10 VPN Configuration Commands

10.1 GRE Configuration Commands

10.1.1 Command Support

Only the following switch models support GRE:

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

10.1.2 description (tunnel interface view)

Function

The **description** command sets the description of the current tunnel interface.

The **undo description** command deletes the description of the current tunnel interface.

By default, a tunnel interface does not have a description.

Format

description *text*

undo description

Parameters

Parameter	Description	Value
text	Specifies the description of a tunnel interface.	The value is a string of 1 to 242 case-sensitive characters, with spaces supported.

Views

Tunnel interface view

Default Level

2: Configuration level

Usage Guidelines

After using the **interface tunnel** command to create a tunnel interface, you can run the **description** command to configure a description of the tunnel interface to facilitate later query.

To check the description of a tunnel interface, run the **display this interface** command in the tunnel interface view or the **display interface tunnel** command.

Example

# Configure the description of Tunnel 1.

```
<HUAWEI> system-view
[HUAWEI] interface tunnel 1
[HUAWEI-Tunnel1] description This is a tunnel from 10.1.1.1 to 10.2.2.2
```

# Delete the description of Tunnel 1.

```
<HUAWEI> system-view
[HUAWEI] interface tunnel 1
[HUAWEI-Tunnel1] undo description
```

10.1.3 destination

Function

The **destination** command specifies the destination IP address of a tunnel interface.

The **undo destination** command deletes the destination IP address of a tunnel interface.

By default, no destination address is configured.

Format

destination [**vpn-instance** *vpn-instance-name*] *dest-ip-address*

undo destination

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Specifies the name of the VPN instance that the destination address of a tunnel belongs to. When the tunnel interface uses GRE, you can specify **vpn-instance** *vpn-instance-name*.	The value is the name of an existing VPN instance.
dest-ip-address	Specifies the destination IP address of a tunnel interface.	The IPv4 address is in dotted decimal notation. The IPv6 address is a 32-digit hexadecimal number, in the format X:X:X:X:X:X:X:X.

Views

Tunnel interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When configuring a GRE, MPLS TE, IPv4 over IPv6 tunnel or manual IPv6 over IPv4 tunnel, create a tunnel interface. After a tunnel interface is created, run the **destination** command to specify the destination IP address for the tunnel interface.

When using the **destination** command on a PE to specify the destination address of a GRE tunnel bound for a CE, you need to set **vpn-instance** *vpn-instance-name* in the command to specify the name of the VPN instance to which the destination address belongs.

Prerequisites

A tunnel interface has been created using the **interface tunnel** command, and the encapsulation mode is set to GRE, MPLS TE, IPv4 over IPv6 or IPv6 over IPv4 of manual mode using the **tunnel-protocol** command.

Precautions

Two tunnel interfaces with the same encapsulation mode, source address, and destination address cannot be configured simultaneously.

You can configure a main interface working in Layer 3 mode as the source tunnel interface.

On the GRE, MPLS TE, IPv4 over IPv6 tunnel or manual IPv6 over IPv4 tunnel, the destination address of the local tunnel interface is the source address of the remote tunnel interface, and the source address of the local tunnel interface is the destination address of the remote tunnel interface.

Example

# Establish a manual IPv6 over IPv4 tunnel between VLANIF 10 at 10.1.1.1 on switch HUAWEI1 and VLANIF 20 at 10.2.1.1 on switch HUAWEI2.

```
<HUAWEI1> system-view
[HUAWEI1] interface tunnel 1
[HUAWEI1-Tunnel1] tunnel-protocol ipv6-ipv4
[HUAWEI1-Tunnel1] source 10.1.1.1
[HUAWEI1-Tunnel1] destination 10.2.1.1
<HUAWEI2> system-view
[HUAWEI2] interface tunnel 1
[HUAWEI2-Tunnel1] tunnel-protocol ipv6-ipv4
[HUAWEI2-Tunnel1] source 10.2.1.1
[HUAWEI2-Tunnel1] destination 10.1.1.1
```

# Set the destination address of the GRE tunnel Tunnel1 to 10.1.1.1 that belongs to vpn1.

```
<HUAWEI> system-view
[HUAWEI] ip vpn-instance vpn1
[HUAWEI-vpn-instance-vpn1] ipv4-family
[HUAWEI-vpn-instance-vpn1-af-ipv4] route-distinguisher 100:1
[HUAWEI-vpn-instance-vpn1-af-ipv4] quit
[HUAWEI-vpn-instance-vpn1] quit
[HUAWEI] interface tunnel 1
[HUAWEI-Tunnel1] tunnel-protocol gre
[HUAWEI-Tunnel1] destination vpn-instance vpn1 10.1.1.1
```

10.1.4 display interface tunnel

Function

The **display interface tunnel** command displays details of the tunnel interface.

Format

display interface tunnel [*interface-number* | **main**]

Parameters

Parameter	Description	Value
interface-number	Specifies the number of the tunnel interface. If this parameter is not specified, the command displays information about all tunnel interfaces.	The value must be the number a tunnel interface that has been created.

Parameter	Description	Value
main	Displays status and traffic statistics about main interface. The interface has no sub-interfaces. Status and traffic statistics about the interface are displayed whether you specify the main parameter or not.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

To check status of tunnels or diagnose the fault in these tunnels, run the **display interface tunnel** command. You can run this command to obtain tunnel interface information when configuring tunnels or when locating the fault on these tunnels.

Prerequisites

Before run **display interface tunnel**, please ensure that tunnel interface has been created using the **interface tunnel** command.

Example

# Display the details of the tunnel interface.

```
<HUAWEI> display interface tunnel 1
Tunnel1 current state : UP
Line protocol current state : UP
Last line protocol up time : 2012-11-16 19:16:33 UTC+08:00
Description:
Route Port,The Maximum Transmit Unit is 1500
Internet Address is 10.3.1.2/24
Encapsulation is TUNNEL, loopback not set
Tunnel source 10.2.1.2 (Vlanif1234), destination 10.2.1.1
Tunnel protocol/transport GRE/IP, key disabled
keepalive enable period 5 retry-times 3
Checksumming of packets disabled
Current system time: 2012-11-16 19:17:39+08:00
Last 300 seconds input rate 16 bits/sec, 0 packets/sec
Last 300 seconds output rate 0 bits/sec, 0 packets/sec
Input:  5 packets, 650 bytes
Output:  0 packets, 0 bytes
    Input bandwidth utilization  :    0%
    Output bandwidth utilization :    0%
```

Table 10-1 Description of the display interface tunnel command output

Item	Description
Tunnel1 current state	Physical layer status of the tunnel interface: - UP: The interface is in normal state. - Administratively DOWN: The network administrator executes the **shutdown** command on the interface. After a tunnel interface is created, its physical layer status is Up.
Line protocol current state	Link protocol status: - UP: The link layer protocol of the tunnel interface works normally. - Down: The link layer protocol of the tunnel interface is abnormal.
Last line protocol up time	Last time the link layer protocol of the tunnel interface goes UP. **NOTE** This field is displayed only when the link layer protocol status of the tunnel interface is UP.
Description	Description of the tunnel interface.
Route Port	Indicates the Layer 3 interface.
The Maximum Transmit Unit is 1500	MTU of tunnel interfaces, which is 1500 bytes by default. Any packet larger than the MTU is fragmented before being sent. If non-fragmentation is configured, the packet is discarded.
Internet Address is 10.3.1.2/24	IP address of the tunnel interface is 10.3.1.2. The mask is 24 bits, that is, 255.255.255.0.
Encapsulation is TUNNEL,	Encapsulation type of packets on a tunnel interface. Packet encapsulation protects a whole IP packet.
loopback not set	The tunnel interface does not support a loopback test.
Tunnel source 10.2.1.2 (Vlanif1234)	The source address of the tunnel is 10.2.1.2. That is, the IP address of the VLANIF 1234 interface sending packets at the source side is 10.2.1.2.
destination 10.2.1.1	Destination address of the tunnel.

Item	Description
Tunnel protocol/ transport GRE/IP, key disabled	The tunnel encapsulation protocol is the GRE protocol, and the transport protocol is the IP protocol. Encapsulation protocol types of a tunnel are as follows: ● GRE: indicates Generic Routing Encapsulation. ● MPLS: encapsulates packets into MPLS packets. ● IPv6 over IPv4: encapsulates IPv6 packets into IPv4 packets. ● IPv4 over IPv6: encapsulates IPv4 packets into IPv6 packets. ● none: indicates no encapsulation. This is the default mode of the tunnel interface. key disabled: the key word recognition function of GRE is not enabled.
keepalive enable period 5 retry-times 3	The keepalive function of GRE.
Checksumming of packets disabled	The check sum function of GRE is not enabled.
Current system time	Current system time. If the time zone is configured and the daylight saving time is used, the time is in YYYY/MM/DD HH:MM:SS UTC±HH:MM DST format.
Last 300 seconds input rate	Incoming packet rate (bits per second and packets per second) within the last 300 seconds.
Last 300 seconds output rate	Outgoing packet rate (bits per second and packets per second) within the last 300 seconds.
Input	Total number of received packets.
Output	Total number of sent packets.
Input bandwidth utilization : --	Input bandwidth usage.
Output bandwidth utilization : --	Output bandwidth usage.

10.1.5 display keepalive packets count

Function

The **display keepalive packets count** command displays the number of Keepalive packets and Keepalive response packets sent and received by the local GRE tunnel interface.

