MA named **ma1** in the MD, and set the outer VLAN ID in outgoing AIS PDUs to 10 and set the inner VLAN ID range to 1 to 100.

```
<HUAWEI> system-view
[HUAWEI] cfm md md1
[HUAWEI-md-md1] ma ma1
[HUAWEI-md-md1-ma-ma1] ais vlan pe-vid 10 ce-vid 1 to 100 mep 1
```

Create an MD named **md1**, create an MA named **ma1** in the MD, and set the range of VLANs to which AIS PDUs are to be sent to 1 to 100 in **ma1**.

```
<HUAWEI> system-view
[HUAWEI] cfm md md1
[HUAWEI-md-md1] ma ma1
[HUAWEI-md-md1-ma-ma1] ais vlan vid 1 to 100 mep 1
```

12.9.8 delay-measure one-way continual

Function

The **delay-measure one-way continual** command configures proactive one-way frame delay measurement.

The **undo delay-measure one-way continual** command cancels the configuration.

By default, proactive one-way frame delay measurement is not configured in an MA.

Format

delay-measure one-way continual send mep *mep-id* { **mac** *mac-address* | **remote-mep** *mep-id* } **interval** { **1000** | **10000** | **30000** | **60000** | **150000** | **300000** }

undo delay-measure one-way continual send [**mep** *mep-id*]

Parameters

Parameter	Description	Value
mep *mep-id*	Specifies the ID of a MEP.	The value is an integer in the range from 1 to 8191.
mac *mac-address*	Specifies the MAC address of an RMEP.	-
remote-mep *mep-id*	Specifies the ID of an RMEP.	The value is an integer in the range from 1 to 8191.
interval { **1000** | **10000** | **30000** | **60000** | **150000** | **300000** }	Specifies the interval at which DM frames are sent.	The value is 1000, 10000, 30000, 60000, 150000, and 300000, in milliseconds.

Views

MA view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Proactive OAM indicates that OAM actions are carried out continuously.

One-way frame delay measurement is implemented between two MEPs by exchanging DM frames. A MEP periodically sends DM frames carrying TxTimeStampf. After receiving a DM frame, the RMEP parses TxTimeStampf and compares this value with RxTimef (the time when the 1DM frame was received). The RMEP calculates the one-way frame delay based on these values using the following formula: Frame delay = RxTimef - TxTimeStampf

When clocks of the MEPs at both ends of a link are synchronized, the **delay-measure one-way continual** command can be used to implement proactive one-way frame delay measurement for a VLAN.

To implement proactive one-way frame delay measurement, specify the RMEP ID or destination MAC address, and interval at which DM frames are sent:

- If the local MEP has not learned the RMEP MAC address, you must specify the destination MAC address for frame delay measurement.
- If the local MEP has learned the RMEP MAC address, you can specify the RMEP ID for frame delay measurement.

Prerequisites

The command takes effect only after the following configurations are completed:

- Run the **cfm version standard** command in the system view to specify IEEE Standard 802.1ag-2007 for CFM.
- Run the **cfm enable (system view)** command to enable CFM globally.
- Run the **cfm md** command in the system view to create an MD.
- Run the **ma** command in the MD view to create an MA.
- Run the **mep mep-id** command in the MA view to create an inward-facing MEP.

If **remote-mep** *mep-id* is specified in the **delay-measure one-way continual** command, the following configurations must be completed:

- Run the **remote-mep** command in the MA view to create an RMEP.
- Run the **mep ccm-send enable** command in the MA view to enable the local MEP in the MA to send CCMs.
- Run the **remote-mep ccm-receive enable** command in the MA view to enable the MEP to receive CCMs from the RMEP in the same MA.

Precautions

- IEEE 802.1ag has two versions: IEEE 802.1ag Draft 7 and IEEE Standard 802.1ag-2007. This command can be used only on the device running IEEE Standard 802.1ag-2007.
- One-way frame delay measurement can be implemented only after the MEP synchronizes the time with its RMEP.

If the configuration changes during on-demand statistics, you can view only the pre-change statistics results. You are advised to run the command for on-demand statistics again for query.

Example

In a VLAN, enable proactive one-way frame delay measurement and set the destination MAC address to 01-22-33 and the interval at which DM frames are sent to 1000 ms.

```
<HUAWEI> system-view
[HUAWEI] cfm enable
[HUAWEI] cfm md md1
[HUAWEI-md-md1] ma ma1
[HUAWEI-md-md1-ma-ma1] map vlan 2
[HUAWEI-md-md1-ma-ma1] delay-measure one-way continual send mep 1 mac 01-22-33 interval 1000
```

In a VLAN, enable proactive one-way frame delay measurement and set the RMEP ID to 2 and the interval at which DM frames are sent to 1000 ms.

```
<HUAWEI> system-view
[HUAWEI] cfm enable
[HUAWEI] cfm md md1
[HUAWEI-md-md1] ma ma1
[HUAWEI-md-md1-ma-ma1] map vlan 2
[HUAWEI-md-md1-ma-ma1] delay-measure one-way continual send mep 1 remote-mep 2 interval 1000
```

12.9.9 delay-measure one-way continual receive

Function

The **delay-measure one-way continual receive** command configures the RMEP to receive DM frames to implement proactive one-way frame delay measurement.

The **undo delay-measure one-way continual receive** command cancels the configuration.

By default, the RMEP enabled with proactive one-way frame delay measurement in an MA is not configured to receive DM frames.

Format

delay-measure one-way continual receive mep *mep-id*

undo delay-measure one-way continual receive [**mep** *mep-id*]

Parameters

Parameter	Description	Value
mep *mep-id*	Specifies the ID of a MEP.	The value is an integer that ranges from 1 to 8191.

Views

MA view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

This command is used in the VLAN scenario to enable the RMEP to receive DM frames to implement proactive one-way frame delay measurement.

Prerequisites

The command takes effect only after the following configurations are completed:

- Run the **cfm version standard** command in the system view to specify IEEE Standard 802.1ag-2007 for CFM.
- Run the **cfm enable (system view)** command to enable CFM globally.
- Run the **cfm md** command in the system view to create an MD.
- Run the **ma** command in the MD view to create an MA.
- Run the **mep mep-id** command in the MA view to create an inward-facing MEP.

Precautions

After the configuration is complete, the remote device can receive DMMs to implement proactive one-way frame delay measurement.

IEEE 802.1ag has two versions: IEEE 802.1ag Draft 7 and IEEE Standard 802.1ag-2007. This command can be used only on the device running IEEE Standard 802.1ag-2007.

Example

Configure the RMEP to receive DM frames in a VLAN.

```
<HUAWEI> system-view
[HUAWEI] cfm enable
[HUAWEI] cfm md md2
[HUAWEI-md-md2] ma ma2
[HUAWEI-md-md2-ma-ma2] map vlan 2
[HUAWEI-md-md2-ma-ma2] mep mep-id 2 interface gigabitethernet 0/0/1 inward
[HUAWEI-md-md2-ma-ma2] delay-measure one-way continual receive mep 2
```


12.9.10 delay-measure one-way send

Function

The **delay-measure one-way send** command configures on-demand one-way frame delay measurement.

By default, on-demand one-way frame delay measurement is not configured in an MA.

Format

delay-measure one-way send mep *mep-id* { **mac** *mac-address* | **remote-mep** *mep-id* } **interval** { **1000** | **10000** } **count** *count-value*

Parameters

Parameter	Description	Value
mac *mac-address*	Specifies the MAC address of an RMEP.	-
remote-mep *mep-id*	Specifies the ID of an RMEP.	The value is an integer that ranges from 1 to 8191.
interval	Specifies the interval at which DM frames are sent.	The value is 1000 or 10000, in milliseconds.
count *count-value*	Specifies the one-way frame delay measurement count. **NOTE** *count-value* must be configured. There is no default value.	The value is an integer that ranges from 1 to 60.

Views

MA view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On-demand OAM indicates that OAM actions are initiated by manual configuration in a limited period of time. On-demand OAM may cause singular or periodic OAM actions during the diagnostic period. DM frames can be used for on-demand OAM to test the link delay.

One-way frame delay measurement is implemented between two MEPs by exchanging DM frames. A MEP periodically sends DM frames carrying

TxTimeStampf. After receiving a DM frame, the RMEP parses TxTimeStampf and compares this value with RxTimef (the time when the 1DM frame was received). The RMEP calculates the one-way frame delay based on these values using the following formula: Frame delay = RxTimef - TxTimeStampf

Prerequisites

The command takes effect only after the following configurations are completed:

- Run the **cfm version standard** command in the system view to specify IEEE Standard 802.1ag-2007 for CFM.
- Run the **cfm enable (system view)** command to enable CFM globally.
- Run the **cfm md** command in the system view to create an MD.
- Run the **ma** command in the MD view to create an MA.
- In a VLAN, outward-facing MEPs are supported. Perform the following operation to create a MEP in the MA view:
  - Run the **mep mep-id** command with *outward* specified to create an outward-facing MEP.

If **remote-mep** *mep-id* is specified in the **delay-measure one-way mep** command, the following configurations must be completed:

- Run the **remote-mep** command in the MA view to create an RMEP.
- Run the **mep ccm-send enable** command in the MA view to enable the local MEP in the MA to send CCMs.
- Run the **remote-mep ccm-receive enable** command in the MA view to enable the MEP to receive CCMs from the RMEP in the same MA.

Precautions

- One-way frame delay measurement can be implemented only after the MEP synchronizes the time with its RMEP.
- To implement one-way frame delay measurement, specify the RMEP ID or destination MAC address, interval at which DM frames are sent, and measurement count:
  - If the local MEP has not learned the RMEP MAC address, you must specify the destination MAC address for one-way frame delay measurement.
  - If the local MEP has learned the RMEP MAC address, you can specify the RMEP ID for one-way frame delay measurement.
- IEEE 802.1ag has two versions: IEEE 802.1ag Draft 7 and IEEE Standard 802.1ag-2007. This command can be used only on the device running IEEE Standard 802.1ag-2007.

If the configuration changes during on-demand statistics, you can view only the pre-change statistics results. You are advised to run the command for on-demand statistics again for query.

Example

In a VLAN, enable one-way frame delay measurement and set the destination MAC address to 01-22-33, interval at which DM frames are sent to 10000 ms, and measurement count to 60.


```
<HUAWEI> system-view
[HUAWEI] cfm enable
[HUAWEI] cfm md md1
[HUAWEI-md-md1] ma ma1
[HUAWEI-md-md1-ma-ma1] map vlan 2
[HUAWEI-md-md1-ma-ma1] delay-measure one-way send mep 1 mac 01-22-33 interval 10000 count 60
```

In a VLAN, enable one-way frame delay measurement and set the RMEP ID to 2, interval at which DM frames are sent to 10000 ms, and measurement count to 60.

```
<HUAWEI> system-view
[HUAWEI] cfm enable
[HUAWEI] cfm md md1
[HUAWEI-md-md1] ma ma1
[HUAWEI-md-md1-ma-ma1] map vlan 2
[HUAWEI-md-md1-ma-ma1] delay-measure one-way send mep 1 remote-mep 2 interval 10000 count
60
```

12.9.11 delay-measure one-way receive

Function

The **delay-measure one-way receive** command enables the RMEP to receive DM frames to implement one-way frame delay measurement.

The **undo delay-measure one-way receive** command cancels the configuration.

By default, the RMEP is not enabled to receive DM frames.

Format

delay-measure one-way receive mep *mep-id*

undo delay-measure one-way receive [**mep** *mep-id*]

Parameters

Parameter	Description	Value
mep *mep-id*	Specifies the ID of a MEP.	The value is an integer that ranges from 1 to 8191.

Views

MA view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

This command is used in a VLAN to enable the RMEP to receive DM frames to implement one-way frame delay measurement.

Prerequisites

The command takes effect only after the following configurations are completed:

- Run the **cfm version standard** command in the system view to specify IEEE Standard 802.1ag-2007 for CFM.
- Run the **cfm enable (system view)** command to enable CFM globally.
- Run the **cfm md** command in the system view to create an MD.
- Run the **ma** command in the MD view to create an MA.
- Run the **mep mep-id** command in the MA view to create an inward-facing MEP.

Precautions

IEEE 802.1ag has two versions: IEEE 802.1ag Draft 7 and IEEE Standard 802.1ag-2007. This command can be used only on the device running IEEE Standard 802.1ag-2007.

Example

Configure the RMEP to receive DM frames in a VLAN.

```
<HUAWEI> system-view
[HUAWEI] cfm enable
[HUAWEI] cfm md md3
[HUAWEI-md-md3] ma ma3
[HUAWEI-md-md3-ma-ma3] map vlan 10
[HUAWEI-md-md3-ma-ma3] mep mep-id 3 interface gigabitethernet 0/0/1 inward
[HUAWEI-md-md3-ma-ma3] delay-measure one-way receive mep 3
```

12.9.12 delay-measure one-way threshold

Function

The **delay-measure one-way threshold** command sets the alarm threshold for one-way frame delay measurement.