Format

display keepalive packets count

Parameters

None

Views

Tunnel interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When a tunnel is a GRE tunnel, you can enable the Keepalive function to check the link connectivity. If the function is disabled, service packets are continuously forwarded through this tunnel interface when the link fails, resulting in a tunnel black hole and loss of service data.

The **display keepalive packets count** command allows you to view the number of Keepalive packets and Keepalive response packets sent and received through the GRE tunnel interface.

Prerequisites

1. The tunnel interface view has been displayed using the **interface tunnel** command.
2. The tunnel type has been set to GRE using the **tunnel-protocol gre** command.
3. The Keepalive function has been enabled for the GRE tunnel using the **keepalive** command.

Follow-up Procedure

Run the **reset keepalive packets count** command to reset the Keepalive packet statistics.

Example

# View the Keepalive packet statistics of GRE tunnel interface 1.

```
<HUAWEI> system-view
[HUAWEI] interface tunnel 1
[HUAWEI-Tunnel1] tunnel-protocol gre
[HUAWEI-Tunnel1] keepalive
[HUAWEI-Tunnel1] display keepalive packets count
Send 10 keepalive packets to peers, Receive 10 keepalive response packets from
peers
Receive 8 keepalive packets from peers, Send 8 keepalive response packets to
peers.
```

Table 10-2 Description of the display keepalive packets count command output

Item	Description
Send 10 keepalive packets to peers	Ten Keepalive packets are sent to the remote end.
Receive 10 keepalive response packets from peers	Ten Keepalive response packets are received from the remote end.
Receive 8 keepalive packets from peers	Eight Keepalive packets are received from the remote end.
Send 8 keepalive response packets to peers	Eight Keepalive response packets are sent to the remote end.

10.1.6 display tunnel-info

Function

The **display tunnel-info** command displays the tunnel information.

Format

display tunnel-info { **tunnel-id** *tunnel-id* | **all** | **statistics** [**slots**] }

Parameters

Parameter	Description	Value
tunnel-id *tunnel-id*	Specifies the tunnel ID. If the specified ID does not exist, the system prompts errors.	A hexadecimal integer ranging from 1 to FFFFFFFE.
all	Displays information about all the tunnels.	-
statistics	Displays statistics about all tunnels.	-
slots	Displays tunnel statistics in the order of slots.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The **display tunnel-info all** command displays existing tunnel IDs, tunnel types, destination IP addresses, and Token information about all tunnels.

The **display tunnel-info tunnel-id** *tunnel-id* command displays detailed information about a tunnel when you only know the tunnel ID.

The **display tunnel-info statistics** command displays the number of tunnels configured on the switch.

Example

# View information about the tunnel.

```
<HUAWEI> display tunnel-info tunnel-id 2
Tunnel ID:                   0x2
Tunnel Token:                  2
Type:                       cr lsp
Destination:                  1.1.1.1
Out Slot:                    0
Instance ID:                  0
Interface:                   Tunnel1
Sub Tunnel ID:                 0x0
<HUAWEI> display tunnel-info tunnel-id 3
Tunnel ID:                   0x3
Tunnel Token:                  3
Type:                       lsp
Destination:                  10.20.10.10
Out Slot:                    0
Instance ID:                  0
Out Interface:                 Vlanif1024
Out Label:                    3
Next Hop:                     10.24.10.200
Lsp Index:                   2048
<HUAWEI> display tunnel-info tunnel-id 10006
Tunnel ID:                   0x10006
Tunnel Token:                  2
Type:                       lsp
Destination:                  6.6.6.6
Out Slot:                    0
Instance ID:                  0
Out Interface:                 Vlanif15
Lsp Index:                   0
SubTunnel Type:                L2VPN QoS Token
```

Table 10-3 Description of the **display tunnel-info tunnel-id** command output

Item	Description
Tunnel ID	Tunnel ID in hexadecimal notation that is assigned by the system.
Tunnel Token	Token value used for MPLS forwarding that is a part of tunnel ID and is assigned by the system.
Type	Type of a tunnel, such as GRE, MPLS LSP, or CR-LSP. The command output varies according to the tunnel type.
Destination	Destination IP address of the tunnel.

Item	Description
Out Slot	Number of the slot that is used when the switch sends packets.
Instance ID	VPN instance ID (0 indicates that a tunnel is a public network tunnel).
Interface	Local tunnel interface.
Sub Tunnel ID	Sub-tunnel ID of VPN QoS in hexadecimal notation that is automatically assigned by the system.
Out Label	Out label value.
Next Hop	Next hop.
Lsp Index	LSP index, which is allocated by MPLS.
Out Interface	Local outbound interface of the tunnel.
SubTunnel Type	Types of tokens of sub-tunnels: ● LDP LSP over TE QoS Token ● LDP LSP QoS Token ● BGP LSP over TE QoS Token ● BGP LSP QoS Token ● Static LSP QoS Token ● CR-LSP over TE QoS Token ● L2VPN over TE QoS Token ● L2VPN QoS Token This field is displayed only for sub-tunnels.

# Display all tunnel information.

```
<HUAWEI> display tunnel-info all
 * -> Allocated VC Token
Tunnel ID          Type               Destination          Token
---------------------------------------------------------------------
0x10006            lsp                10.2.1.1             6
```

# Display tunnel statistics.

```
<HUAWEI> display tunnel-info statistics
LSP/32bit LSP :                    0/0
GRE :                              2
CRLSP :                            0
LOCAL IFNET :                      0
MPLS LOCAL IFNET :                 0
VPN QOS LSP :                      0
Reserved :                         0
Vxlan :                            0
```

Table 10-4 Description of the **display tunnel-info statistics** command output

Item	Description
LSP/32bit LSP	Number of LSP tunnels created in the system view/Number of LSP tunnels triggered by the route of host with the 32-bit mask address.
GRE	Number of tunnel IDs allocated to the GRE tunnels.
CRLSP	Number of tunnel IDs allocated to the CR-LSP tunnels.
LOCAL IFNET	Number of tunnels used by the VPN internal module.
MPLS LOCAL IFNET	Number of tunnels used by the MPLS internal module.
VPN QOS LSP	Number of the tunnel ID allocated to the LSP used in VPN QoS.
Reserved	Number of the tunnel ID allocated to the product.
Vxlan	Number of tunnel IDs allocated to the Vxlan tunnels.

# Display tunnel statistics in the order of slots.

```
<HUAWEI> display tunnel-info statistics slots
--------------------------------------------------------------------
Slot       LSP     CR      GRE     LCL     MPLS-L  VPN     VXLAN
Num                LSP             IFNET   IFNET   QOS
--------------------------------------------------------------------
0          0       0       0       0       0       0       0
Logic Slot: 0                      Total:  0
```

Table 10-5 Description of the display tunnel-info statistics slots command output

Item	Description
Slot Num	Slot number used by the device to send packets.
LSP	Total LSP tunnels set up by the device.
CR LSP	Number of CR-LSPs created on the device.
GRE	Number of GRE tunnels created on the device.
LCL IFNET	Number of tunnels used by the VPN module.
MPLS-L IFNET	Number of tunnels used by the MPLS module.
VPN QOS	Number of tunnels used for VPN QoS.
VXLAN	Number of VXLAN tunnels created on the device.

10.1.7 gre key

Function

The **gre key** command sets the key number of a GRE tunnel.

The **undo gre key** command deletes the key number of a GRE tunnel.

By default, the GRE key number is not configured.

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

gre key { **plain** *key-number* | [**cipher**] *plain-cipher-text* }

undo gre key

Parameters

Parameter	Description	Value
plain *key-number*	Specifies a plaintext key. **NOTICE** If **plain** is selected, the key is saved in the configuration file in plain text. This brings security risks. It is recommended that you select **cipher** to save the key in cipher text.	The value is an integer that ranges from 0 to 4294967295.
[**cipher**] *plain-cipher-text*	Specifies that a ciphertext key is displayed.	You can specify a plaintext key (integer) ranging from 0 to 4294967295 or a ciphertext key of 32 or 48 characters.

Views

Tunnel interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can configure key numbers for both ends of a GRE tunnel to improve GRE tunnel security. This security mechanism ensures that a device accepts only packets sent from the valid tunnel interface and discards invalid packets.

Prerequisites

The tunnel interface view has been displayed using the **interface tunnel** command.

The tunnel type has been set to GRE using the **tunnel-protocol gre** command.

Precautions

Packets pass authentication only when the key numbers set on both ends of the tunnel are consistent. Otherwise, the packets are discarded.

When you run the **gre key** command several times, the latest configuration overrides the previous configurations.

Example

# Configure the GRE key number for the ends of a tunnel is 123.

```
<HUAWEI> system-view
[HUAWEI] interface tunnel 1
[HUAWEI-Tunnel1] tunnel-protocol gre
[HUAWEI-Tunnel1] gre key cipher 123
```

10.1.8 interface tunnel

Function

The **interface tunnel** command creates a tunnel interface.

The **undo interface tunnel** command deletes the configured tunnel interface.

By default, no tunnel interface is configured.

Format

interface tunnel *interface-number*

undo interface tunnel *interface-number*

Parameters

Parameter	Description	Value
interface-number	Specifies the number of the tunnel interface.	The value is an integer that ranges from 0 to 2047 .

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To forward data over a tunnel, ensure that the tunnel has been created. The system supports the following types of tunnels:

- LSP (Static LSP, BGP LSP, LDP LSP)
- MPLS TE
- GRE
- IPv6 over IPv4
- IPv4 over IPv6

You must use the **interface tunnel** command to create a tunnel interface when creating a tunnel except for LSP tunnels.