The **undo delay-measure one-way threshold** command cancels the configuration.

Format

delay-measure one-way threshold *threshold-value*

undo delay-measure one-way threshold

Parameters

Parameter	Description	Value
threshold-value	Specifies the alarm threshold for one-way frame delay measurement.	The value is an integer that ranges from 1 to 4294967295, in microseconds.

Views

MA view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **delay-measure one-way threshold** command sets an alarm threshold for one-way frame delay measurement between a MEP and an RMEP. When the one-way frame delay exceeds the alarm threshold, an alarm is generated.

Precautions

IEEE 802.1ag has two versions: IEEE 802.1ag Draft 7 and IEEE Standard 802.1ag-2007. This command can be used only on the device running IEEE Standard 802.1ag-2007.

This command is applicable to VLANs.

NOTE

Before setting the alarm threshold, you must correctly configure the MD and MA.

Example

Set the alarm threshold for one-way frame delay measurement in the VLAN to 10.

```
<HUAWEI> system-view
[HUAWEI] cfm enable
[HUAWEI] cfm md md1
[HUAWEI-md-md1] ma ma1
[HUAWEI-md-md1-ma-ma1] map vlan 100
[HUAWEI-md-md1-ma-ma1] delay-measure one-way threshold 10
```

12.9.13 delay-measure two-way continual

Function

The **delay-measure two-way continual** command configures proactive two-way frame delay measurement.

The **undo delay-measure two-way continual** command cancels the configuration.

By default, proactive two-way frame delay measurement is not configured in an MA.

Format

delay-measure two-way continual send mep *mep-id* { **mac** *mac-address* | **remote-mep** *mep-id* } **interval** { **1000** | **10000** | **30000** | **60000** | **150000** | **300000** }

undo delay-measure two-way continual send [**mep** *mep-id*]

Parameters

Parameter	Description	Value
mep *mep-id*	Specifies the ID of a MEP.	The value is an integer that ranges from 1 to 8191.
mac *mac-address*	Specifies the MAC address of an RMEP.	-
remote-mep *mep-id*	Specifies the ID of an RMEP.	The value is an integer that ranges from 1 to 8191.
interval { **1000** | **10000** | **30000** | **60000** | **150000** | **300000** }	Specifies the interval at which DMMs frames are sent.	The value is 1000, 10000, 30000, 60000, 150000, and 300000, in milliseconds.

Views

MA view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Proactive OAM indicates that OAM actions are carried out continuously.

Two-way frame delay measurement is performed by a local MEP to send a DMM to its RMEP and then receive a DMR from the RMEP. After the two-way frame delay measurement is configured, a MEP periodically sends DMMs carrying TxTimeStampf (the time when the DMM was sent). After receiving the DMM, the RMEP replies with a DMR. The DMR carries RxTimeStampf (the time when the DMM was received) and TxTimeStampb (the time when the DMR was sent). The value in every field of the DMM is copied to the DMR except that the source and destination MAC addresses were interchanged. Upon receiving the DMR, the MEP calculates the two-way frame delay by using the following formula: Frame delay = (RxTimeb - TxTimeStampf) - (TxTimeStampb - RxTimeStampf)

When clocks of the MEPs at both ends of a link are not synchronized, the **delay-measure two-way continual** command can be used to implement proactive two-way frame delay measurement for a VLAN.

To implement proactive two-way frame delay measurement, you need to specify the RMEP ID or destination MAC address, interval at which DMMs are sent, and measurement count:

- If the local MEP has not learned the RMEP MAC address, you must specify the destination MAC address for two-way frame delay measurement.

- If the local MEP has learned the RMEP MAC address, you can specify the RMEP ID for two-way frame delay measurement.

Prerequisites

The command takes effect only after the following configurations are completed:

- Run the **cfm version standard** command in the system view to specify IEEE Standard 802.1ag-2007 for CFM.
- Run the **cfm enable (system view)** command to enable CFM globally.
- Run the **cfm md** command in the system view to create an MD.
- Run the **ma** command in the MD view to create an MA.
- Run the **mep mep-id** command with *inward* specified in the MA view to create an inward-facing MEP.

If **remote-mep** *mep-id* is specified in the **delay-measure two-way continual** command, the following configurations need to be completed in addition to the preceding configurations:

- Run the **remote-mep** command in the MA view to create an RMEP.
- Run the **mep ccm-send enable** command in the MA view to enable the local MEP in the MA to send CCMs.
- Run the **remote-mep ccm-receive enable** command in the MA view to enable the MEP to receive CCMs from the RMEP in the same MA.

Precautions

IEEE 802.1ag has two versions: IEEE 802.1ag Draft 7 and IEEE Standard 802.1ag-2007. This command can be used only on the device running IEEE Standard 802.1ag-2007.

Example

In a VLAN, enable proactive two-way frame delay measurement and set the destination MAC address to 01-22-33 and the interval at which DMMs are sent to 30s.

```
<HUAWEI> system-view
[HUAWEI] cfm enable
[HUAWEI] cfm md md1
[HUAWEI-md-md1] ma ma1
[HUAWEI-md-md1-ma-ma1] map vlan 2
[HUAWEI-md-md1-ma-ma1] delay-measure two-way continual send mep 1 mac 01-22-33 interval 30000
```

In a VLAN, enable proactive two-way frame delay measurement and set the RMEP ID to 2 and the interval at which DMMs are sent to 30s.

```
<HUAWEI> system-view
[HUAWEI] cfm enable
[HUAWEI] cfm md md1
[HUAWEI-md-md1] ma ma1
[HUAWEI-md-md1-ma-ma1] map vlan 2
[HUAWEI-md-md1-ma-ma1] delay-measure two-way continual send mep 1 remote-mep 2 interval 30000
```


12.9.14 delay-measure two-way continual send test-id

Function

The **delay-measure two-way continual send test-id** command configures two-way proactive frame delay measurement (DM).

The **undo delay-measure two-way continual send test-id** command deletes the configuration.

By default, two-way proactive frame DM is not configured in an MA.

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

delay-measure two-way continual send test-id *test-id* **interval** { **1000** | **10000** | **15000** | **30000** } [**packet-size** *packet-size*]

undo delay-measure two-way continual send test-id *test-id*

Parameters

Parameter	Description	Value
test-id	Specifies the ID of a test instance.	The value is an integer ranging from 1 to 4294967295.
interval { **1000** | **10000** | **15000** | **30000** }	Specifies the interval at which DMMs are sent.	Enumerated value, in milliseconds: • 1000 • 10000 • 15000 • 30000
packet-size *packet-size*	Specifies the size of the sent packets.	The value is an integer ranging from 64 to 1518, in bytes. The default value is 64.

Views

MA view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In VLAN scenarios, to implement two-way proactive frame DM, run the **delay-measure two-way continual** command. This command does not take effect in point-to-multipoint link scenarios. To implement two-way proactive frame DM for point-to-multipoint links, run the **delay-measure two-way continual send test-id** command.

Prerequisites

A test instance has been created using the **test-id** command in the MA view.

Precautions

The **delay-measure two-way continual send test-id** and **delay-measure two-way continual** commands are mutually exclusive.

Example

Configure two-way proactive frame DM with the test instance of 1 and DMM transmission interval of 30s.

```
<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] quit
[HUAWEI] set service-mode enhanced
Warning: This command will effect forward performance. Continue? [Y/N]:y
[HUAWEI] cfm enable
[HUAWEI] cfm md md1
[HUAWEI-md-md1] ma ma1
[HUAWEI-md-md1-ma-ma1] map vlan 100
[HUAWEI-md-md1-ma-ma1] mep mep-id 1 interface gigabitethernet 0/0/1 inward
[HUAWEI-md-md1-ma-ma1] remote-mep mep-id 2
[HUAWEI-md-md1-ma-ma1] mep ccm-send enable
[HUAWEI-md-md1-ma-ma1] remote-mep ccm-receive enable
[HUAWEI-md-md1-ma-ma1] test-id 1 mep 1 remote-mep 2
[HUAWEI-md-md1-ma-ma1] delay-measure two-way continual send test-id 1 interval 30000
```

12.9.15 delay-measure two-way delay-threshold test-id

Function

The **delay-measure two-way delay-threshold test-id** command configures alarm thresholds for two-way proactive frame delay measurement (DM).

The **undo delay-measure two-way delay-threshold test-id** command deletes the alarm thresholds configured for two-way proactive frame DM.

By default, no alarm thresholds are configured for two-way proactive frame DM.

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

delay-measure two-way delay-threshold test-id *test-id* **upper-limit** *upper-limit* **lower-limit** *lower-limit*

undo delay-measure two-way delay-threshold test-id *test-id* [**upper-limit** *upper-limit* **lower-limit** *lower-limit*]

Parameters

Parameter	Description	Value
test-id	Specifies the ID of a test instance.	The value is an integer ranging from 1 to 4294967295.
upper-limit *upper-limit*	Specifies an upper alarm threshold for two-way proactive frame DM.	The value is an integer ranging from 0 to 4294967295, in microseconds.
lower-limit *lower-limit*	Specifies a lower alarm threshold for two-way proactive frame DM.	The value is an integer ranging from 0 to 4294967295, in microseconds. The lower alarm threshold must be less than the upper alarm threshold.

Views

MA view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To configure upper and lower alarm thresholds for two-way proactive frame DM that monitors link quality, run the **delay-measure two-way delay-threshold test-id** command. After configuring upper and lower alarm thresholds, you can obtain data (such as the number of times that a threshold-crossing event occurs) within a sampling period to monitor network performance.

Prerequisites

A test instance has been created using the **test-id** command in the MA view.

Precautions

Thresholds can be configured only for two-way proactive frame DM and cannot be configured for two-way on-demand frame DM.

Example

Set lower and upper alarm thresholds for two-way proactive frame DM in VLAN scenarios to 200 microseconds and 400 microseconds, respectively.

```
<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] quit
```



```
[HUAWEI] set service-mode enhanced
Warning: This command will effect forward performance. Continue? [Y/N]:y
[HUAWEI] cfm enable
[HUAWEI] cfm md md1
[HUAWEI-md-md1] ma ma1
[HUAWEI-md-md1-ma-ma1] map vlan 100
[HUAWEI-md-md1-ma-ma1] mep mep-id 1 interface gigabitethernet 0/0/1 inward
[HUAWEI-md-md1-ma-ma1] remote-mep mep-id 2
[HUAWEI-md-md1-ma-ma1] mep ccm-send enable
[HUAWEI-md-md1-ma-ma1] remote-mep ccm-receive enable
[HUAWEI-md-md1-ma-ma1] test-id 1 mep 1 remote-mep 2
[HUAWEI-md-md1-ma-ma1] delay-measure two-way delay-threshold test-id 1 upper-limit 400 lower-limit 200
```

12.9.16 delay-measure two-way send

Function

The **delay-measure two-way send** command configures on-demand two-way frame delay measurement.

By default, on-demand two-way frame delay measurement is not configured in an MA.

Format

delay-measure two-way send mep *mep-id* { **mac** *mac-address* | **remote-mep** *mep-id* } **interval** { **1000** | **10000** } **count** *count-value*

Parameters

Parameter	Description	Value
mep *mep-id*	Specifies the ID of a MEP.	The value is an integer that ranges from 1 to 8191.
mac *mac-address*	Specifies the MAC address of an RMEP.	-
remote-mep *mep-id*	Specifies the ID of an RMEP.	The value is an integer that ranges from 1 to 8191.
interval	Specifies the interval at which DMMs are sent.	The value is 1000 or 10000, in milliseconds.
count *count-value*	Specifies the number of sent DMMs.	The value is an integer that ranges from 1 to 60.

Views

MA view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On-demand OAM indicates that OAM actions are initiated by manual configuration in a limited period of time. On-demand OAM may cause singular or periodic OAM actions during the diagnostic period. DM frames can be used for on-demand OAM to test the link delay.

Two-way frame delay measurement is performed by a local MEP to send a DMM to its RMEP and then receive a DMR from the RMEP. After the two-way frame delay measurement is configured, a MEP periodically sends DMMs carrying TxTimeStampf (the time when the DMM was sent). After receiving the DMM, the RMEP replies with a DMR. The DMR carries RxTimeStampf (the time when the DMM was received) and TxTimeStampb (the time when the DMR was sent). The value in every field of the DMM is copied to the DMR except that the source and destination MAC addresses were interchanged. Upon receiving the DMR, the MEP calculates the two-way frame delay by using the following formula: Frame delay = (RxTimeb - TxTimeStampf) - (TxTimeStampb - RxTimeStampf)

Prerequisites

The command takes effect only after the following configurations are completed:

- Run the **cfm version standard** command in the system view to specify IEEE Standard 802.1ag-2007 for CFM.
- Run the **cfm enable (system view)** command to enable CFM globally.
- Run the **cfm md** command in the system view to create an MD.
- Run the **ma** command in the MD view to create an MA.

If **remote-mep** *mep-id* is specified in this command, the following configurations need to be completed in addition to the preceding configurations:

- Run the **remote-mep** command in the MA view to create an RMEP.
- Run the **mep ccm-send enable** command in the MA view to enable the local MEP in the MA to send CCMs.
- Run the **remote-mep ccm-receive enable** command in the MA view to enable the MEP to receive CCMs from the RMEP in the same MA.

Precautions

- IEEE 802.1ag has two versions: IEEE 802.1ag Draft 7 and IEEE Standard 802.1ag-2007. This command can be used only on the device running IEEE Standard 802.1ag-2007.
- To implement on-demand two-way frame delay measurement, you need to specify the RMEP ID or destination MAC address, interval at which DMMs are sent, and measurement count:
  - If the local MEP has not learned the RMEP MAC address, you must specify the destination MAC address for two-way frame delay measurement.
  - If the local MEP has learned the RMEP MAC address, you can specify the RMEP ID for two-way frame delay measurement.

If the configuration changes during on-demand statistics, you can view only the pre-change statistics results. You are advised to run the command for on-demand statistics again for query.

Example

In a VLAN, enable on-demand two-way frame delay measurement and set the destination MAC address to 01-22-33, interval at which DMMs are sent to 10000 ms, and measurement count to 60.

```
<HUAWEI> system-view
[HUAWEI] cfm enable
[HUAWEI] cfm md md1
[HUAWEI-md-md1] ma ma1
[HUAWEI-md-md1-ma-ma1] map vlan 100
[HUAWEI-md-md1-ma-ma1] delay-measure two-way send mep 1 mac 01-22-33 interval 10000 count 60
```

In a VLAN, enable on-demand two-way frame delay measurement and set the RMEP ID to 2, interval at which DMMs are sent to 10000 ms, and measurement count to 60.

```
<HUAWEI> system-view
[HUAWEI] cfm enable
[HUAWEI] cfm md md1
[HUAWEI-md-md1] ma ma1
[HUAWEI-md-md1-ma-ma1] map vlan 100
[HUAWEI-md-md1-ma-ma1] delay-measure two-way send mep 1 remote-mep 2 interval 10000 count 60
```

12.9.17 delay-measure two-way receive

Function

The **delay-measure two-way receive** command enables the RMEP to receive DMMs to implement two-way frame delay measurement.

The **undo delay-measure two-way receive** command cancels the configuration.

By default, the RMEP in an MA is not enabled to receive DMMs.

Format

delay-measure two-way receive mep *mep-id*

undo delay-measure two-way receive [**mep** *mep-id*]

Parameters

Parameter	Description	Value
mep *mep-id*	Specifies the ID of a MEP.	The value is an integer that ranges from 1 to 8191.

Views

MA view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

This command is used to enable the RMEP to receive DMMs to implement proactive or on-demand two-way frame delay measurement. This command is used in a VLAN where an outward-facing MEP is configured with two-way frame delay measurement.

Prerequisites

The command takes effect only after the following configurations are completed:

- Run the **cfm version standard** command in the system view to specify IEEE Standard 802.1ag-2007 for CFM.
- Run the **cfm enable (system view)** command to enable CFM globally.
- Run the **cfm md** command in the system view to create an MD.
- Run the **ma** command in the MD view to create an MA.
- Run the **remote-mep** command in the MA view to create an RMEP.

Precautions

IEEE 802.1ag has two versions: IEEE 802.1ag Draft 7 and IEEE Standard 802.1ag-2007. This command can be used only on the device running IEEE Standard 802.1ag-2007.

Example

Enable the RMEP to receive DMMs in the MA **ma1** and MD **md1**, with the VLAN ID as 100.

```
<HUAWEI> system-view
[HUAWEI] cfm enable
[HUAWEI] cfm md md1
[HUAWEI-md-md1] ma ma1
[HUAWEI-md-md1-ma-ma1] map vlan 100
[HUAWEI-md-md1-ma-ma1] mep mep-id 1 interface gigabitethernet 0/0/1 outward
[HUAWEI-md-md1-ma-ma1] delay-measure two-way receive mep 1
```

12.9.18 delay-measure two-way receive test-id

Function

The **delay-measure two-way receive test-id** command enables a Remote Maintenance Association End Point (RMEP) to receive Delay Measure Messages (DMMs) for two-way frame delay measurement (DM).

The **undo delay-measure two-way receive test-id** command disables an RMEP from receiving DMMs for two-way frame DM.

By default, the RMEP in a Maintenance Association (MA) is disabled from receiving DMMs.

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

delay-measure two-way receive test-id *test-id*

undo delay-measure two-way receive [**test-id** *test-id*]

Parameters

Parameter	Description	Value
test-id	Specifies the ID of a test instance.	The value is an integer ranging from 1 to 4294967295.

Views

MA view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After running the **delay-measure two-way continual send test-id** or **delay-measure two-way send test-id** command to enable a MEP to send DMMs for two-way frame DM, run the **delay-measure two-way receive test-id** command to enable the RMEP to receive DMMs.

Prerequisites

A test instance has been created using the **test-id** command in the MA view.

Precautions

The **delay-measure two-way receive test-id** and **delay-measure two-way receive** commands are mutually exclusive.

Example

Enable the RMEP to receive DMMs for two-way frame DM with the test instance of 1.

```
<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] quit
[HUAWEI] set service-mode enhanced
Warning: This command will effect forward performance. Continue? [Y/N]:y
[HUAWEI] cfm enable
```



```
[HUAWEI] cfm md md1
[HUAWEI-md-md1] ma ma1
[HUAWEI-md-md1-ma-ma1] map vlan 100
[HUAWEI-md-md1-ma-ma1] mep mep-id 1 interface gigabitethernet 0/0/1 inward
[HUAWEI-md-md1-ma-ma1] remote-mep mep-id 2
[HUAWEI-md-md1-ma-ma1] test-id 1 mep 1 remote-mep 2
[HUAWEI-md-md1-ma-ma1] delay-measure two-way receive test-id 1
```

12.9.19 delay-measure two-way send test-id

Function

The **delay-measure two-way send test-id** command configures on-demand two-way frame delay measurement based on the test instance.

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

delay-measure two-way send test-id *test-id* **interval** { **1000** | **10000** } **count** *count* [**packet-size** *packet-size*]

Parameters

Parameter	Description	Value
test-id	Specifies the ID of a test instance.	The value is an integer ranging from 1 to 4294967295.
interval { **1000** | **10000** }	Specifies the interval at which DMMs are sent.	The value is either 1000 or 10000, expressed in milliseconds.
count *count*	Specifies the number of times that DMMs are sent.	The value is an integer ranging from 1 to 60.
packet-size *packet-size*	Specifies the size of the sent packets.	The value is an integer ranging from 64 to 1518, in bytes. The default value is 64.

Views

MA view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In VLAN scenarios, to implement two-way on-demand frame DM, run the **delay-measure two-way send** command. This command does not take effect in point-to-multipoint link scenarios.

To implement two-way on-demand frame DM for point-to-multipoint links, run the **delay-measure two-way send test-id** command.

Prerequisites

A test instance has been created using the **test-id** command in the MA view.

Precautions

The **delay-measure two-way send test-id** and **delay-measure two-way send** commands are mutually exclusive.

If the configuration changes during on-demand statistics, you can view only the pre-change statistics results. You are advised to run the command for on-demand statistics again for query.

Example

Configure two-way frame DM with the test instance ID of 1, DMM transmission interval of 10s, and measurement times of 60.

```
<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] quit
[HUAWEI] set service-mode enhanced
Warning: This command will effect forward performance. Continue? [Y/N]:y
[HUAWEI] cfm enable
[HUAWEI] cfm md md1
[HUAWEI-md-md1] ma ma1
[HUAWEI-md-md1-ma-ma1] map vlan 100
[HUAWEI-md-md1-ma-ma1] mep mep-id 1 interface gigabitethernet 0/0/1 inward
[HUAWEI-md-md1-ma-ma1] remote-mep mep-id 2
[HUAWEI-md-md1-ma-ma1] remote-mep ccm-receive enable
[HUAWEI-md-md1-ma-ma1] test-id 1 mep 1 remote-mep 2
[HUAWEI-md-md1-ma-ma1] delay-measure two-way send test-id 1 interval 10000 count 60
```

12.9.20 delay-measure two-way threshold

Function

The **delay-measure two-way threshold** command sets the alarm threshold for two-way frame delay measurement.

The **undo delay-measure two-way threshold** command cancels the configuration.

Format

delay-measure two-way threshold *threshold-value*

undo delay-measure two-way threshold

Parameters

Parameter	Description	Value
threshold-value	Specifies the alarm threshold for two-way frame delay measurement.	The value is an integer that ranges from 1 to 4294967295, in microseconds.

Views

MA view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

This command is applicable to VLANs. You can set the alarm threshold for two-way frame delay measurement on the MEP or RMEP. When the two-way delay exceeds the alarm threshold, an alarm is generated.

Precautions

IEEE 802.1ag has two versions: IEEE 802.1ag Draft 7 and IEEE Standard 802.1ag-2007. This command can be used only on the device running IEEE Standard 802.1ag-2007.

NOTE

Before setting the alarm threshold, you must correctly configure the MD and MA.

Example

Set the alarm threshold for two-way frame delay measurement in the VLAN to 10.

```
<HUAWEI> system-view
[HUAWEI] cfm enable
[HUAWEI] cfm md md1
[HUAWEI-md-md1] ma ma1
[HUAWEI-md-md1-ma-ma1] map vlan 100
[HUAWEI-md-md1-ma-ma1] delay-measure two-way threshold 10
```

12.9.21 delay-measure two-way trigger if-down

Function

The **delay-measure two-way trigger if-down** command triggers an interface to go ETHOAM down when the delay or delay variation based on a test instance ID exceeds a specified threshold.

The **undo delay-measure two-way trigger if-down** command restores the default configuration.

By default, an interface is not triggered to go ETHOAM down when the delay or delay variation based on a test instance ID exceeds a specified threshold.

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

delay-measure two-way { **delay-threshold** | **variation-threshold** } **test-id** *test-id* **trigger if-down**

undo delay-measure two-way { **delay-threshold** | **variation-threshold** } **test-id** *test-id* **trigger if-down**

Parameters

Parameter	Description	Value
delay-threshold	Indicates that an interface is triggered to go ETHOAM down when the delay exceeds a specified threshold.	-
variation-threshold	Indicates that an interface is triggered to go ETHOAM down when the delay variation exceeds a specified threshold.	-
test-id *test-id*	Specifies the ID of a test instance.	The value is an integer that ranges from 1 to 4294967295.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When no service is bound to the MA, the interface where the MEP resides is an Eth-Trunk interface's primary member interface. To ensure the quality of the primary link, run the **delay-measure two-way trigger if-down** command on the interface where the MEP resides. If the delay or delay variation based on a test instance ID exceeds the threshold configured using the **delay-measure two-way delay-threshold test-id** or **delay-measure two-way variation-threshold test-id** command, the primary link has poor quality. In this case, the interface is triggered to go ETHOAM down, triggering an active/standby Eth-Trunk link switchover.

Prerequisites

A test instance has been created using the **test-id** command in the MA view.

Example

Trigger the Eth-Trunk member interface GE 0/0/1 to go Down when the two-way delay based on a test instance ID of 2 exceeds a specified threshold.

```
<HUAWEI> system-view
[HUAWEI] set service-mode enhanced
Warning: This command will effect forward performance. Continue? [Y/N]:y
[HUAWEI] cfm enable
[HUAWEI] cfm md md1
[HUAWEI-md-md1] ma ma1
[HUAWEI-md-md1-ma-ma1] mep mep-id 8 interface gigabitethernet 0/0/1 outward
[HUAWEI-md-md1-ma-ma1] remote-mep mep-id 9
[HUAWEI-md-md1-ma-ma1] test-id 2 mep 8 remote-mep 9
[HUAWEI] interface eth-trunk 1
[HUAWEI-Eth-Trunk1] quit
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] eth-trunk 1
[HUAWEI-GigabitEthernet0/0/1] delay-measure two-way delay-threshold test-id 2 trigger if-down
```

12.9.22 delay-measure two-way variation-threshold test-id

Function

The **delay-measure two-way variation-threshold test-id** command configures variation thresholds for two-way proactive frame delay measurement (DM).

The **undo delay-measure two-way variation-threshold test-id** command deletes the variation thresholds configured for two-way proactive frame DM.

By default, no variation thresholds are configured for two-way proactive frame DM.

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

delay-measure two-way variation-threshold test-id *test-id* **upper-limit** *upper-limit* **lower-limit** *lower-limit*

undo delay-measure two-way variation-threshold test-id *test-id* [**upper-limit** *upper-limit* **lower-limit** *lower-limit*]

Parameters

Parameter	Description	Value
test-id	Specifies the ID of a test instance.	The value is an integer ranging from 1 to 4294967295.

Parameter	Description	Value
upper-limit *upper-limit*	Specifies an upper variation threshold for two-way proactive frame DM.	The value is an integer ranging from 0 to 4294967295, in microseconds.
lower-limit *lower-limit*	Specifies a lower variation threshold for two-way proactive frame DM.	The value is an integer ranging from 0 to 4294967295, in microseconds. The lower variation threshold must be less than the upper variation threshold.