Precautions

Tunnel interface numbers are valid on the local device only. You can configure different numbers for the tunnel interfaces on the two ends.

Follow-up Procedure

After a tunnel interface is created, you need to configure an IP address and encapsulation type for the tunnel interface.

To save IP addresses, run the **ip address unnumbered** command to configure the tunnel interface to borrow an IP address of another interface.

The **tunnel-protocol** command configures an encapsulation protocol for the tunnel interface. Then basic configurations are performed based on the encapsulation protocol:

- On an MPLS TE tunnel, run the **destination**, **mpls te tunnel-id**, **mpls te signal-protocol**, and **mpls te commit** commands.
- On the GRE, IPv4 over IPv6 tunnel or manual IPv6 over IPv4 tunnel, run the **source** and **destination** commands.

Example

# Create a tunnel interface.

```
<HUAWEI> system-view
[HUAWEI] interface tunnel 1
[HUAWEI-Tunnel1]
```

10.1.9 keepalive

Function

The **keepalive** command enables the Keepalive function of GRE tunnels.

The **undo keepalive** command disables the Keepalive function of GRE tunnels.

By default, the Keepalive function of a GRE tunnel is disabled.

Format

keepalive [**period** *period* [**retry-times** *retry-times*]]

undo keepalive

Parameters

Parameter	Description	Value
period *period*	Specifies the interval for sending Keepalive packets.	The value is an integer that ranges from 1 to 32767, in seconds. The default value is 5 seconds.
retry-times *retry-times*	Specifies the parameter of the unreachable counter.	The value is an integer that ranges from 1 to 255. The default value is 3.

Views

Tunnel interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Before you configure a tunnel policy and set the VPN tunnel type to GRE, you need to enable the Keepalive function. After Keepalive is enabled, the VPN cannot choose a tunnel with an unreachable remote end, preventing data loss.

When Keepalive is disabled on a local end, the tunnel interface status of the local end might be Up even if the remote end is unreachable. After Keepalive is enabled on the local end, the tunnel interface status of the local end changes to Down if the remote end is unreachable. Therefore, when the remote end is unreachable, the VPN cannot choose the GRE tunnel, preventing data loss.

The Keepalive function takes effect uni-directionally. To enable the Keepalive function on both ends of a tunnel, run the **keepalive** command on each end of the tunnel. The Keepalive configuration takes effect on one end even if the function is disabled on the other end. However, it is recommended that you enable the Keepalive function on both ends.

After the Keepalive function is enabled on a GRE tunnel, the tunnel periodically sends Keepalive packets. The unreachable counter increases by one each time a packet is sent. If no response packet is received when the value of the counter reaches the value of *retry-times*, the remote end is considered unreachable.

Prerequisites

The **keepalive** command can be used only when the encapsulation mode has been set to GRE on an interface.

Precautions

When you run the **keepalive** command several times, the latest configuration overrides the previous configurations.

When the VPN instance to which a GRE tunnel interface is bound is not the specified destination VPN instance, the **keepalive** command cannot be used to check GRE tunnel connectivity. If this command is used in this situation, the Keepalive function cannot be implemented.

Follow-up Procedure

Run the **display keepalive packets count** command to display the number of Keepalive packets and Keepalive response packets sent and received by the local GRE tunnel interface.

Example

# Enable the Keepalive function for the GRE tunnel using default parameters.

```
<HUAWEI> system-view
[HUAWEI] interface tunnel 1
[HUAWEI-Tunnel1] tunnel-protocol gre
[HUAWEI-Tunnel1] keepalive
```

# Enable the Keepalive function for the GRE tunnel, and set the interval for sending Keepalive packets to 12 seconds and **retry-times** to 4.

```
<HUAWEI> system-view
[HUAWEI] interface tunnel 1
[HUAWEI-Tunnel1] tunnel-protocol gre
[HUAWEI-Tunnel1] keepalive period 12 retry-times 4
```

10.1.10 map interface virtual-ethernet

Function

The **map interface virtual-ethernet** command binds an L2VE interface to a tunnel interface.

The **undo map interface virtual-ethernet** command deletes the binding relationship between a tunnel interface and a specified VE interface.

The **undo map** command deletes the binding relationship between a tunnel interface and all VE interfaces.

By default, no L2VE interface is bound to a tunnel interface.

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S support this function.

Format

map interface virtual-ethernet *ve-number*

undo map interface virtual-ethernet *ve-number*

undo map

Parameters

Parameter	Description	Value
ve-number	Specifies the number of a VE interface.	The VE interface number must already exist.

Views

Tunnel interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Customers want to use GRE to transparently transmit Ethernet packets over networks of a different network layer protocol, such as the IPv4 network. You can configure Ethernet over GRE to achieve this purpose. Run the **map interface virtual-ethernet** command in the tunnel interface view to bind a VE interface to a tunnel interface. After the binding, the tunnel interface can transparently transmit Ethernet packets over the GRE tunnel.

Prerequisites

- A VE interface has been created by using the **interface virtual-ethernet** *ve-number* command, and the VE interface has been changed from Layer 3 mode to Layer 2 mode by using the **portswitch** command.
- The tunnel protocol of a tunnel interface has been set to GRE by using the **tunnel-protocol gre** command in the tunnel interface view.

Precautions

NOTE

- If a VLANIF interface has been created for a VLAN, this VLAN cannot be specified for a VE interface. If a VLAN has been specified for a VE interface, no VLANIF interface can be created for this VLAN.
- One tunnel interface can be bound with two VE interfaces, but one VE interface can be bound to only one tunnel interface.
- Only VE interfaces of the Trunk type can be bound to a tunnel interface.
- A tunnel interface bound with a VE interface does not support the IPv6 protocol stack. A VE interface cannot be bound to a tunnel interface enabled with the IPv6 protocol stack.
- To prevent loops, packets transmitted through an Ethernet over GRE tunnel cannot be sent to a GRE tunnel again.
- Ensure that the VE interfaces at both ends of a GRE tunnel are added to the same VLAN. Otherwise, the VE interfaces will learn MAC addresses not in the VLANs to which the VE interfaces belong, and these MAC addresses cannot be deleted using the **undo mac-address** command. Run the **undo mac-address** [*mac-address*] [**vlan** *vlan-id*] command to delete a specific MAC address or delete MAC addresses by VLAN ID, or wait until the MAC addresses automatically age out.
- When configuring Ethernet over GRE, ensure that routes can recurse to GRE tunnels. Otherwise, packets cannot be encapsulated using Ethernet over GRE.

Example

# Bind Virtual-Ethernet 0/0/1 to Tunnel 1.

```
<HUAWEI> system-view
[HUAWEI] interface virtual-ethernet 0/0/1
[HUAWEI-Virtual-Ethernet0/0/1] portswitch
[HUAWEI-Virtual-Ethernet0/0/1] port link-type trunk
[HUAWEI-Virtual-Ethernet0/0/1] undo port trunk allow-pass vlan 1
[HUAWEI-Virtual-Ethernet0/0/1] port trunk allow-pass vlan 10
[HUAWEI-Virtual-Ethernet0/0/1] quit
[HUAWEI] interface tunnel 1
[HUAWEI-Tunnel1] tunnel-protocol gre
[HUAWEI-Tunnel1] map interface virtual-ethernet 0/0/1
```

10.1.11 reset keepalive packets count

Function

The **reset keepalive packets count** command clears the statistics on Keepalive packets sent and received by a GRE tunnel interface.

Format

reset keepalive packets count

Parameters

None

Views

Tunnel interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the Keepalive function is enabled on a GRE tunnel, the VPN cannot choose a tunnel with an unreachable remote end, preventing data loss. You can run the **display keepalive packets count** command to view the statistics on Keepalive packets and Keepalive response packets sent and received by the GRE tunnel interface, and the running status of the GRE tunnel.

The **reset keepalive packets count** command resets the statistics of Keepalive packets and Keepalive response packets sent and received by the GRE tunnel interface. You can monitor the running status of the GRE tunnel.

Precautions

The cleared packet statistics cannot be restored. Exercise caution when you run the command.

Example

# Reset the Keepalive packet statistics of GRE tunnel interface 1.

```
<HUAWEI> system-view
[HUAWEI] interface tunnel 1
[HUAWEI-Tunnel1] tunnel-protocol gre
[HUAWEI-Tunnel1] reset keepalive packets count
 Info: Succeeded in resetting tunnel keepalive packets count.
```

10.1.12 source

Function

The **source** command configures the source address or source interface of the tunnel.

The **undo source** command deletes the configured source address or source interface.

The source address and source interface of a tunnel are not specified by default.

Format

source { *source-ip-address* | *interface-type interface-number* }

undo source

Parameters

Parameter	Description	Value
source-ip-address	Specifies the source address of a tunnel interface. If a tunnel interface works in IPv4-IPv6 mode, specify an IPv6 address as the source address of the tunnel interface.	The IPv4 address is in dotted decimal notation. The IPv6 address is a 32-digit hexadecimal number, in the format X:X:X:X:X:X:X:X.
interface-type interface-number	Specifies the type and the number of the source interface of the tunnel. The following types of interfaces are often used: VLANIF and loopback.	-

Views

Tunnel interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When configuring a GRE, MPLS TE, IPv4 over IPv6 tunnel or manual IPv6 over IPv4 tunnel, create a tunnel interface. After a tunnel interface is created, run the **source** command to specify the source IP address for the tunnel interface.