Views

MA view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To configure upper and lower variation thresholds for two-way proactive frame DM that monitors link quality, run the **delay-measure two-way variation-threshold test-id** command. After configuring upper and lower variation thresholds, you can obtain data (such as the number of times that a threshold-crossing event occurs) within a sampling period to monitor network performance.

Prerequisites

A test instance has been created using the **test-id** command in the MA view.

Precautions

The configured threshold makes sense only after the proactive measurement is configured.

Example

Set lower and upper variation thresholds for two-way proactive frame DM in VLAN scenarios to 200 microseconds and 400 microseconds, respectively.

```
<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] quit
[HUAWEI] set service-mode enhanced
Warning: This command will effect forward performance. Continue? [Y/N]:y
[HUAWEI] cfm enable
[HUAWEI] cfm md md1
[HUAWEI-md-md1] ma ma1
[HUAWEI-md-md1-ma-ma1] map vlan 100
[HUAWEI-md-md1-ma-ma1] mep mep-id 1 interface gigabitethernet 0/0/1 inward
[HUAWEI-md-md1-ma-ma1] remote-mep mep-id 2
```



```
[HUAWEI-md-md1-ma-ma1] mep ccm-send enable
[HUAWEI-md-md1-ma-ma1] remote-mep ccm-receive enable
[HUAWEI-md-md1-ma-ma1] test-id 1 mep 1 remote-mep 2
[HUAWEI-md-md1-ma-ma1] delay-measure two-way variation-threshold test-id 1 upper-limit 400 lower-limit 200
```

12.9.23 display y1731 statistic-type

Function

The **display y1731 statistic-type** command displays performance statistics collected through Y.1731.

Format

display y1731 statistic-type { **oneway-delay** | **twoway-delay** } **md** *md-name* **ma** *ma-name* [**count** *count-value*]

display y1731 statistic-type { **single-loss** | **dual-loss** } **md** *md-name* **ma** *ma-name* [**count** *count-value*] (Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.)

display y1731 statistic-type single-loss test-id *test-id* [**count** *count-value*] (Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.)

display y1731 statistic-type single-synthetic-loss test-id *test-id* [**count** *count-value*] (Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.)

display y1731 statistic-type twoway-delay test-id *test-id* [**count** *count-value*] (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
dual-loss	Displays statistics about dual-ended frame loss measurement.	-
single-loss	Displays statistics about single-ended frame loss measurement.	-
oneway-delay	Displays statistics about the one-way frame delay.	-
twoway-delay	Displays statistics about the two-way frame delay.	-

Parameter	Description	Value
md *md-name*	Specifies the name of an MD.	The value is a string of 1 to 43 characters without spaces, hyphens (-), and question marks (?). MD names on a device are unique.
ma *ma-name*	Specifies the name of an MA.	The value is a string of characters without spaces, hyphens (-), and question marks (?). The total length of the names of the MA and MD must be within 44 characters. Names of MAs in an MD are unique.
count *count-value*	Specifies the number of statistics entries to be displayed. If the parameter is not specified, the command output displays all the statistics.	The value is an integer in the range from 1 to 60.
test-id *test-id*	Specifies the ID of a test instance.	The value is an integer in the range from 1 to 4294967295.
single-synthetic-loss	Displays statistics about single-ended SLM.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

You can run the **display y1731 statistic-type** command to display performance statistics collected through Y.1731, including single-ended frame loss statistics, dual-ended frame loss statistics, single-ended SLM statistics, one-way frame delay statistics, and two-way frame delay statistics.

Prerequisites

The **cfm enable (system view)** command has been run to enable the CFM function globally.

Example

Display the statistics about the one-way frame delay in the MA **ma1** in the MD **md1**.

```
<HUAWEI> display y1731 statistic-type oneway-delay md md1 ma ma1
Latest one-way delay statistics:
--------------------------------------------------------------------------------
Index    Delay(usec)    Delay variation(usec)
--------------------------------------------------------------------------------
  1         10000                  -
  2         10000                  0
  3         10000                  0
  4         10000                  0
  5         10000                  0
  6         10000                  0
  7         10000                  0
  8         10000                  0
  9         10000                  0
 10         10000                  0
 11         10000                  0
 12         40000              30000
 13         10000              30000
 14         10000                  0
 15         10000                  0
 16         10000                  0
 17         10000                  0
--------------------------------------------------------------------------------
Average delay(usec) :      11764    Average delay variation(usec) :      3750
Maximum delay(usec) :      40000    Maximum delay variation(usec) :      30000
Minimum delay(usec) :      10000    Minimum delay variation(usec) :          0
```

Table 12-70 Description of the **display y1731 statistic-type** command output

Item	Description
Latest one-way delay statistics	Statistics about the one-way frame delay.
Index	Measurement index.
Delay(usec)	One-way delay, in microseconds.
Delay variation(usec)	One-way delay variation, in microseconds.
Average delay(usec)	Average one-way delay, in microseconds.
Average delay variation(usec)	Average one-way delay variation, in microseconds.
Maximum delay(usec)	Maximum one-way delay, in microseconds.
Maximum delay variation(usec)	Maximum one-way delay variation, in microseconds.
Minimum delay(usec)	Minimum one-way delay, in microseconds.
Minimum delay variation(usec)	Minimum one-way delay variation, in microseconds.

Display the statistics about the two-way frame delay in the MA **ma2** in the MD **md2**.


```
<HUAWEI> display y1731 statistic-type twoway-delay md md2 ma ma2
Latest two-way delay statistics:
--------------------------------------------------------------------------------
Index    Delay(usec)    Delay variation(usec)
--------------------------------------------------------------------------------
  1           0                  -
  2           0                  0
  3           0                  0
  4           0                  0
  5           0                  0
  6           0                  0
  7           0                  0
  8           0                  0
  9           0                  0
 10           0                  0
--------------------------------------------------------------------------------
Average delay(usec) :          0    Average delay variation(usec) :          0
Maximum delay(usec) :          0    Maximum delay variation(usec) :          0
Minimum delay(usec) :          0    Minimum delay variation(usec) :          0
```

Table 12-71 Description of the **display y1731 statistic-type** command output

Item	Description
Latest two-way delay statistics	Statistics about the two-way frame delay.
Index	Measurement index.
Delay(usec)	Two-way delay, in microseconds.
Delay variation(usec)	Two-way delay variation, in microseconds.
Average delay(usec)	Average two-way delay, in microseconds.
Average delay variation(usec)	Average two-way delay variation, in microseconds.
Maximum delay(usec)	Maximum two-way delay, in microseconds.
Maximum delay variation(usec)	Maximum two-way delay variation, in microseconds.
Minimum delay(usec)	Minimum two-way delay, in microseconds.
Minimum delay variation(usec)	Minimum two-way delay variation, in microseconds.

Display proactive single-ended SLM statistics in test instance 2.

```
<HUAWEI> display y1731 statistic-type single-synthetic-loss test-id 2
--------------------------------------------------------------------------------
Index      L-send R-send L-recv Unack  L-loss R-loss L-loss-ratio R-loss-ratio
--------------------------------------------------------------------------------
667        1000   1000   1000   0       0      0      0.0000%     0.0000%
668        1000   1000   1000   0       0      0      0.0000%     0.0000%
669        1000   1000   1000   0       0      0      0.0000%     0.0000%
670        1000   1000   1000   0       0      0      0.0000%     0.0000%
671        1000   1000   1000   0       0      0      0.0000%     0.0000%
672        1000   1000   1000   0       0      0      0.0000%     0.0000%
673        1000   1000   1000   0       0      0      0.0000%     0.0000%
674        1000   1000   1000   0       0      0      0.0000%     0.0000%
675        1000   1000   1000   0       0      0      0.0000%     0.0000%
676        1000   1000   1000   0       0      0      0.0000%     0.0000%
```



```
677         1000   1000   1000   0          0      0      0.0000%      0.0000%
678         1000   1000   1000   0          0      0      0.0000%      0.0000%
679         1000   1000   1000   0          0      0      0.0000%      0.0000%
680         1000   1000   1000   0          0      0      0.0000%      0.0000%
681         1000   1000   1000   0          0      0      0.0000%      0.0000%
682         1000   1000   1000   0          0      0      0.0000%      0.0000%
683         1000   1000   1000   0          0      0      0.0000%      0.0000%
684         1000   1000   1000   0          0      0      0.0000%      0.0000%
------------------------------------------------------------------------------
Average Local-loss  :          0    Average Local-loss Ratio  :         0.0000%
Maximum Local-loss  :          0    Maximum Local-loss Ratio  :         0.0000%
Minimum Local-loss  :          0    Minimum Local-loss Ratio  :         0.0000%
Average Remote-loss :          0    Average Remote-loss Ratio :         0.0000%
Maximum Remote-loss :          0    Maximum Remote-loss Ratio :         0.0000%
Minimum Remote-loss :          0    Minimum Remote-loss Ratio :         0.0000%
```

Table 12-72 Description of the **display y1731 statistic-type** command output

Item	Description
Index	Measurement index.
L-send	Number of packets sent from the local end in each round.
R-send	Number of packets sent from the remote end in each round.
L-recv	Number of packets received by the local end in each round.
Unack	Number of unacknowledged packets.
L-loss	Number of lost packets on the local end in each round.
R-loss	Number of lost packets on the remote end in each round.
L-loss-ratio	Packet loss rate on the local end in each round.
R-loss-ratio	Packet loss rate on the remote end in each round.
Average Local-loss	Average number of lost packets on the local end.
Average Local-loss Ratio	Average packet loss rate on the local end.
Maximum Local-loss	Maximum number of lost packets on the local end.
Maximum Local-loss Ratio	Maximum packet loss rate on the local end.
Minimum Local-loss	Minimum number of lost packets on the local end.
Minimum Local-loss Ratio	Minimum packet loss rate on the local end.

Item	Description
Average Remote-loss	Average number of lost packets on the remote end.
Average Remote-loss Ratio	Average packet loss rate on the remote end.
Maximum Remote-loss	Maximum number of lost packets on the remote end.
Maximum Remote-loss Ratio	Maximum packet loss rate on the remote end.
Minimum Remote-loss	Minimum number of lost packets on the remote end.
Minimum Remote-loss Ratio	Minimum packet loss rate on the remote end.

Display on-demand single-ended SLM statistics.

```
<HUAWEI> display y1731 statistic-type single-synthetic-loss test-id 1
Measurement Start Time : 2014-05-23 16:32:13-08:00
--------------------------------------------------------------------------------
Index       L-send R-send L-recv Unack  L-loss R-loss L-loss-ratio R-loss-ratio
--------------------------------------------------------------------------------
1           10     10     10     0           0      0      0.0000%      0.0000%
--------------------------------------------------------------------------------
Average Local-loss  :          0    Average Local-loss Ratio  :         0.0000%
Maximum Local-loss  :          0    Maximum Local-loss Ratio  :         0.0000%
Minimum Local-loss  :          0    Minimum Local-loss Ratio  :         0.0000%
Average Remote-loss :          0    Average Remote-loss Ratio :         0.0000%
Maximum Remote-loss :          0    Maximum Remote-loss Ratio :         0.0000%
Minimum Remote-loss :          0    Minimum Remote-loss Ratio :         0.0000%
```

Table 12-73 Description of the **display y1731 statistic-type** command output

Item	Description
Measurement Start Time	Start time of measurement.
Index	Measurement index.
L-send	Number of packets sent from the local end in each round.
R-send	Number of packets sent from the remote end in each round.
L-recv	Number of packets received by the local end in each round.
Unack	Number of unacknowledged packets.
L-loss	Number of lost packets on the local end in each round.

Item	Description
R-loss	Number of lost packets on the remote end in each round.
L-loss-ratio	Packet loss rate on the local end in each round.
R-loss-ratio	Packet loss rate on the remote end in each round.
Average Local-loss	Average number of lost packets on the local end.
Average Local-loss Ratio	Average packet loss rate on the local end.
Maximum Local-loss	Maximum number of lost packets on the local end.
Maximum Local-loss Ratio	Maximum packet loss rate on the local end.
Minimum Local-loss	Minimum number of lost packets on the local end.
Minimum Local-loss Ratio	Minimum packet loss rate on the local end.
Average Remote-loss	Average number of lost packets on the remote end.
Average Remote-loss Ratio	Average packet loss rate on the remote end.
Maximum Remote-loss	Maximum number of lost packets on the remote end.
Maximum Remote-loss Ratio	Maximum packet loss rate on the remote end.
Minimum Remote-loss	Minimum number of lost packets on the remote end.
Minimum Remote-loss Ratio	Minimum packet loss rate on the remote end.

Display statistics about on-demand two-way frame delay measurement.

```
<HUAWEI> display y1731 statistic-type twoway-delay test-id 1
Measurement Start Time : 2017-07-29 08:43:12
Latest two-way delay statistics:
--------------------------------------------------------------------------------
Index    Delay(usec)    Delay variation(usec)
--------------------------------------------------------------------------------
  1          202                -
  2          237               35
  3          219               18
  4          234               15
  5          243                9
  6          262               19
  7          263                1
```



```
  8          245                  18
  9          229                  16
 10          237                   8
--------------------------------------------------------------------------------
Average delay(usec) :       237    Average delay variation(usec) :       15
Maximum delay(usec) :       263    Maximum delay variation(usec) :       35
Minimum delay(usec) :       202    Minimum delay variation(usec) :       1
```

Table 12-74 Description of the **display y1731 statistic-type** command output

Item	Description
Measurement Start Time	Start time of measurement.
Latest two-way delay statistics	Statistics about the two-way frame delay.
Index	Measurement index.
Delay(usec)	Two-way delay, in microseconds.
Delay variation(usec)	Two-way delay variation, in microseconds.
Average delay(usec)	Average two-way delay, in microseconds.
Maximum delay(usec)	Maximum two-way delay, in microseconds.
Minimum delay(usec)	Minimum two-way delay, in microseconds.
Average delay variation(usec)	Average two-way delay variation, in microseconds.
Maximum delay variation(usec)	Maximum two-way delay variation, in microseconds.
Minimum delay variation(usec)	Minimum two-way delay variation, in microseconds.

Display dual-ended frame loss measurement statistics in the MA **ma2** in the MD **md2**.

```
<HUAWEI> display y1731 statistic-type dual-loss md md2 ma ma2
Measurement Start Time : 2018-09-28 16:48:39
Latest dual-ended loss statistics:
--------------------------------------------------------------------------------
Index    Local-loss    Local-loss ratio    Remote-loss    Remote-loss ratio
--------------------------------------------------------------------------------
  1          0          0.0000%             0          0.0000%
  2          0          0.0000%             0          0.0000%
  3          0          0.0000%             0          0.0000%
  4          0          0.0000%             0          0.0000%
  5          0          0.0000%             0          0.0000%
  6          0          0.0000%             0          0.0000%
  7          0          0.0000%             0          0.0000%
  8          0          0.0000%             0          0.0000%
  9          0          0.0000%             0          0.0000%
 10          0          0.0000%             0          0.0000%
 11          0          0.0000%             0          0.0000%
 12          0          0.0000%             0          0.0000%
 13          0          0.0000%             0          0.0000%
 14          0          0.0000%             0          0.0000%
 15          0          0.0000%             0          0.0000%
--------------------------------------------------------------------------------
Average Local-loss  :        0    Average Local-loss Ratio  :   0.0000%
```



```
Maximum Local-loss  :          0    Maximum Local-loss Ratio  :   0.0000%
Minimum Local-loss  :          0    Minimum Local-loss Ratio  :   0.0000%
Average Remote-loss :          0    Average Remote-loss Ratio :   0.0000%
Maximum Remote-loss :          0    Maximum Remote-loss Ratio :   0.0000%
Minimum Remote-loss :          0    Minimum Remote-loss Ratio :   0.0000%
```

Table 12-75 Description of the **display y1731 statistic-type** command output

Item	Description
Measurement Start Time	Start time of measurement.
Index	Measurement index.
Local-loss	Number of lost packets on the local end.
Local-loss ratio	Packet loss rate on the local end.
Remote-loss	Number of lost packets on the remote end.
Remote-loss ratio	Packet loss rate on the remote end, Packet loss rate on the remote end = Number of packets lost on the remote end/Number of packets sent by the local end.
Average Local-loss	Average number of lost packets on the local end.
Maximum Local-loss	Maximum number of lost packets on the local end.
Minimum Local-loss	Minimum number of lost packets on the local end.
Average Local-loss Ratio	Average packet loss rate on the local end.
Maximum Local-loss Ratio	Maximum packet loss rate on the local end.
Minimum Local-loss Ratio	Minimum packet loss rate on the local end.
Average Remote-loss	Average number of lost packets on the remote end.
Maximum Remote-loss	Maximum number of lost packets on the remote end.
Minimum Remote-loss	Minimum number of lost packets on the remote end.
Average Remote-loss Ratio	Average packet loss rate on the remote end.
Maximum Remote-loss Ratio	Maximum packet loss rate on the remote end.
Minimum Remote-loss Ratio	Minimum packet loss rate on the remote end.

Display single-ended frame loss measurement statistics in the MA **ma2** in the MD **md2**.

```
<HUAWEI> display y1731 statistic-type single-loss md md2 ma ma2
Measurement Start Time : 2018-09-28 16:48:39
Latest dual-ended loss statistics:
--------------------------------------------------------------------------------
Index    Local-loss    Local-loss ratio    Remote-loss    Remote-loss ratio
--------------------------------------------------------------------------------
  1          0          0.0000%             0           0.0000%
  2          0          0.0000%             0           0.0000%
  3          5         50.0000%            10           50.0000%
  4          0          0.0000%             0           0.0000%
  5          5         50.0000%            10           50.0000%
  6         10          50.0000%            5           50.0000%
  7          5         50.0000%            10           50.0000%
  8         10          50.0000%            5           50.0000%
  9         10          50.0000%            5           50.0000%
 10          5          50.0000%           10           50.0000%
 11          5          50.0000%           10           50.0000%
 12         10          50.0000%            5           50.0000%
 13          5          50.0000%           10           50.0000%
 14         10          50.0000%            5           50.0000%
 15          5          50.0000%           10           50.0000%
 16         10          50.0000%            5           50.0000%
--------------------------------------------------------------------------------
Average Local-loss  :         5    Average Local-loss Ratio  : 40.6250%
Maximum Local-loss  :        10    Maximum Local-loss Ratio  : 50.0000%
Minimum Local-loss  :         0    Minimum Local-loss Ratio  :  0.0000%
Average Remote-loss :         6    Average Remote-loss Ratio : 40.6250%
Maximum Remote-loss :        10    Maximum Remote-loss Ratio : 50.0000%
Minimum Remote-loss :         0    Minimum Remote-loss Ratio :  0.0000%
```

Table 12-76 Description of the **display y1731 statistic-type** command output

Item	Description
Measurement Start Time	Start time of measurement.
Index	Measurement index.
Local-loss	Number of lost packets on the local end.
Local-loss ratio	Packet loss rate on the local end.
Remote-loss	Number of lost packets on the remote end.
Remote-loss ratio	Packet loss rate on the remote end, Packet loss rate on the remote end = Number of packets lost on the remote end/Number of packets sent by the local end.
Average Local-loss	Average number of lost packets on the local end.
Maximum Local-loss	Maximum number of lost packets on the local end.
Minimum Local-loss	Minimum number of lost packets on the local end.
Average Local-loss Ratio	Average packet loss rate on the local end.

Item	Description
Maximum Local-loss Ratio	Maximum packet loss rate on the local end.
Minimum Local-loss Ratio	Minimum packet loss rate on the local end.
Average Remote-loss	Average number of lost packets on the remote end.
Maximum Remote-loss	Maximum number of lost packets on the remote end.
Minimum Remote-loss	Minimum number of lost packets on the remote end.
Average Remote-loss Ratio	Average packet loss rate on the remote end.
Maximum Remote-loss Ratio	Maximum packet loss rate on the remote end.
Minimum Remote-loss Ratio	Minimum packet loss rate on the remote end.

12.9.24 display y1731 test-info

Function

The **display y1731 test-info** command displays information about test instances for Y.1731 statistics collection.

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

display y1731 test-info [**test-id** *test-id*]

Parameters

Parameter	Description	Value
test-id *test-id*	Displays information about a specified test instance.	The value is an integer ranging from 1 to 4294967295.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

To view information about test instances for Y.1731 statistics collection, run the **display y1731 test-info** command.

Example

Display information about test instance 1 for Y.1731 statistics collection on a device.

```
<HUAWEI> display y1731 test-info test-id 1
------------------------------------------------------------
 TestId 1 information:
------------------------------------------------------------
 MD Name                    : md1
 MA Name                    : ma
 MEP ID                   : 1
 Local Mac                : xxxx-xxxx-xxxx
 Remote MEP ID              : 2
 Bind Mac                 : --
 Send Mac                 : --
 8021p                    : --
 Uplink 8021p               : --
 Downlink 8021p             : --
 Single LM                : disabled
 Single LM Interval         : --
 Single LM Count            : --
 Single LM Receive          : disabled
 OneWay DM                  : disabled
 OneWay DM Interval         : --
 OneWay DM Count            : --
 OneWay DM Packet Size      : --
 OneWay DM Receive          : disabled
 TwoWay DM                : disabled
 TwoWay DM Interval         : --
 TwoWay DM Count            : --
 TwoWay DM Packet Size      : --
 TwoWay DM Receive          : disabled
 Single SLM               : continual
 Single SLM Interval        : 10ms
 Single SLM SendingCount    : 10
 Single SLM SendTimeout     : 5s
 Single SLM Receive         : disabled
 Single SLM RecvTimeout     : --
```

Table 12-77 Description of the **display y1731 test-info** command output

Item	Description
TestId 1 information	Information about test instance 1.
MD Name	Name of the MD.
MA Name	Name of the MA.
MEP ID	MEP ID.
Local Mac	Local MAC address.

Item	Description
Remote MEP ID	RMEP ID.
Bind Mac	MAC address of the RMEP.
Send Mac	MAC address carried in frames.
8021p	802.1p priority value specified in a specified test instance. To set the 802.1p priority value specified in a specified test instance, run the **test-id** command.
Uplink 8021p	Priority value of upstream packets. The switch does not support this function.
Downlink 8021p	Priority value of downstream packets. The switch does not support this function.
Single LM	Whether Y.1731 packet sending is enabled for single-ended frame LM. ● enabled ● disabled To enable Y.1731 packet sending for single-ended frame LM, run the **loss-measure single-ended send test-id** or **loss-measure single-ended continual send test-id** command.
Single LM Interval	Interval at which Y.1731 packets are sent for single-ended frame LM. To set the interval at which Y.1731 packets are sent for single-ended frame LM, run the **loss-measure single-ended send test-id** or **loss-measure single-ended continual send test-id** command.
Single LM Count	Number of Y.1731 packets that are to be sent for single-ended frame LM. To set the number of Y.1731 packets sent for single-ended frame LM, run the **loss-measure single-ended send test-id** command.
Single LM Receive	Whether Y.1731 packet receiving is enabled for single-ended frame LM. ● enabled ● disabled To enable SLM frame sending for single-ended SLM, run the **loss-measure single-ended receive test-id** command.

Item	Description
OneWay DM	Whether Y.1731 packet sending is enabled for one-way frame DM. • enabled • disabled The switch does not support one-way frame delay measurement based on test instances.
OneWay DM Interval	Interval at which Y.1731 packets are sent for one-way frame DM. The switch does not support one-way frame delay measurement based on test instances.
OneWay DM Count	Number of Y.1731 packets sent for one-way frame DM. The switch does not support one-way frame delay measurement based on test instances.
OneWay DM Packet Size	Size of Y.1731 packets transmitted for one-way frame DM. The switch does not support one-way frame delay measurement based on test instances.
OneWay DM Receive	Whether Y.1731 packet receiving is enabled for one-way frame DM. • enabled • disabled The switch does not support one-way frame delay measurement based on test instances.
TwoWay DM	Whether Y.1731 packet sending is enabled for two-way frame DM. • enabled • disabled To enable Y.1731 packet sending for two-way frame DM, run the **delay-measure two-way send test-id** or **delay-measure two-way continual send test-id** command.

Item	Description
TwoWay DM Interval	Interval at which Y.1731 packets are sent for two-way frame DM. To set the interval at which Y.1731 packets are sent for two-way frame DM, run the **delay-measure two-way send test-id** or **delay-measure two-way continual send test-id** command.
TwoWay DM Count	Number of Y.1731 packets sent for two-way frame DM. To set the number of Y.1731 packets sent for two-way frame DM, run the **delay-measure two-way send test-id** command.
TwoWay DM Packet Size	Size of Y.1731 packets transmitted for two-way frame DM. To set the size of Y.1731 packets transmitted for two-way frame DM, run the **delay-measure two-way send test-id** or **delay-measure two-way continual send test-id** command.
TwoWay DM Receive	Whether Y.1731 packet receiving is enabled for two-way frame DM. ● enabled ● disabled To enable Y.1731 packet receiving for two-way frame DM, run the **delay-measure two-way receive test-id** command.
Single SLM	Whether Y.1731 packet sending is enabled for single-ended SLM. ● enabled ● disabled To enable Y.1731 packet sending for single-ended SLM, run the **loss-measure single-ended-synthetic send** or **loss-measure single-ended-synthetic continual send** command.
Single SLM Interval	Interval at which SLM frames are sent for single-ended SLM. To set the interval at which SLM frames are sent for single-ended SLM, run the **loss-measure single-ended-synthetic send** or **loss-measure single-ended-synthetic continual send** command.