Prerequisites

A tunnel interface has been created using the **interface tunnel** command, and the encapsulation mode is set to GRE, MPLS TE, IPv4 over IPv6 or IPv6 over IPv4 of manual mode using the **tunnel-protocol** command.

Precautions

Two tunnel interfaces with the same encapsulation mode, source address, and destination address cannot be configured simultaneously.

You can configure a main interface working in Layer 3 mode as the source tunnel interface.

On the GRE, MPLS TE, IPv4 over IPv6 tunnel or manual IPv6 over IPv4 tunnel, the source address of the local tunnel interface is the destination address of the remote tunnel interface, and the destination address of the local tunnel interface is the source address of the remote tunnel interface.

Example

# Set the tunnel type of Tunnel1 to IPv6 over IPv4 of manual mode and configure the source IP address of Tunnel1 as 10.1.1.1.

```
<HUAWEI> system-view
[HUAWEI] interface tunnel 1
[HUAWEI-Tunnel1] tunnel-protocol ipv6-ipv4
[HUAWEI-Tunnel1] source 10.1.1.1
```

# Configure Tunnel1 of GRE and use Loopback1 address as the interface address.

```
<HUAWEI> system-view
[HUAWEI] interface Loopback 1
[HUAWEI-LoopBack1] ip address 10.2.1.1 32
[HUAWEI-LoopBack1] quit
[HUAWEI] interface tunnel 1
[HUAWEI-Tunnel1] tunnel-protocol gre
[HUAWEI-Tunnel1] source loopback 1
```

10.1.13 statistic enable (Tunnel interface view)

Function

The **statistic enable** command enables traffic statistics collection on a Tunnel interface.

The **undo statistic enable** command disables traffic statistics collection on a Tunnel interface.

By default, traffic statistics collection is disabled on a Tunnel interface.

Format

statistic enable { **both** | **inbound** | **outbound** }

undo statistic enable { **both** | **inbound** | **outbound** }

Parameters

Parameter	Description	Value
both	Enables traffic statistics collection for incoming and outgoing traffic.	-
inbound	Enables incoming traffic statistics collection.	-
outbound	Enables outgoing traffic statistics collection.	-

Views

Tunnel interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To check the network status or locate network faults, you can use the **statistic enable** command to enable traffic statistics collection on Tunnel interfaces. The device then collect traffic statistics on the Tunnel interfaces.

Prerequisites

The protocol type of the tunnel interface has been configured using the **tunnel-protocol** command.

Precautions

After running the **statistic enable** command on an interface, you can run the **display interface tunnel** command to view the traffic statistics on the interface. The traffic statistics help you diagnose the fault of a tunnel.

Example

# Enable incoming traffic statistics collection on a Tunnel interface.

```
<HUAWEI> system-view
[HUAWEI] interface tunnel 1
[HUAWEI-Tunnel1] statistic enable inbound
```

10.1.14 tunnel-protocol

Function

The **tunnel-protocol** command configures the tunnel protocol on a tunnel interface.

The **undo tunnel-protocol** command restores the tunnel protocol to the default configuration.

By default, no tunnel protocol is used on a tunnel interface.

Format

tunnel-protocol { **gre** | **ipv6-ipv4** [**6to4** | **isatap**] | **ipv4-ipv6** | **mpls te** | **none** }

undo tunnel-protocol

Parameters

Parameter	Description	Value
gre	Indicate that the GRE tunnel protocol is configured on a tunnel 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 the parameters.	-
ipv4-ipv6	Indicate that the IPv4 to IPv6 tunnel protocol is configured on a tunnel interface. **NOTE** Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S support the parameter.	-
ipv6-ipv4 [**6to4** | **isatap**]	Configure the tunnel protocol of the tunnel interface as ipv6-ipv4: ● **ipv6-ipv4**: use a manual IPv6 over IPv4 tunnel ● **ipv6-ipv4 6to4** : using 6to4 tunnel ● **ipv6-ipv4 isatap** : using isatap tunnel **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 these parameter.	-
mpls te	Indicate that the MPLS TE tunnel protocol is configured on a tunnel interface. **NOTE** Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6720-EI, S6720S-EI, S6730-H, S6730-S, S6730S-S, and S6730S-H support the parameter.	-
none	Indicate that no tunnel protocol is configured on a tunnel interface.	-

Views

Tunnel interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After creating a tunnel interface using the **interface tunnel** command, run the **tunnel-protocol** command to configure the tunnel encapsulation mode for the tunnel interface.

The following tunnel encapsulation modes are available:

- GRE: encapsulates packets of some network layer protocols such as IP or IPX to enable these encapsulated packets to be transmitted on networks running other protocols such as IP.
- IPv4-IPv6: creates tunnels on the IPv6 networks to connect IPv4 isolated sites so that IPv4 isolated sites can access other IPv4 networks through the IPv6 public network.
- IPv6-IPv4: creates tunnels on the IPv4 networks to connect IPv6 isolated sites so that IPv6 packets can be transmitted on IPv4 networks.
- MPLS TE: integrates the MPLS technology with traffic engineering. It can reserve resources by setting up LSP tunnels for a specified path in an attempt to avoid network congestion and balance network traffic.

Precautions

- The **none** mode indicates the initial configuration, that is, no tunnel encapsulation mode is configured. In practice, you must select another tunnel encapsulation mode.
- You must configure the tunnel encapsulation mode before setting the source IP address or other parameters for a tunnel interface. Changing the encapsulation mode of a tunnel interface deletes other parameters of the tunnel interface.

Example

# Set the tunnel encapsulation mode of Tunnel2 to GRE.

```
<HUAWEI> system-view
[HUAWEI] interface tunnel 2
[HUAWEI-Tunnel2] tunnel-protocol gre
```

10.2 IPSec Configuration Commands (IPSec Encryption)

10.2.1 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.

10.2.2 ah authentication-algorithm

Function

The **ah authentication-algorithm** command configures the authentication algorithm for AH.

The **undo ah authentication-algorithm** command restores the default authentication algorithm for AH.

By default, AH uses the Secure Hash Algorithm-256 (SHA2-256) authentication algorithm.

Format

ah authentication-algorithm { **sha1** | **sha2-256** }

undo ah authentication-algorithm

Parameters

Parameter	Description	Value
sha1	Specifies Secure Hash Algorithm-1 (SHA-1) as the authentication algorithm. SHA-1 generates a 160-bit message summary based on a message of less than 2^{64} bits.	-
sha2-256	Specifies SHA2-256 as the authentication algorithm. SHA2-256 generates a 256-bit message summary based on a message of less than 2^{64} bits.	-

Views

IPSec proposal view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

IPSec can use AH to authenticate packets, preventing packets from being intercepted or modified, you can run the **ah authentication-algorithm** command to configure the authentication algorithm for AH.

Prerequisite

The protocol of this IPSec proposal has been configured to AH using the **transform** command.

Precautions

The authentication algorithms on both IPSec peers must be identical.

The system software does not support the **md5** parameter. To use the **md5** parameter, you need to install the WEAKEA plug-in. For higher security purposes, you are advised to specify the **sha2-256** parameter.

For details about how to install the WEAKEA plug-in, see WEAKEA Configuration.

Example

# Configure the IPSec proposal **prop1** to use the AH protocol, and specify SHA2-256 as the authentication algorithm.

```
<HUAWEI> system-view
[HUAWEI] ipsec proposal prop1
[HUAWEI-ipsec-proposal-prop1] transform ah
[HUAWEI-ipsec-proposal-prop1] ah authentication-algorithm sha2-256
```

10.2.3 display ipsec proposal

Function

The **display ipsec proposal** command displays IPSec proposal information.

Format

display ipsec proposal [**name** *proposal-name*]

Parameters

Parameter	Description	Value
name *proposal-name*	Specifies the name of an IPSec proposal.	The value is an existing name of an IPSec proposal.

Views

All views

Default Level

1: Monitoring Level

Usage Guidelines

After IPSec is configured, when valid packets are dropped between IPSec peers, you can run the **display ipsec proposal** command to check whether the IPSec proposal configurations on both IPSec peers are identical.

IPSec ensures security using the IPSec proposal. You can run the **display ipsec proposal** command to view the following information:

- Name of the IPSec proposal

- Encapsulation mode defined in the IPSec proposal
- Security protocol defined in the IPSec proposal
- Authentication and encryption algorithms defined in the IPSec proposal

Example

# Display information about all IPSec proposals.

```
<HUAWEI> display ipsec proposal
  Total IP security proposal number: 1

  IP security proposal name: proposal1
    encapsulation mode: transport
    transform: esp-new
    ESP protocol: authentication SHA2-HMAC-256, encryption AES-192
```

Table 10-6 Description of the **display ipsec proposal** command output

Item	Description
Total IP security proposal number	Number of IPSec proposals created.
IP security proposal name	Name of an IPSec proposal. To configure an IPSec proposal, run the **ipsec proposal** command.
encapsulation mode	IPSec encapsulation mode: ● transport ● tunnel To configure an encapsulation mode, run the **encapsulation-mode** command.
transform	Security protocol defined in the security proposal: ● esp-new: ESP ● ah-new: AH To configure a security protocol, run the **transform** command.
ESP protocol	The authentication algorithm and encryption algorithm used by the ESP protocol. To configure the authentication algorithm and encryption algorithm, run the **esp authentication-algorithm** and **esp encryption-algorithm** command separately.
AH protocol	To configure an authentication algorithm used by the AH protocol, run the **ah authentication-algorithm** command.