Item	Description
Single SLM SendingCount	Number of SLM frames to be sent for single-ended SLM within each measurement period. To set the number of SLM frames to be sent for single-ended SLM within each measurement period, run the **loss-measure single-ended-synthetic send** or **loss-measure single-ended-synthetic continual send** command.
Single SLM SendTimeout	Timeout period for the transmit end to receive SLM frames. To set the timeout period for the transmit end to receive SLM frames, run the **loss-measure single-ended-synthetic send** or **loss-measure single-ended-synthetic continual send** command.
Single SLM Receive	Whether SLM frame sending is enabled for single-ended SLM. • enabled • disabled To enable SLM frame sending for single-ended SLM, run the **loss-measure single-ended-synthetic receive** command.
Single SLM RecvTimeout	Timeout period for the receive end to receive SLM frames. To set the timeout period for the receive end to receive SLM frames, run the **loss-measure single-ended-synthetic receive** command.

12.9.25 loss-measure dual-ended continual

Function

The **loss-measure dual-ended continual** command enables proactive dual-ended frame loss measurement.

The **undo loss-measure dual-ended continual** command disables proactive dual-ended frame loss measurement.

By default, dual-ended frame loss measurement is disabled.

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

loss-measure dual-ended continual mep *mep-id* **remote-mep** *mep-id*

undo loss-measure dual-ended continual [**mep** *mep-id* [**remote-mep** *mep-id*]]

Parameters

Parameter	Description	Value
mep-id *mep-id*	Specifies the ID of a MEP.	The value is an integer in the range from 1 to 8191.
remote-mep *mep-id*	Specifies the ID of an RMEP.	The value is an integer in the range from 1 to 8191.

Views

MA view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The dual-ended frame loss measurement function is service-oriented. You can estimate quality of services based on the calculated packet loss rate.

Dual-ended frame loss measurement is deployed on end-to-end MEPs. In Y.1731, frame loss statistics are collected based on the transmit and receive counters carried in CCMs.

NOTE

The interval for collecting dual-ended frame loss statistics does not need to be configured separately, because it equals the interval at which CCMs are sent.

Prerequisites

The command takes effect only after the following configurations are completed:

- Run the **cfm version standard** command in the system view to specify IEEE Standard 802.1ag-2007 for CFM.
- Run the **cfm enable (system view)** command to enable CFM globally.
- Run the **cfm md** command in the system view to create an MD.
- Run the **ma** command in the MD view to create an MA.
- Run the **mep mep-id** command in the MA view to create an inward-facing MEP.

If **remote-mep** *mep-id* is specified in the **delay-measure one-way continual** command, the following configurations must be completed:

- Run the **remote-mep** command in the MA view to create an RMEP.
- Run the **mep ccm-send enable** command in the MA view to enable the local MEP in the MA to send CCMs.
- Run the **remote-mep ccm-receive enable** command in the MA view to enable the MEP to receive CCMs from the RMEP in the same MA.

Example

Enable dual-ended frame loss measurement in the VLAN scenario.

```
<HUAWEI> system-view
[HUAWEI] cfm enable
[HUAWEI] cfm md md1
[HUAWEI-md-md1] ma ma1
[HUAWEI-md-md1-ma-ma1] map vlan 10
[HUAWEI-md-md1-ma-ma1] mep mep-id 1 interface GigabitEthernet0/0/1 outward
[HUAWEI-md-md1-ma-ma1] mep ccm-send mep-id 1 enable
[HUAWEI-md-md1-ma-ma1] remote-mep ccm-receive mep-id 2 enable
[HUAWEI-md-md1-ma-ma1] loss-measure dual-ended continual mep 1 remote-mep 2
```

12.9.26 loss-measure single-ended continual send

Function

The **loss-measure single-ended continual send** command enables proactive single-ended frame loss measurement.

The **undo loss-measure single-ended continual send** command disables proactive single-ended frame loss measurement.

By default, proactive single-ended frame loss measurement is disabled.

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

loss-measure single-ended continual send mep *mep-id* { **mac** *mac-address* | **remote-mep** *mep-id* } **interval** { **1000** | **10000** | **30000** }

undo loss-measure single-ended continual send [**mep** *mep-id*]

Parameters

Parameter	Description	Value
mep *mep-id*	Specifies the ID of a MEP.	The value is an integer in the range from 1 to 8191.
mac *mac-address*	Specifies the MAC address of an RMEP.	The value is in the format of H-H-H, where H is a hexadecimal number of 1 to 4 digits.

Parameter	Description	Value
remote-mep *mep-id*	Specifies the ID of an RMEP.	The value is an integer in the range from 1 to 8191.
interval	Specifies the interval at which LMMs are sent.	The value is 1000, 10000, or 30000, in milliseconds.

Views

MA view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The collection interval can be specified to collect statistics about and analyze packet loss data in a period of time.

NOTE

Single-ended frame loss measurement is implemented for the link between the local MEP and an RMEP identified by an ID or a MAC address.

- If the local MEP has not learned the MAC address of the RMEP, the MAC address of the RMEP must be specified to implement single-ended frame loss measurement.
- If the local MEP has learned the MAC address of the RMEP, the ID of the RMEP can be used to implement single-ended frame loss measurement.

Prerequisites

The command takes effect only after the following configurations are completed:

- Run the **cfm version standard** command in the system view to specify IEEE Standard 802.1ag-2007 for CFM.
- Run the **cfm enable (system view)** command to enable CFM globally.
- Run the **cfm md** command in the system view to create an MD.
- Run the **ma** command in the MD view to create an MA.
- Run the **mep mep-id** command in the MA view to create an inward-facing MEP.

If **remote-mep** *mep-id* is specified in the **delay-measure one-way continual** command, the following configurations must be completed:

- Run the **remote-mep** command in the MA view to create an RMEP.
- Run the **mep ccm-send enable** command in the MA view to enable the local MEP in the MA to send CCMs.
- Run the **remote-mep ccm-receive enable** command in the MA view to enable the MEP to receive CCMs from the RMEP in the same MA.

Example

Enable single-ended frame loss measurement in the VLAN scenario and set the RMEP ID to 2 and interval to 30 seconds.

```
<HUAWEI> system-view
[HUAWEI] cfm enable
[HUAWEI] cfm md md1
[HUAWEI-md-md1] ma ma1
[HUAWEI-md-md1-ma-ma1] map vlan 10
[HUAWEI-md-md1-ma-ma1] loss-measure single-ended continual send mep 1 remote-mep 2 interval 30000
```

12.9.27 loss-measure single-ended continual send test-id

Function

The **loss-measure single-ended continual send test-id** command enables single-ended frame loss measurement based on the test instance.

The **undo loss-measure single-ended continual send test-id** command disables on-demand single-ended frame loss measurement.

By default, on-demand single-ended frame loss measurement is disabled.

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

loss-measure single-ended continual send test-id *test-id* **interval** { **1000** | **10000** | **30000** }

undo loss-measure single-ended continual send [**test-id** *test-id*]

Parameters

Parameter	Description	Value
test-id *test-id*	Specifies the ID of a test instance.	The value is an integer in the range from 1 to 4294967295.
interval	Specifies the interval at which LMMs are sent.	The value is 1000, 10000, or 30000, in milliseconds.

Views

MA view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Statistics based on a test instance are mainly used in the P2MP scenario. You can run this command to collect non-stop packet loss statistics.

Prerequisites

The **test-id** *test-id* command has been run in the MA view to create a test instance.

Example

Enable single-ended frame loss measurement based on test instance 1 in the VLAN scenario and set the interval to 30 seconds.

```
<HUAWEI> system-view
[HUAWEI] cfm enable
[HUAWEI] cfm md md1
[HUAWEI-md-md1] ma ma1
[HUAWEI-md-md1-ma-ma1] map vlan 10
[HUAWEI-md-md1-ma-ma1] loss-measure single-ended continual send test-id 1 interval 30000
```

12.9.28 loss-measure single-ended receive

Function

The **loss-measure single-ended receive** command enables the remote device to receive LMMs to implement single-ended frame loss measurement.

The **undo loss-measure single-ended receive** command disables the remote device from receiving LMMs.

By default, the remote device is disabled from receiving LMMs in an MA.

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

loss-measure single-ended receive mep *mep-id*

undo loss-measure single-ended receive [**mep** *mep-id*]

Parameters

Parameter	Description	Value
mep *mep-id*	Specifies the ID of an MEP.	The value is an integer in the range from 1 to 8191.

Views

MA view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the packet loss rate is detected on a link to evaluate the link performance, you can run this command to enable the remote device to receive LMMs. This command is used to configure the remote device in the single-ended frame loss measurement in the VLAN scenario.

Prerequisites

The command takes effect only after the following configurations are completed:

- Run the **cfm version standard** command in the system view to specify IEEE Standard 802.1ag-2007 for CFM.
- Run the **cfm enable (system view)** command to enable CFM globally.
- Run the **cfm md** command in the system view to create an MD.
- Run the **ma** command in the MD view to create an MA.
- Run the **mep mep-id** command in the MA view to create an inward-facing MEP.

Example

Configure the remote device to receive LMMs in a VLAN.

```
<HUAWEI> system-view
[HUAWEI] cfm enable
[HUAWEI] cfm md md1
[HUAWEI-md-md1] ma ma1
[HUAWEI-md-md1-ma-ma1] map vlan 10
[HUAWEI-md-md1-ma-ma1] mep mep-id 1 interface GigabitEthernet0/0/1 outward
[HUAWEI-md-md1-ma-ma1] loss-measure single-ended receive mep 1
```

12.9.29 loss-measure single-ended receive test-id

Function

The **loss-measure single-ended receive test-id** command enables the remote device to receive LMMs based on the test instance to implement single-ended frame loss measurement.

The **undo loss-measure single-ended receive test-id** command disables the remote device from receiving LMMs based on the test instance.

By default, the remote device is disabled from receiving LMMs in an MA.

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

loss-measure single-ended receive test-id *test-id*

undo loss-measure single-ended receive [**test-id** *test-id*]

Parameters

Parameter	Description	Value
test-id	Specifies the ID of a test instance.	The value is an integer in the range from 1 to 4294967295.

Views

MA view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Statistics based on a test instance are mainly used in the P2MP scenario. When the packet loss rate is detected on a link to evaluate the link performance, you can run this command to enable the remote device to receive LMMs.

Prerequisites

The **test-id** *test-id* command has been run in the MA view to create a test instance.

Example

Configure the remote device to receive LMMs based on the test instance.

```
<HUAWEI> system-view
[HUAWEI] cfm enable
[HUAWEI] cfm md md1
[HUAWEI-md-md1] ma ma1
[HUAWEI-md-md1-ma-ma1] map vlan 10
[HUAWEI-md-md1-ma-ma1] loss-measure single-ended receive test-id 1
```

12.9.30 loss-measure single-ended send

Function

The **loss-measure single-ended send** command enables single-ended frame loss measurement.

By default, single-ended frame loss measurement is disabled.

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

loss-measure single-ended send mep *mep-id* [**mac** *mac-address* | **remote-mep** *mep-id*] **interval** { **1000** | **10000** } **count** *count-value*

Parameters

Parameter	Description	Value
mep *mep-id*	Specifies the ID of a MEP.	The value is an integer in the range from 1 to 8191.
mac *mac-address*	Specifies the MAC address of an RMEP.	The value is in the format of H-H-H, where H is a hexadecimal number of 1 to 4 digits.
remote-mep *mep-id*	Specifies the ID of an RMEP.	The value is an integer in the range from 1 to 8191.
interval	Specifies the interval at which LMMs are sent.	The value is 1000 or 10000, in milliseconds.
count *count-value*	Specifies the single-ended frame loss measurement count.	The value is an integer in the range from 1 to 60.

Views

MA view

Default Level

2: Configuration level

Usage Guidelines

When the packet loss rate is detected on a link to evaluate the link performance, you can run this command to enable the remote device to receive LMMs.

NOTE

Single-ended frame loss measurement is implemented for the link between the local MEP and an RMEP identified by an ID or a MAC address.

- If the local MEP has not learned the MAC address of the RMEP, the MAC address of the RMEP must be specified to implement single-ended frame loss measurement.
- If the local MEP has learned the MAC address of the RMEP, the ID of the RMEP can be used to implement single-ended frame loss measurement.

Prerequisites

The command takes effect only after the following configurations are completed:

- Run the **cfm version standard** command in the system view to specify IEEE Standard 802.1ag-2007 for CFM.
- Run the **cfm enable (system view)** command to enable CFM globally.
- Run the **cfm md** command in the system view to create an MD.
- Run the **ma** command in the MD view to create an MA.
- Run the **mep mep-id** command in the MA view to create an inward-facing MEP.

If **remote-mep** *mep-id* is specified in the **delay-measure one-way continual** command, the following configurations must be completed:

- Run the **remote-mep** command in the MA view to create an RMEP.
- Run the **mep ccm-send enable** command in the MA view to enable the local MEP in the MA to send CCMs.
- Run the **remote-mep ccm-receive enable** command in the MA view to enable the MEP to receive CCMs from the RMEP in the same MA.

Example

In the VLAN scenario, enable single-ended frame loss measurement and set the RMEP ID to 2, measurement interval to 10 seconds, and measurement count to 60 times.

```
<HUAWEI> system-view
[HUAWEI] cfm enable
[HUAWEI] cfm md md1
[HUAWEI-md-md1] ma ma1
[HUAWEI-md-md1-ma-ma1] map vlan 10
[HUAWEI-md-md1-ma-ma1] mep mep-id 1 interface GigabitEthernet0/0/1 outward
[HUAWEI-md-md1-ma-ma1] mep ccm-send mep-id 1 enable
[HUAWEI-md-md1-ma-ma1] remote-mep ccm-receive mep-id 2 enable
[HUAWEI-md-md1-ma-ma1] loss-measure single-ended send mep 1 remote-mep 2 interval 10000 count 60
```

12.9.31 loss-measure single-ended send test-id

Function

The **loss-measure single-ended send test-id** command enables single-ended frame loss measurement based on the test instance.

By default, single-ended frame loss measurement based on the test instance is disabled.

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

loss-measure single-ended send test-id *test-id* **interval** { **1000** | **10000** } **count** *count-value*

Parameters

Parameter	Description	Value
test-id	Specifies the ID of a test instance.	The value is an integer in the range from 1 to 4294967295.
interval	Specifies the interval at which LMMs are sent.	The value is 1000 or 10000, in milliseconds.
count *count-value*	Specifies the single-ended frame loss measurement count.	The value is an integer in the range from 1 to 60.

Views

MA view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Statistics collection based on the test instance is applicable to the P2MP scenario. You can run this command to check the packet loss on the link periodically or once only.

Prerequisites

The **test-id** *test-id* command has been run in the MA view to create a test instance.

Example

In the VLAN scenario, enable single-ended frame loss measurement based on the test instance 1 and set the measurement interval to 10 seconds and measurement count to 60 times.

```
<HUAWEI> system-view
[HUAWEI] cfm enable
[HUAWEI] cfm md md1
[HUAWEI-md-md1] ma ma1
[HUAWEI-md-md1-ma-ma1] map vlan 10
[HUAWEI-md-md1-ma-ma1] loss-measure single-ended send test-id 1 interval 10000 count 60
```

12.9.32 loss-measure single-ended-synthetic continual send

Function

The **loss-measure single-ended-synthetic continual send** command enables proactive single-ended synthetic loss measurement (SLM).

The **undo loss-measure single-ended-synthetic continual send** command disables proactive single-ended SLM.

By default, proactive single-ended SLM is disabled.

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

loss-measure single-ended-synthetic continual send test-id *test-id* **interval** { **3.3** | **10** | **100** | **1000** | **10000** } [**sending-count** *count-value*] [**time-out** *timeout*] [**packet-size** *packet-size*]

undo loss-measure single-ended-synthetic continual send test-id *test-id*

Parameters

Parameter	Description	Value
test-id *test-id*	Specifies the ID of a test instance.	The value is an integer that ranges from 1 to 4294967295.
interval { **3.3** | **10** | **100** | **1000** | **10000** }	Specifies the interval at which SLM frames are sent.	Enumerated value, in milliseconds: • 3.3 • 10 • 100 • 1000 • 10000
sending-count *count-value*	Specifies the times that SLM frames are sent within each measurement period.	The value is an integer ranging from 1 to 1000. The default value is 10.
timeout *timeout*	Specifies the timeout period during which the device waits for a response.	The value is an integer ranging from 1 to 10, in seconds. The default value is 5s.
packet-size *packet-size*	Specifies the size of the SLM frames.	The value is an integer ranging from 64 to 1518, in bytes. The default value is 64.

Views

MA view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To collect accurate frame loss statistics on a point-to-multipoint network, run the **loss-measure single-ended-synthetic continual send** command to configure proactive single-ended SLM.

Prerequisites

A test instance has been created using the **test-id** command in the MA view.

Example

Configure SLM with **test id** of 1 and statistics collection interval of 10s.

```
<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] quit
[HUAWEI] set service-mode enhanced
Warning: This command will effect forward performance. Continue? [Y/N]:y
[HUAWEI] cfm enable
[HUAWEI] cfm md md1
[HUAWEI-md-md1] ma ma1
[HUAWEI-md-md1-ma-ma1] map vlan 100
[HUAWEI-md-md1-ma-ma1] mep mep-id 1 interface gigabitethernet 0/0/1 inward
[HUAWEI-md-md1-ma-ma1] remote-mep mep-id 2
[HUAWEI-md-md1-ma-ma1] test-id 1 mep 1 remote-mep 2
[HUAWEI-md-md1-ma-ma1] loss-measure single-ended-synthetic continual send test-id 1 interval 10
```

12.9.33 loss-measure single-ended-synthetic local-ratio-threshold test-id

Function

The **loss-measure single-ended-synthetic local-ratio-threshold test-id** command configures local packet loss ratio thresholds for single-ended synthetic loss measurement (SLM).

The **undo loss-measure single-ended-synthetic local-ratio-threshold test-id** command deletes the local packet loss ratio thresholds configured for single-ended SLM.

By default, no local packet loss ratio thresholds are configured for single-ended SLM.

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

loss-measure single-ended-synthetic local-ratio-threshold test-id *test-id* **upper-limit** *upper-limit* **lower-limit** *lower-limit*

undo loss-measure single-ended-synthetic local-ratio-threshold test-id *test-id* [**upper-limit** *upper-limit* **lower-limit** *lower-limit*]

Parameters

Parameter	Description	Value
test-id	Specifies the ID of a test instance.	The value is an integer that ranges from 1 to 4294967295.
upper-limit *upper-limit*	Specifies an upper local packet loss ratio threshold for single-ended SLM.	The value is a string of 1 to 8 characters in the format of *xxx.xxxx*, in percentages.
lower-limit *lower-limit*	Specifies a lower local packet loss ratio threshold for single-ended SLM.	The value is a string of 1 to 8 characters in the format of *xxx.xxxx*, in percentages. The lower local packet loss ratio threshold must be less than the upper local packet loss ratio threshold.

Views

MA view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On a point-to-multipoint or multipoint-to-multipoint network, run the **loss-measure single-ended-synthetic local-ratio-threshold test-id** command to configure local packet loss ratio thresholds for single-ended SLM. After configuring upper and lower local packet loss ratio thresholds, you can obtain data (such as the number of times that a threshold-crossing event occurs) within a sampling period to monitor network performance.

Prerequisites

A test instance has been created using the **test-id** command in the MA view.

Precautions

Thresholds can be configured only for proactive single-ended SLM and cannot be configured for on-demand single-ended SLM.

Example

Set lower and upper local packet loss ratio thresholds for single-ended SLM to 10.1111 and 11.1111 respectively for test instance 1.

```
<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] quit
[HUAWEI] set service-mode enhanced
Warning: This command will effect forward performance. Continue? [Y/N]:y
[HUAWEI] cfm enable
[HUAWEI] cfm md md1
[HUAWEI-md-md1] ma ma1
[HUAWEI-md-md1-ma-ma1] map vlan 100
[HUAWEI-md-md1-ma-ma1] mep mep-id 1 interface gigabitethernet 0/0/1 inward
[HUAWEI-md-md1-ma-ma1] remote-mep mep-id 2
[HUAWEI-md-md1-ma-ma1] test-id 1 mep 1 remote-mep 2
[HUAWEI-md-md1-ma-ma1] loss-measure single-ended-synthetic local-ratio-threshold test-id 1 upper-limit 11.1111 lower-limit 10.1111
```

12.9.34 loss-measure single-ended-synthetic receive

Function

The **loss-measure single-ended-synthetic receive** command enables a device to receive synthetic loss measurement (SLM) frames for single-ended SLM.

The **undo loss-measure single-ended-synthetic receive** command disables the device from receiving SLM frames.

By default, no device in a maintenance association (MA) is enabled to receive SLM frames.

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

loss-measure single-ended-synthetic receive test-id *test-id* [**time-out** *timeout-value*]

undo loss-measure single-ended-synthetic receive test-id *test-id*

Parameters

Parameter	Description	Value
test-id *test-id*	Specifies the ID of a test instance.	The value is an integer that ranges from 1 to 4294967295.
time-out *timeout-value*	Specifies the timeout period for the receive end to receive SLM frames.	The value is an integer that ranges from 10 to 300, in seconds. The default value is 300.

Views

MA view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the **loss-measure single-ended-synthetic send** command is run to configure on-demand single-ended SLM or the **loss-measure single-ended-synthetic continual send** command is run to configure proactive single-ended SLM, run the **loss-measure single-ended-synthetic receive** command to enable the device to receive SLM frames.

Prerequisites

A test instance has been created using the **test-id** command in the MA view.

Precautions

If you delete or modify the configuration on the receive end more than once, the statistical data may become incorrect. Therefore, do not delete or modify the statistical task after the configuration is complete.

To modify the configuration, disable the device from receiving SLM frames and then perform reconfiguration.

For a proactive single-ended SLM task, set **time-out** on the receive end to a value greater than the value of **interval** on the transmit end.

Example

Configure the remote end to receive SLM frames, set the value of **test id** to 1, and set the timeout period for the receive end to receive SLM frames to 200s.

```
<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] quit
[HUAWEI] set service-mode enhanced
Warning: This command will effect forward performance. Continue? [Y/N]:y
[HUAWEI] cfm enable
[HUAWEI] cfm md md1
[HUAWEI-md-md1] ma ma1
[HUAWEI-md-md1-ma-ma1] map vlan 100
[HUAWEI-md-md1-ma-ma1] mep mep-id 1 interface gigabitethernet 0/0/1 inward
[HUAWEI-md-md1-ma-ma1] remote-mep mep-id 2
[HUAWEI-md-md1-ma-ma1] test-id 1 mep 1 remote-mep 2
[HUAWEI-md-md1-ma-ma1] loss-measure single-ended-synthetic receive test-id 1 time-out 200
```

12.9.35 loss-measure single-ended-synthetic remote-ratio-threshold test-id

Function

The **loss-measure single-ended-synthetic remote-ratio-threshold test-id** command configures remote packet loss ratio thresholds for single-ended synthetic loss measurement (SLM).

The **undo loss-measure single-ended-synthetic remote-ratio-threshold test-id** command deletes the remote packet loss ratio thresholds configured for single-ended SLM.

By default, no remote packet loss ratio thresholds are configured for single-ended SLM.

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

loss-measure single-ended-synthetic remote-ratio-threshold test-id *test-id* **upper-limit** *upper-limit* **lower-limit** *lower-limit*

undo loss-measure single-ended-synthetic remote-ratio-threshold test-id *test-id* [**upper-limit** *upper-limit* **lower-limit** *lower-limit*]

Parameters

Parameter	Description	Value
test-id	Specifies the ID of a test instance.	The value is an integer ranging from 1 to 4294967295.
upper-limit *upper-limit*	Specifies an upper remote packet loss ratio threshold for single-ended SLM.	The value is a string of 1 to 8 characters in the format of *xxx.xxxx*, in percentages.
lower-limit *lower-limit*	Specifies a lower remote packet loss ratio threshold for single-ended SLM.	The value is a string of 1 to 8 characters in the format of *xxx.xxxx*, in percentages. The lower remote packet loss ratio threshold must be less than the upper remote packet loss ratio threshold.

Views

MA view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In a point-to-multipoint or multipoint-to-multipoint scenario, you can run this command to configure remote packet loss ratio thresholds for single-ended SLM. After the thresholds are configured, you can obtain data such as the number of times that a threshold-crossing event occurs.

Prerequisites

A test instance has been created using the **test-id** command in the MA view.

Precautions

Thresholds can be configured only for proactive single-ended SLM and cannot be configured for on-demand single-ended SLM.

Example

Set lower and upper remote packet loss ratio thresholds for single-ended SLM to 10.1111 and 11.1111 respectively for test instance 1.

```
<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] quit
[HUAWEI] set service-mode enhanced
Warning: This command will effect forward performance. Continue? [Y/N]:y
[HUAWEI] cfm enable
[HUAWEI] cfm md md1
[HUAWEI-md-md1] ma ma1
[HUAWEI-md-md1-ma-ma1] map vlan 100
[HUAWEI-md-md1-ma-ma1] mep mep-id 1 interface gigabitethernet 0/0/1 inward
[HUAWEI-md-md1-ma-ma1] remote-mep mep-id 2
[HUAWEI-md-md1-ma-ma1] test-id 1 mep 1 remote-mep 2
[HUAWEI-md-md1-ma-ma1] loss-measure single-ended-synthetic remote-ratio-threshold test-id 1
upper-limit 11.1111 lower-limit 10.1111
```

12.9.36 loss-measure single-ended-synthetic send

Function

The **loss-measure single-ended-synthetic send** command configures on-demand single-ended synthetic loss measurement (SLM).

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

loss-measure single-ended-synthetic send test-id *test-id* **interval** { **3.3** | **10** | **100** | **1000** | **10000** } [**sending-count** *count-value*] [**time-out** *time-out-value*] [**packet-size** *packet-size*] [**measurement-count** *measurement-count*]

Parameters

Parameter	Description	Value
test-id *test-id*	Specifies the ID of a test instance.	The value is an integer ranging from 1 to 4294967295.