10.2.4 display ipsec sa

Function

The **display ipsec sa** command displays information about a Security Association (SA).

Format

display ipsec sa [**name** *sa-name*] [**brief**]

Parameters

Parameter	Description	Value
name *sa-name*	Specifies the SA name.	The value is an existing SA name.
brief	Displays brief information of the SA, such as the SA name and the Security Parameter Index (SPI) value.	-

Views

All views

Default Level

1: Monitoring Level

Usage Guidelines

Usage Scenario

You can run the **display ipsec sa** command to check whether the SA configurations for outgoing packets on the local end are identical with those for incoming packets on the peer end. The **display ipsec sa** command output displays the following information:

- SA name
- Security proposal applied to the SA
- Number of times the SA is applied
- SA configurations for incoming Authentication Header (AH) packets
- SA configurations for outgoing AH packets
- SA configurations for incoming Encapsulating Security Payload (ESP) packets
- SA configurations for outgoing ESP packets

Example

# Display configurations of the SA.

```
<HUAWEI> display ipsec sa
 IP security association name: sa1
 Number of references: 0
   proposal name: prop1
   inbound AH setting:
     AH spi:
     AH string-key:
     AH authentication hex key: %^%#0D_@HS5002;U1AR{t$3W:H188Ghs~N'_r`Y&R<j70V5-,r-NF(z!
92N)oSNA%^%#
   inbound ESP setting:
     ESP spi:
     ESP string-key:
     ESP encryption hex key: %^%#A*v9(B!U3U%*HL%Rod;%|G}F;B3[5%q#VMTG#9EP%^%#
     ESP authentication hex key: %^%#w_eeVg;FD3ybX!(2&P2ecMN%'JMGWXm^bR#qcUNKj_3AGrb@#
\B4(Vn5cYC%^%#
   outbound AH setting:
     AH spi:
     AH string-key:
     AH authentication hex key: %^%#jp!o1aA7qD^qMN&yI4M8nG_(~~O.{8;tyqI3%o5M4&L@G]rJw/
au]r'm=j^9%^%#
   outbound ESP setting:
     ESP spi:
     ESP string-key:
     ESP encryption hex key: %^%#".dAYkLlqV_o-'SI0.":&<M';66l4UGMEjB9Cl\S%^%#
     ESP authentication hex key: %^%#Nkz8Z-sF*Pw3clT]@_F9B4:8>RIwc'r#sCJl0N[;{drLI|
%uU5lVUWQkY3p1%^%#
```

Table 10-7 Description of the **display ipsec sa** command output

Item	Description
IP security association name	SA name
Number of references	Number of times the SA is applied
proposal name	Security proposal applied to the SA
inbound AH setting	SA configurations for incoming AH packets
AH spi	SPI for AH
AH string-key	Authentication key for AH in the string format displayed in cipher text
AH authentication hex key	Authentication key for AH in cipher text
inbound ESP setting	SA configurations for incoming ESP packets
ESP spi	SPI for ESP
ESP string-key	Authentication key for ESP in the string format displayed in cipher text
ESP encryption hex key	Encryption key for ESP in cipher format

Item	Description
ESP authentication hex key	Authentication key for ESP in cipher text
outbound AH setting	SA configurations for outgoing AH packets
outbound ESP setting	SA configurations for outgoing ESP packets

10.2.5 display ipsec statistics

Function

The **display ipsec statistics** command displays the statistics about packets processed by IPSec.

Format

display ipsec statistics [**sa-name** *sa-name* **slot** *slot-number*]

Parameters

Parameter	Description	Value
sa-name *sa-name*	Specifies the IPSec Security Association (SA) name.	The value is an existing SA name.
slot *slot-number*	Displays the IPSec SA statistics of the specified slot.	The value is an integer, and the value range depends on the device configuration.

Views

All views

Default Level

1: Monitoring Level

Usage Guidelines

Usage Scenario

After IPSec protection is configured for a routing protocol, you can run the **display ipsec statistics** command to view information about transmitted packets and dropped packets. The details are as follows:

- Number of received and sent packets
- Number of received and sent bytes
- Number of dropped incoming and outgoing packets
- Detailed information about dropped packets

Example

# Display statistics about packets processed by IPSec.

```
<HUAWEI> display ipsec statistics
 IPv6 security packet statistics:
   input/output security packets: 0/0
   input/output security bytes: 0/0
   input/output dropped security packets: 0/0
   dropped security packet detail:
     memory process problem: 0
     can't find SA: 0
     queue is full: 0
     authentication is failed: 0
     wrong length: 0
     replay packet: 0
     too long packet: 0
     invalid SA: 0
     policy deny: 0
 the normal packet statistics:
   input/output dropped normal packets: 0/0
 IPv4 security packet statistics:
   input/output security packets: 0/0
   input/output security bytes: 0/0
   input/output dropped security packets: 0/0
   dropped security packet detail:
     memory process problem: 0
     can't find SA: 0
     queue is full: 0
     authentication is failed: 0
     wrong length: 0
     replay packet: 0
     too long packet: 0
     invalid SA: 0
     policy deny: 0
 the normal packet statistics:
   input/output dropped normal packets: 0/0
```

Table 10-8 Description of the **display ipsec statistics** command output

Item	Description
IPv6 security packet statistics	Statistics on IPv6 security packets.
IPv4 security packet statistics	Statistics on IPv4 security packets.
input/output security packets	Indicates the number of received and sent packets.
input/output security bytes	Indicates the number of received and sent bytes.
input/output dropped security packets	Indicates the number of dropped incoming and outgoing packets.

Item	Description
dropped security packet detail	Detailed information about dropped packets.
memory process problem	Indicates the number of packets that are dropped due to a memory fault.
can't find SA	Indicates the number of packets that are dropped because no SA is found.
queue is full	Indicates the number of packets that are dropped because the queue is full.
authentication is failed	Indicates the number of packets that are dropped due to authentication failure.
wrong length	Indicates the number of packets that are dropped due to a packet length fault.
replay packet	Indicates the number of packets that are dropped due to repeated transmission.
too long packet	Indicates the number of packets that are dropped due to excess packet length.
invalid SA	Indicates the number of packets that are dropped due to an invalid SA.
policy deny	Indicates the number of packets that are dropped due to a deny action in the policy.
the normal packet statistics	Statistics about normal packets.
input/output dropped normal packets	Indicates the number of received/sent normal packets that are dropped.

10.2.6 encapsulation-mode

Function

The **encapsulation-mode** command sets the encapsulation mode for IP packets.

The **undo encapsulation-mode** command restores the default encapsulation mode for IP packets.

By default, the encapsulation mode is set to **tunnel**.

Format

encapsulation-mode { **transport** | **tunnel** }

undo encapsulation-mode

Parameters

Parameter	Description	Value
transport	Sets the encapsulation mode to **transport**.	-
tunnel	Sets the encapsulation mode to **tunnel**.	-

Views

IPSec proposal view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can configure Authentication Header (AH) or Encapsulating Security Payload (ESP) to ensure security based on data confidentiality. If AH is configured, an AH header is generated; if ESP is configured, an ESP header, an ESP tail, and an ESP authentication field are generated. Two encapsulation modes are available for IPSec: transport and tunnel.

- The transport mode is applicable to a scenario in which two hosts, or a host and a security gateway, are communicating with each other. In transport mode, the two devices encrypting and decrypting packets must be the original packet sender and the final receiver, respectively.
- The tunnel mode is generally applied to a scenario in which two security gateways are communicating with each other. The packets that are encrypted on the local security gateway can be decrypted only on the peer security gateway. Therefore, an IP packet must be encapsulated using the tunnel mode and an IP header embed. After arriving at the peer security gateway, the IP packet can be decrypted.

Precautions

The encapsulation modes on both IPSec peers must be identical.

Example

# Set the encapsulation mode to **transport** in the security proposal named **prop2**.

```
<HUAWEI> system-view
[HUAWEI] ipsec proposal prop2
[HUAWEI-ipsec-proposal-prop2] encapsulation-mode transport
```

10.2.7 esp authentication-algorithm

Function

The **esp authentication-algorithm** command configures the authentication algorithm for ESP.

The **undo esp authentication-algorithm** command cancels the authentication algorithm for ESP.

By default, ESP uses the Secure Hash Algorithm-256 (SHA2-256) authentication algorithm.

Format

esp authentication-algorithm { **sha1** | **sha2-256** }

undo esp authentication-algorithm

Parameters

Parameter	Description	Value
sha1	Specifies Secure Hash Algorithm-1 (SHA-1) as the authentication algorithm. SHA-1 generates a 160-bit message summary based on a message of less than 2^{64} bits.	-
sha2-256	Specifies SHA2-256 as the authentication algorithm. SHA2-256 generates a 256-bit message summary based on a message of less than 2^{64} bits.	-

Views

IPSec proposal view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

IPSec can use ESP protocol to authenticate and encrypt packets, preventing packets from being intercepted or modified, you can run the **esp authentication-algorithm** command to configure the authentication algorithm for ESP.

Prerequisite

The protocol of this IPSec proposal has been configured to ESP using the **transform** command.

Precautions

The authentication algorithms on both IPSec peers must be identical.

The authentication algorithm and encryption algorithm cannot be both set to **NULL** for ESP.

The system software does not support the **md5** parameter. To use the **md5** parameter, you need to install the WEAKEA plug-in. For higher security purposes, you are advised to specify the **sha2-256** parameter.

For details about how to install the WEAKEA plug-in, see WEAKEA Configuration.

Example

# Configure the IPSec proposal **prop1** to use the ESP protocol, and specify SHA2-256 as the authentication algorithm.

```
<HUAWEI> system-view
[HUAWEI] ipsec proposal prop1
[HUAWEI-ipsec-proposal-prop1] transform esp
[HUAWEI-ipsec-proposal-prop1] esp authentication-algorithm sha2-256
```

10.2.8 esp encryption-algorithm

Function

The **esp encryption-algorithm** command configures the encryption algorithm for ESP protocol.

The **undo esp encryption-algorithm** command cancels the encryption algorithm for ESP protocol.

By default, ESP protocol uses the Advanced Encryption Standard-256 (AES-256) encryption algorithm.

Format

esp encryption-algorithm { **3des** | **aes** [**128** | **192** | **256**] }

undo esp encryption-algorithm

Parameters

Parameter	Description	Value
3des	Indicates that ESP uses 3DES algorithm to encrypt packets.	-

Parameter	Description	Value
aes	Indicates that ESP uses Advanced Encryption Standard (AES) algorithm in CBC mode to encrypt packets. By default, If 128, 192 and 256 are not configured, AES 128 bits algorithm is used for ESP to encrypt packets.	-
128	Indicates that ESP uses AES 128 bits algorithm to encrypt packets.	-
192	Indicates that ESP uses AES 192 bits algorithm to encrypt packets.	-
256	Indicates that ESP uses AES 256 bits algorithm to encrypt packets.	-

Views

IPSec proposal view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

IPSec can use ESP protocol to authenticate and encrypt packets, preventing packets from being intercepted or modified, you can run the **esp encryption-algorithm** command to configure the encryption algorithm for ESP protocol.

Prerequisite

The protocol of this IPSec proposal has been configured to ESP using the **transform** command.

Precautions

The encryption algorithms on both IPSec peers must be identical.

The authentication algorithm and encryption algorithm cannot be both set to **NULL** for ESP.

The system software does not support the **des** parameter. To use the **des** parameter, you need to install the WEAKEA plug-in. For higher security purposes, you are advised to specify the **aes** [**128** | **192** | **256**] parameter.

For details about how to install the WEAKEA plug-in, see WEAKEA Configuration.

Example

# Configure the IPSec proposal **prop1** to use the ESP protocol, and specify AES-128 as the encryption algorithm.

```
<HUAWEI> system-view
[HUAWEI] ipsec proposal prop1
[HUAWEI-ipsec-proposal-prop1] transform esp
[HUAWEI-ipsec-proposal-prop1] esp encryption-algorithm aes 128
```

10.2.9 ipsec proposal

Function

The **ipsec proposal** command creates an IPSec proposal and displays the IPSec proposal view.

The **undo ipsec proposal** command deletes an IPSec proposal.

By default, no IPSec proposal is configured.

Format

ipsec proposal *proposal-name*

undo ipsec proposal *proposal-name*

Parameters

Parameter	Description	Value
proposal-name	Specifies the name of an IPSec proposal.	The value is a string of 1 to 15 case-insensitive characters without question marks (?) or spaces. When double quotation marks are used around the string, spaces are allowed in the string.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

An IPSec proposal, part of an IPSec SA, defines security parameters for IPSec SA negotiation, including the security protocol, encryption and authentication algorithms, and encapsulation mode.

Follow-up Procedure

Run the **proposal** command to reference the IPSec proposal in an IPSec SA.

Precautions

Both ends of an IPSec tunnel must be configured with the same parameters.

You cannot delete the security proposal applied on a Security Association (SA). However, you can apply the same proposal on different SA's. To delete a security proposal, run the **undo proposal** command to remove a security proposal from the SA.

Example

# Create an IPSec proposal **newprop1**.

```
<HUAWEI> system-view
[HUAWEI] ipsec proposal newprop1
[HUAWEI-ipsec-proposal-newprop1]
```

10.2.10 ipsec sa

Function

The **ipsec sa** command creates an SA and displays the SA view.

The **undo ipsec sa** command deletes an SA.

By default, no SA is created.

Format

ipsec sa *sa-name*

undo ipsec sa *sa-name*

Parameters

Parameter	Description	Value
sa-name	Specifies the name of an SA.	The value is a string of 1 to 15 case-insensitive characters without question marks (?) or spaces. When double quotation marks are used around the string, spaces are allowed in the string.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

IPSec uses an SA to ensure security during data transmission. When configuring IPSec, run the **ipsec sa** command to create an SA and configure SA parameters.

Follow-up Procedure

Run the **proposal** command to import a security proposal; run the **sa spi** command to configure the SPI; run the **sa string-key** or **sa authentication-hex** command to configure the authentication key.

Precautions

An SA is unidirectional. Incoming packets and outgoing packets are processed by different SAs.

An SA can be configured with only one security protocol.

Example

# Create an SA.

```
<HUAWEI> system-view
[HUAWEI] ipsec sa sa1
[HUAWEI-ipsec-sa-sa1]
```

10.2.11 proposal

Function

The **proposal** command applies a security proposal to a Security Association (SA).

The **undo proposal** command removes a security proposal from an SA.

By default, no security proposal is created.

Format

proposal *proposal-name*

undo proposal

Parameters

Parameter	Description	Value
proposal-name	Specifies the name of an IPSec proposal.	The value is an existing IPSec proposal name.

Views

SA view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

An SA defines a protection policy, and a security proposal defines a protection method. Data protection can be implemented only after a security proposal is applied to an SA.

Prerequisite

The **ipsec proposal** command has been run to create a security proposal before the **proposal** command is run. If no security proposal has been created, an error message will be displayed when the **proposal** command is run.

Before running the **proposal** command, it needs to set the encapsulation mode to transport.

Precautions

After the **proposal** command is run, the security proposal is applied to an SA and cannot be deleted.

Example

# Create an IPSec proposal **prop1** and configure it to use the default parameters. Then reference the IPSec proposal in IPSec SA **sa1**.

```
<HUAWEI> system-view
[HUAWEI] ipsec proposal prop1
[HUAWEI-ipsec-proposal-prop1] transform ah
[HUAWEI-ipsec-proposal-prop1] encapsulation-mode transport
[HUAWEI-ipsec-proposal-prop1] quit
[HUAWEI] ipsec sa sa1
[HUAWEI-ipsec-sa-sa1] proposal prop1
```

10.2.12 reset ipsec statistics

Function

The **reset ipsec statistics** command clears statistics about packets processed by IPSec.

Format

reset ipsec statistics [**sa-name** *sa-name* **slot** *slot-number*]

Parameters

Parameter	Description	Value
sa-name *sa-name*	Specifies the IPSec Security Association (SA) name.	The value is an existing SA name.
slot *slot-number*	Displays the IPSec SA statistics of the specified slot.	The value is an integer, and the value range depends on the device configuration.

Views

User view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Before collecting statistics about packets processed by IPSec in a specified length of time, you can run the **reset ipsec statistics** command to clear the original statistics.

Follow-up Procedure

Run the **display ipsec statistics** command to check statistics about packets processed by IPSec.

Precautions

The statistics cannot be restored after being cleared. Therefore, confirm the action before running this command.

Example

# Clear statistics about packets processed by IPSec.

```
<HUAWEI> reset ipsec statistics
```

10.2.13 sa authentication-hex

Function

The **sa authentication-hex** command sets an authentication in hexadecimal format or cipher text for Security Associations (SAs).

The **undo sa authentication-hex** command deletes an authentication key from SAs.

By default, no authentication key is created.

Format

sa authentication-hex { **inbound** | **outbound** } { **ah** | **esp** } [**cipher**] { *hex-plain-key* | *hex-cipher-key* }

undo sa authentication-hex { **inbound** | **outbound** } { **ah** | **esp** }

Parameters

Parameter	Description	Value
inbound	Specifies SA parameters for incoming packets.	-
outbound	Specifies SA parameters for outgoing packets.	-
ah	Specifies SA parameters for Authentication Header (AH). If the security proposal applied to an SA uses AH, **ah** must be configured in the **sa authentication-hex** command.	-
esp	Specifies SA parameters for Encapsulating Security Payload (ESP). If the security proposal applied to an SA uses ESP, **esp** must be configured in the **sa authentication-hex** command.	-
cipher	Indicates the cipher text used for authentication.	-
hex-plain-key	Sets the authentication password to be in plaintext format.	The value is in hexadecimal notation. ● If authentication algorithm Message Digest 5 (MD5) is used, the length of the key is 16 bytes. ● If authentication algorithm Secure Hash Algorithm-1 (SHA-1) is used, the length of the key is 20 bytes. ● If authentication algorithm SHA2-256 is used, the length of the key is 32 bytes.

Parameter	Description	Value
hex-cipher-key	Sets the authentication password to be in ciphertext format.	The value is a string of case-insensitive characters, spaces not supported. ● If authentication algorithm MD5 is used, the length of the key is 68. ● If authentication algorithm SHA-1 is used, the length of the key is 88. ● If authentication algorithm SHA2-256 is used, the length of the key is 108.

Views

SA view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

AH and ESP can use either MD5, SHA-1, or SHA-256 that require an authentication key in the string or hexadecimal format. If an authentication key in the hexadecimal format is required, run the **sa authentication-hex** command. The MD5 and SHA-1 algorithms are not recommended because they cannot meet your security defense requirements.