Parameter	Description	Value
interval { **3.3** | **10** | **100** | **1000** | **10000** }	Specifies the interval at which SLM frames are sent.	Enumerated value, in milliseconds: • 3.3 • 10 • 100 • 1000 • 10000
sending-count *count-value*	Specifies the times that SLMs are sent within each measurement period.	The value is an integer ranging from 1 to 1000. The default value is 10.
time-out *time-out-value*	Specifies the timeout period during which the device waits for a reply.	The value is an integer ranging from 1 to 10, in seconds. The default value is 5s.
packet-size *packet-size*	Specifies the size of the sent packet.	The value is an integer ranging from 64 to 1518, in bytes. The default value is 64.
measurement-count *measurement-count*	Specifies the number of measurements.	The value is an integer ranging from 1 to 60. The default value is 1.

Views

MA view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When implementing frame loss measurement (LM), Maintenance Association End Points (MEPs) exchange ETH-LM frames. However, single-ended frame LM cannot collect accurate frame loss statistics on a point-to-multipoint or multipoint-to-multipoint network. To resolve this issue, configure on-demand single-ended SLM.

Prerequisites

A test instance has been created using the **test-id** command in the MA view.

Precautions

If the configuration changes during on-demand statistics, you can view only the pre-change statistics results. You are advised to run the command for on-demand statistics again for query.

Example

Configure single-ended SLM with the test ID of 1, SLM frame transmission interval of 1s, SLM frame transmission times of 10, and timeout period waiting for a reply of 5s.

```
<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] quit
[HUAWEI] set service-mode enhanced
Warning: This command will effect forward performance. Continue? [Y/N]:y
[HUAWEI] cfm enable
[HUAWEI] cfm md md1
[HUAWEI-md-md1] ma ma1
[HUAWEI-md-md1-ma-ma1] map vlan 100
[HUAWEI-md-md1-ma-ma1] mep mep-id 1 interface gigabitethernet 0/0/1 inward
[HUAWEI-md-md1-ma-ma1] remote-mep mep-id 2
[HUAWEI-md-md1-ma-ma1] test-id 1 mep 1 remote-mep 2
[HUAWEI-md-md1-ma-ma1] loss-measure single-ended-synthetic send test-id 1 interval 1000 sending-count 10 time-out 5
```

12.9.37 loss-measure single-ended-synthetic trigger if-down

Function

The **loss-measure single-ended-synthetic trigger if-down** command triggers an interface to go ETHOAM down when the near- or far-end frame loss ratio based on a test instance ID exceeds a specified threshold.

The **undo loss-measure single-ended-synthetic trigger if-down** command restores the default configuration.

By default, an interface is not triggered to go ETHOAM down when the near- or far-end frame loss ratio based on a test instance ID exceeds a specified threshold.

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

loss-measure single-ended-synthetic { **local-ratio-threshold** | **remote-ratio-threshold** } **test-id** *test-id* **trigger if-down**

undo loss-measure single-ended-synthetic { **local-ratio-threshold** | **remote-ratio-threshold** } **test-id** *test-id* **trigger if-down**

Parameters

Parameter	Description	Value
local-ratio-threshold	Indicates that an interface is triggered to go ETHOAM down when the near-end frame loss ratio exceeds a specified threshold.	-
remote-ratio-threshold	Indicates that an interface is triggered to go ETHOAM down when the far-end frame loss ratio exceeds a specified threshold.	-
test-id *test-id*	Specifies the ID of a test instance.	The value is an integer that ranges from 1 to 4294967295.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When no service is bound to the MA, the interface where the MEP resides is an Eth-Trunk interface's primary member interface. To ensure the quality of the primary link, run the **loss-measure single-ended-synthetic trigger if-down** command on the interface where the MEP resides. If the near- or far-end frame loss ratio based on a test instance ID exceeds the threshold configured using the **loss-measure single-ended-synthetic local-ratio-threshold test-id** or **loss-measure single-ended-synthetic remote-ratio-threshold test-id** command, the primary link has poor quality. In this case, the interface is triggered to go ETHOAM down, triggering a primary/secondary Eth-Trunk link switchover.

Prerequisites

A test instance has been created using the **test-id** command in the MA view.

Example

Trigger the Eth-Trunk member interface GE 0/0/1 to go ETHOAM down when the near-end frame loss ratio based on a test instance ID of 2 exceeds a specified threshold.

```
<HUAWEI> system-view
[HUAWEI] set service-mode enhanced
Warning: This command will effect forward performance. Continue? [Y/N]:y
[HUAWEI] cfm enable
[HUAWEI] cfm md md1
```



```
[HUAWEI-md-md1] ma ma1
[HUAWEI-md-md1-ma-ma1] mep mep-id 8 interface gigabitethernet 0/0/1 outward
[HUAWEI-md-md1-ma-ma1] remote-mep mep-id 9
[HUAWEI-md-md1-ma-ma1] test-id 2 mep 8 remote-mep 9
[HUAWEI] interface eth-trunk 1
[HUAWEI-Eth-Trunk1] quit
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] eth-trunk 1
[HUAWEI-GigabitEthernet0/0/1] loss-measure single-ended-synthetic local-ratio-threshold test-id 2
trigger if-down
```

12.9.38 ping mac multicast

Function

The **ping mac multicast** command configures multicast MAC ping in the current MA.

Format

ping mac multicast mep *mep-id* [**-c** *count* | **-p** *priority-value* | **-t** *timeout*] *

Parameters

Parameter	Description	Value
mep *mep-id*	Specifies the ID of a MEP.	The value is an integer ranging from 1 to 8191.
-c *count*	Specifies the number of multicast Loopback Messages (LBMs) to be sent.	The value is an integer ranging from 1 to 4294967295. The default value is 3.
-p *priority-value*	Specifies the priority of the multicast LBM.	The value is an integer ranging from 0 to 7. The default value is the same as the 802.1p priority of the 802.1ag packets which is specified in MA view (**packet-priority**).
-t *timeout*	Specifies the timeout period for waiting for a Loopback Reply (LBR).	The value is an integer that ranges from 1 to 65535, in milliseconds. By default, the value is 5000 milliseconds.

Views

MA view

Default Level

0: Visit level

Usage Guidelines

Usage Scenario

The destination MAC address of multicast MAC ping is a multicast MAC address. Multicast MAC ping provides two functions, that is, acknowledging faults and discovering RMEPs.

- Acknowledging faults: Multicast MAC ping provides the fault acknowledgement function similar to that provided by 802.1ag MAC ping. In a multicast MAC ping test, test packets are sent to test whether the path from the local device to the destination device is reachable. Multicast MAC ping can acknowledge the faults of links between multiple MEPs once.
- Discovering RMEPs: All RMEPs in the MA can be discovered.

  For example, there are three MEPs in an MA: MEP1, MEP2, and MEP3. After multicast MAC ping is configured on MEP1, MEP1 sends multicast LBMs. After MEP2 and MEP3 receive the LBM, they reply with an LBR. The LBR carries the MAC address of MEP2 or MEP3, MEP ID, and delay. Before configuring the **remote-mep** command on MEP1, you can configure multicast MAC ping to detect all RMEPs in an MA.

Prerequisites

A MEP has been created using the **mep mep-id** command.

Precautions

IEEE 802.1ag has two versions: IEEE 802.1ag Draft 7 and IEEE Standard 802.1ag-2007. This command can be used only on the device running IEEE Standard 802.1ag-2007. Before using the **ping mac multicast** command, you must use the **cfm version** command to set the Ethernet CFM version to IEEE Standard 802.1ag-2007.

Example

Create an MD named **md1**, create an MA named **ma1** in the MD, and configure multicast MAC ping in **ma1**.

```
<HUAWEI> system-view
[HUAWEI] cfm md md1
[HUAWEI-md-md1] ma ma1
[HUAWEI-md-md1-ma-ma1] mep mep-id 1 interface gigabitethernet 0/0/1 inward
[HUAWEI-md-md1-ma-ma1] ping mac multicast mep 1 -p 6 –c 1 –t 3
Reply from 00e0-fc00-0204 mep id 10: time = 9ms
Reply from 00e0-fc00-0269 mep id 11: time = 11ms
Packets: Sent = 1, Received = 2
Minimum = 9ms, Maximum = 11ms, Average = 10ms
```

Table 12-78 Description of the **ping mac multicast** command output

Item	Description
Reply from	MAC address of the RMEP.
mep id	MEP ID.
time	Delay, in millisecond.

Item	Description
Sent	Number of sent multicast LBMs.
Received	Number of received LBRs.
Minimum	Minimum delay, in millisecond.
Maximum	Maximum delay, in millisecond.
Average	Average delay, in millisecond.

12.9.39 reset y1731 statistic-type

Function

The **reset y1731 statistic-type** command clears statistics collected through Y.1731.

Format

reset y1731 statistic-type { **oneway-delay** | **twoway-delay** } **md** *md-name* **ma** *ma-name*

reset y1731 statistic-type { **single-loss** | **dual-loss**} **md** *md-name* **ma** *ma-name* (Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.)

reset y1731 statistic-type twoway-delay test-id *test-id* (Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.)

reset y1731 statistic-type single-synthetic-loss test-id *test-id* (Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.)

reset y1731 statistic-type single-loss test-id *test-id* (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
oneway-delay	Clears statistics about one-way frame delay measurement.	-
twoway-delay	Clears statistics about two-way frame delay measurement.	-

Parameter	Description	Value
single-loss	Clears statistics about single-ended frame loss measurement.	-
dual-loss	Clears statistics about dual-ended frame loss measurement.	-
md *md-name*	Clears statistics about a specified MD.	The MD must exist.
ma *ma-name*	Clears statistics about a specified MA.	The MA must exist.
test-id *test-id*	Clears statistics about a specified test instance.	The test instance ID must exist.
single-synthetic-loss	Clears single-ended SLM statistics.	-

Views

All views

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To obtain Y.1731 statistics within a specified period of time, run the **reset y1731 statistic-type** command to delete existing Y.1731 statistics, and then run the **display y1731 statistic-type** command after a period of time.

Precautions

After the **reset y1731 statistic-type** command is executed, statistics are cleared and cannot be restored. Exercise caution when you run the command.

Example

Clear statistics about the one-way frame delay.
<HUAWEI> **reset y1731 statistic-type oneway-delay md mdname ma maname**

12.9.40 test-id

Function

The **test-id** command creates a test instance for Y.1731 statistics collection.

The **undo test-id** command deletes a test instance.

By default, no test instance is created in an MA for Y.1731 statistics collection.

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

test-id *test-id* **mep** *mep-id* { **remote-mep** *mep-id* } [**8021p** *8021p-value*] [**description** *description*]

undo test-id *test-id*

Parameters

Parameter	Description	Value
test-id *test-id*	Specifies the ID of a test instance.	The value is an integer ranging from 1 to 4294967295.
mep *mep-id*	Specifies the MEP ID.	The value is an integer that ranges from 1 to 8191.
remote-mep *mep-id*	Specifies the RMEP ID.	The value is an integer that ranges from 1 to 8191.
8021p *8021p-value*	Specifies a priority value for packets.	The value is an integer that ranges from 0 to 7.
description *description*	Specifies the description of a test instance.	The value is a string of 1 to 63 case-sensitive characters without spaces.

Views

MA view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To implement single-ended SLM, run the **test-id** command to create a test instance.

During two-way frame delay measurement in point-to-multipoint scenarios, you need to run this command to configure a test instance.

During two-way frame delay measurement, if the size or priority of outgoing DMMs needs to be specified or there is the high requirement on the detection accuracy, you can run this command to configure a test instance.

Prerequisites

- A MEP has been created using the **mep mep-id** command in the MA view.
- An RMEP has been created using the **remote-mep** command in the MA view.

Precautions

To configure a test instance, run the **set service-mode** command in the system view to configure the device to work in enhanced (S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S is enhanced-oam) mode before enabling CFM globally.

IEEE 802.1ag has two versions: IEEE 802.1ag Draft 7 and IEEE Standard 802.1ag-2007. This command can be used only on the device running IEEE Standard 802.1ag-2007. Before using the **test-id** command, you must use the **cfm version** command to set the Ethernet CFM version to IEEE Standard 802.1ag-2007.

When you run this command in the same MA view to configure multiple test instances, the RMEPs of the local MEP must be different switches.

Example

Configure test instance 200, and specify the MEP ID as 8 and RMEP ID as 9.

```
<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] quit
[HUAWEI] set service-mode enhanced
Warning: This command will effect forward performance. Continue? [Y/N]:y
[HUAWEI] cfm enable
[HUAWEI] cfm md md1
[HUAWEI-md-md1] ma ma1
[HUAWEI-md-md1-ma-ma1] map vlan 100
[HUAWEI-md-md1-ma-ma1] mep mep-id 8 interface gigabitethernet 0/0/1 inward
[HUAWEI-md-md1-ma-ma1] remote-mep mep-id 9
[HUAWEI-md-md1-ma-ma1] test-id 200 mep 8 remote-mep 9
```