Precautions

Set parameters for both **inbound** and **outbound** SAs.

SA parameters on both IPSec peers must be identical. The authentication key for incoming packets on the local end must be identical with that for outgoing packets on the peer end and vice versa.

The authentication key can be in the hexadecimal or string format. To configure an authentication key in the string format, run the **sa string-key** command. If multiple authentication keys are configured, the latest one takes effect. The formats of authentication keys on both IPSec peers must be identical. If an authentication key in the string format is configured on one end and an authentication key in the hexadecimal format on another end, the two ends cannot communicate.

Example

# In an IPSec SA, set the authentication key of the inbound SA to 112233445566778899aabbccddeeff00, and the authentication key of the

outbound SA to aabbccddeeff001100aabbccddeeff00. The authentication key is displayed in cipher text.

```
<HUAWEI> system-view
[HUAWEI] ipsec sa sa1
[HUAWEI-ipsec-sa-sa1] sa authentication-hex inbound ah cipher 112233445566778899aabbccddeeff00
[HUAWEI-ipsec-sa-sa1] sa authentication-hex outbound ah cipher aabbccddeeff001100aabbccddeeff00
```

10.2.14 sa encryption-hex

Function

The **sa encryption-hex** command configures an encryption key for manual Security Association (SA) in hexadecimal format.

The **undo sa encryption-hex** command deletes an encryption key for manual SA configured in hexadecimal format.

By default, no encryption key is created.

Format

sa encryption-hex { **inbound** | **outbound** } **esp** [**cipher**] { *hex-plain-key* | *hex-cipher-key* }

undo sa encryption-hex { **inbound** | **outbound** } **esp**

Parameters

Parameter	Description	Value
inbound	Specifies SA parameters for incoming packets.	-
outbound	Specifies SA parameters for outgoing packets.	-
esp	Specifies SA parameters for Encapsulating Security Payload (ESP). If the security proposal applied to an SA uses ESP, **esp** must be configured in the **sa encryption-hex** command.	-
cipher	Indicates the ciphertext used for encryption.	-

Parameter	Description	Value
hex-plain-key	Sets the authentication password to be in plaintext format.	The value is in hexadecimal notation. ● If encryption algorithm Data Encryption Standard (DES) is used, the length of the key is 8 bytes. ● If encryption algorithm Triple Data Encryption Standard (3DES) is used, the length of the key is 24 bytes. ● If encryption algorithm Advanced Encryption Standard 128 (AES-128) is used, the length of the key is 16 bytes. ● If encryption algorithm AES-192 is used, the length of the key is 24 bytes. ● If encryption algorithm AES-256 is used, the length of the key is 32 bytes.
hex-cipher-key	Sets the authentication password to be in ciphertext format.	The value is a string of case-insensitive characters, spaces not supported. ● If encryption algorithm DES is used, the length of the key is 48. ● If encryption algorithm 3DES is used, the length of the key is 88. ● If encryption algorithm AES-128 is used, the length of the key is 68. ● If encryption algorithm AES-192 is used, the length of the key is 88. ● If encryption algorithm AES-256 is used, the length of the key is 108.

Views

SA view

Default Level

2: Configuration level

Usage Guidelines

ESP security protocol support encryption of IP packets. The algorithm used for encryption/decryption is either DES, 3DES or AES. These algorithms need a key either in hexadecimal format to operate. The hexadecimal key to be used for encryption is configured using the **sa encryption-hex** command.

NOTICE

- The DES and 3DES algorithms have security risks; therefore, you are advised to use AES algorithm preferentially.
- If **sa encryption-hex** command is configured, then the encryption key configured using **sa string-key** command is deleted automatically.

Example

# In an IPSec SA, set the encryption key of the inbound SA to 0x1234567890abcdef, and the encryption key of the outbound SA to 0xabcdefabcdef1234. The encryption key is displayed in cipher text.

```
<HUAWEI> system-view
[HUAWEI] ipsec sa sa1
[HUAWEI-ipsec-sa-sa1] sa encryption-hex inbound esp cipher 1234567890abcdef
[HUAWEI-ipsec-sa-sa1] sa encryption-hex outbound esp cipher abcdefabcdef1234
```

10.2.15 sa spi

Function

The **sa spi** command configures the Security Parameter Index (SPI) for a Security Association (SA).

The **undo sa spi** command deletes the SPI from an SA.

By default, no SPI is configured.

Format

sa spi { **inbound** | **outbound** } { **ah** | **esp** } *spi-number*

undo sa spi { **inbound** | **outbound** } { **ah** | **esp** }

Parameters

Parameter	Description	Value
inbound	Specifies SA parameters for incoming packets.	-
outbound	Specifies SA parameters for outgoing packets.	-
ah	Specifies SA parameters for Authentication Header (AH). If the security proposal applied to an SA uses AH, **ah** must be configured in the **sa spi** command.	-

Parameter	Description	Value
esp	Specifies SA parameters for Encapsulating Security Payload (ESP). If the security proposal applied to an SA uses ESP, **esp** must be configured in the **sa spi** command.	-
spi-number	Specifies the SPI.	The value is an integer ranging from 256 to 4294967295.

Views

SA view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

SPI uniquely identifies an SA. When an SPI is configured for an SA, the SPI is carried in each sent packet. The receiver checks the packet authenticity based on the SPI. When the **ipsec sa** *sa-name* command is used to create an SA, run the **sa spi** command to configure the SPI.

Precautions

Set parameters for both **inbound** and **outbound** SAs.

The SPI for incoming packets on the local end must be identical with that for outgoing packets on the peer end and vice versa.

Example

# In an IPSec SA, set the SPI of the inbound SA to 10000 and the SPI of the outbound SA to 20000.

```
<HUAWEI> system-view
[HUAWEI] ipsec sa sa1
[HUAWEI-ipsec-sa-sa1] sa spi inbound ah 10000
[HUAWEI-ipsec-sa-sa1] sa spi outbound ah 20000
```

10.2.16 sa string-key

Function

The **sa string-key** command configures an authentication key in the string format.

The **undo sa string-key** command deletes an authentication key from Security Associations (SAs).

By default, no authentication key is created.

Format

sa string-key { **inbound** | **outbound** } { **ah** | **esp** } [**cipher**] *string-cipher-key*

undo sa string-key { **inbound** | **outbound** } { **ah** | **esp** }

Parameters

Parameter	Description	Value
inbound	Specifies SA parameters for incoming packets.	-
outbound	Specifies SA parameters for outgoing packets.	-
ah	Specifies SA parameters for Authentication Header (AH). If the security proposal applied to an SA uses AH, **ah** must be configured in the **sa string-key** command.	-
esp	Specifies SA parameters for Encapsulating Security Payload (ESP). If the security proposal applied to an SA uses ESP, **esp** must be configured in the **sa string-key** command.	-
cipher	Indicates the cipher text used for authentication.	-
string-cipher-key	Specifies the cipher text key.	The value is a string of case-sensitive characters that can be letters or digits. The authentication password can be a string of 1 to 127 characters in plain text or a string of 20 to 392 characters in encrypted text. Except the question mark (?) and space. However, when quotation marks (") are used around the string, spaces are allowed in the string.

Views

SA view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

AH and ESP can use either Message Digest 5 (MD5), Secure Hash Algorithm 1 (SHA-1) or SHA-256, that require an authentication key in the string or hexadecimal format. If an authentication key in the string format is required, run the **sa string-key** command. The MD5 and SHA-1 algorithms are not recommended because they cannot meet your security defense requirements.

Precautions

Set parameters for both **inbound** and **outbound** SAs.

SA parameters on both IPSec peers must be identical. The authentication key for incoming packets on the local end must be identical with that for outgoing packets on the peer end and vice versa.

The authentication key can be in the hexadecimal or string format. To configure an authentication key in the hexadecimal format, run the **sa authentication-hex** command. If multiple authentication keys are configured, the latest one takes effect. The formats of authentication keys on both IPSec peers must be identical. If an authentication key in the string format is configured on one end and an authentication key in the hexadecimal format on another end, the two ends cannot communicate.

Example

# In an IPSec SA, set the authentication key of the inbound SA to abcdef, and the authentication key of the outbound SA to efcdab. The authentication key is displayed in cipher text.

```
<HUAWEI> system-view
[HUAWEI] ipsec sa sa1
[HUAWEI-ipsec-sa-sa1] sa string-key inbound ah cipher abcdef
[HUAWEI-ipsec-sa-sa1] sa string-key outbound ah cipher efcdab
```

10.2.17 transform

Function

The **transform** command configures the security protocol in a security proposal.

The **undo transform** command restores the default security protocol.

By default, the Encapsulating Security Payload (ESP) protocol is used, as defined in RFC.

Format

transform { **ah** | **esp** }

undo transform

Parameters

Parameter	Description	Value
ah	Configures Authentication Header (AH) as the security protocol.	-
esp	Configures ESP as the security protocol.	-

Views

IPSec proposal view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

- When AH is specified, AH only authenticates packets.

  When AH is specified, by default, AH uses the SHA-256 authentication algorithm.
- When ESP is specified, ESP can encrypt/authenticate, or encrypt and authenticate packets.

  When ESP is specified, ESP uses the SHA-256 authentication algorithm, the AES-256 encryption algorithm.

AH prevents data tampering but cannot prevent data interception, so it applies only to the transmission of non-confidential data. ESP provides authentication service inferior to that of AH, but it can encrypt packet payloads.

Follow-up Procedure

Configure the authentication algorithm for AH when AH is used.

Configure the authentication and encryption algorithms for ESP when ESP is used.

Precautions

When multiple security proposals are configured, the latest configuration takes effect, and the default authentication and encryption algorithms will be restored.

The IPSec proposals configured on both ends of an IPSec tunnel must use the same security tunnel.

Example

# Configure AH for the security proposal named **prop**.

```
<HUAWEI> system-view
[HUAWEI] ipsec proposal prop
[HUAWEI-ipsec-proposal-prop] transform ah
```

10.3 IPSec Configuration Commands (IPSec Efficient VPN)

10.3.1 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.

10.3.2 anti-replay window

Function

The **anti-replay window** command sets the anti-replay window size for an IPSec tunnel.

The **undo anti-replay window** command restores the default anti-replay window size of an IPSec tunnel.

By default, the anti-replay window size of a single IPSec tunnel is not set. The global value is used.

Format

anti-replay window *window-size*

undo anti-replay window

Parameters

Parameter	Description	Value
window-size	Specifies the anti-replay window size of an IPSec tunnel.	The value can be 32, 64, 128, 256, 512, or 1024, in bits.

Views

Efficient VPN policy view

Default Level

2: Configuration level

Usage Guidelines

Configuration Impact

You may need to change the anti-replay window size for an IPSec tunnel in some situations. For example, if QoS is performed for packets passing an IPSec tunnel, sequence numbers of service data packets may be different from those in common data packets. As a result, these service data packets are dropped as replay attack packets. To prevent such packets from being dropped incorrectly, you can disable the anti-replay function or increase the anti-replay window size for the IPSec tunnel.

Prerequisites

The anti-replay function is enabled for the IPSec tunnel. By default, the anti-replay function is enabled (through the **ipsec anti-reply enable** command).

Precautions

When both **anti-replay window** and **ipsec anti-replay window** are configured, the **anti-replay window** configuration takes effect. When **anti-replay window** is not configured, the **ipsec anti-replay window** configuration takes effect.

Example

# Set the IPSec anti-replay window size to 128 bits.

```
<HUAWEI> system-view
[HUAWEI] ipsec efficient-vpn evpn mode client
[HUAWEI-ipsec-efficient-vpn-evpn] anti-replay window 128
```

10.3.3 dh

Function

The **dh** command specifies a Diffie-Hellman (DH) group used for IKE negotiation.

The **undo dh** command restores the default DH group for IKE negotiation.

By default, group14 is used for IKE negotiation.

Format

dh { **group14** | **group19** | **group20** | **group21** }

undo dh

Parameters

Parameter	Description	Value
group14	Uses the 2048-bit DH group in IKE negotiation phase 1.	-
group19	Uses the 256-bit Elliptic Curve Groups modulo a Prime (ECP) DH group in IKE negotiation phase 1.	-
group20	Uses the 384-bit Elliptic Curve Groups modulo a Prime (ECP) DH group in IKE negotiation phase 1.	-

Parameter	Description	Value
group21	Uses the 521-bit Elliptic Curve Groups modulo a Prime (ECP) DH group in IKE negotiation phase 1.	-

Views

Efficient VPN policy view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The DH algorithm is a public key algorithm. Two communicating parties calculate a shared key based on data exchanged between them, without transmitting the key. A third party (such as a hacker) cannot calculate the actual key even if it obtains all exchanged data for key calculation.

Precautions

- Both ends of an IPSec tunnel must be configured with the same DH group. Otherwise, the negotiation fails.
- The security level order of the DH groups is: **group21** > **group20** > **group19** > **group14**.
- The system software does not support the **group1**, **group2**, and **group5** parameters. To use these DH groups, you need to install the WEAKEA plug-in. For higher security purposes, you are advised to specify other DH groups.

  For details about how to install the WEAKEA plug-in, see "WEAKEA Configuration" in the *CLI-based Configuration Guide*.

Example

# Specify the 2048-bit DH group for the IPSec Efficient VPN policy.

```
<HUAWEI> system-view
[HUAWEI] ipsec efficient-vpn evpn mode client
[HUAWEI-ipsec-efficient-vpn-evpn] dh group14
```

10.3.4 display ike error-info

Function

The **display ike error-info** command displays information about IPSec tunnel negotiation failures using IKE.

Format

display ike error-info [**verbose**] [**peer** *remote-address*]

Parameters

Parameter	Description	Value
verbose	Displays details about IPSec tunnel negotiation failures using IKE.	-
peer *remote-address*	Displays information about IPSec tunnel negotiation failures using IKE with a specified remote IP address.	The value is in dotted decimal notation.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The command output contains information of the latest 200 IPSec tunnel negotiation failures using IKE.

Example

# Display information about IPSec tunnel negotiation failures using IKE.

```
<HUAWEI> display ike error-info

  current info Num :2
  Ike error information:
  current ike Error-info number :2
  ---------------------------------------------------------------------------
  peer       port      error-reason               version     error-time
  ---------------------------------------------------------------------------
  10.1.1.1   500       phase1 proposal mismatch     v1         2013-08-26 13:42:37
  10.1.1.1   500       phase1 proposal mismatch     v1         2013-08-26 13:08:45
  ---------------------------------------------------------------------------
```

# Display details about IPSec tunnel negotiation failures using IKE.

```
<HUAWEI> display ike error-info verbose

  current info Num :1
  Ike error information:
  current ike Error-info number :1
-------------------------------------------------------------------------
Peer       : 10.1.1.1
Port       : 500
version    : v1
Reason     : phase1 proposal mismatch
Detail     : phase1 proposal mismatch
Error-time : 2013-08-26 12:02:37
-------------------------------------------------------------------------
```

Table 10-9 Description of the **display ike error-info** command output

Item	Description
current info Num	Current information number.
Ike error information	Information about IPSec tunnel negotiation failures using IKE.
current ike Error-info number	Number of IPSec tunnel negotiation failures using IKE.
peer or Peer	Peer IP address.
port or Port	Peer UDP port number.

Item	Description
error-reason or Reason	Causes for IPSec tunnel negotiation failures using IKE: ● phase1 proposal mismatch: IKE proposal parameters of the two ends do not match. ● phase2 proposal or pfs mismatch: IPSec proposal parameters, pfs algorithm, or security ACL of the two ends do not match. ● responder dh mismatch: The DH algorithm of the responder does not match. ● initiator dh mismatch: The DH algorithm of the initiator does not match. ● encapsulation mode mismatch: The encapsulation mode does not match. ● flow or peer mismatch: The security ACL or IKE peer address of the two ends does not match. ● version mismatch: The IKE version number of the two ends does not match. ● peer address mismatch: The IKE peer address of the two ends does not match. ● config ID mismatch: The IKE peer of the specified ID is not found. ● exchange mode mismatch: The negotiation mode of the two ends does not match. ● authentication fail: Identity authentication fails. ● construct local ID fail: The local ID fails to be constructed. ● rekey no find old sa: The old SA is not found during re-negotiation. ● rekey fail: The old SA is going offline during re-negotiation. ● first packet limited: The rate of the first packet is limited. ● unsupported version: The IKE version number is not supported. ● malformed message: Malformed message. ● malformed payload: Malformed payload. ● critical drop: Unidentified critical payload. ● cookie mismatch: Cookie mismatch. ● invalid cookie: Invalid cookie. ● invalid length: Invalid packet length. ● unknown exchange type: Unknown negotiation mode. ● uncritical drop: Unidentified non-critical payload. ● local address mismatch: The local IP address in IKE negotiation and interface IP address do not match.

Item	Description
	● dynamic peers number reaches limitation: The number of IKE peers reaches the upper limit. ● ipsec tunnel number reaches limitation: The number of IPSec tunnels reaches the upper limit. ● no policy applied on interface: No policy is applied to an interface. ● nat detection fail: NAT detailed failed. ● fragment packet limit: Fragment packets exceed the limit. ● fragment packet reassemble timeout: Fragment packet reassembly times out. ● max transmit reached: Tunnel negotiation fails after the number of IKE packet retransmissions reaches the maximum value. ● no valid local cert: No valid CA/local certificate exists.
version	IKE version.
Error-time/error-time	Time of IPSec tunnel negotiation failures using IKE.

Item	Description
Detail	Details about IPSec tunnel negotiation failures using IKE. ● phase1 proposal mismatch: IKE proposal parameters of the two ends do not match. ● phase2 proposal or pfs mismatch: IPSec proposal parameters, pfs algorithm, or security ACL of the two ends do not match. ● responder dh mismatch: The DH algorithm of the responder does not match. ● initiator dh mismatch: The DH algorithm of the initiator does not match. ● encapsulation mode mismatch: The encapsulation mode does not match. ● flow or peer mismatch: The security ACL or IKE peer address of the two ends does not match. ● version mismatch: The IKE version number of the two ends does not match. ● peer address mismatch: The IKE peer address of the two ends does not match. ● config ID mismatch: The IKE peer of the specified ID is not found. ● exchange mode mismatch: The negotiation mode of the two ends does not match. ● authentication fail: Identity authentication fails. ● construct local ID fail: The local ID fails to be constructed. ● rekey no find old sa: The old SA is not found during re-negotiation. ● rekey fail: The old SA is going offline during re-negotiation. ● first packet limited: The rate of the first packet is limited. ● unsupported version: The IKE version number is not supported. ● malformed message: Malformed message. ● malformed payload: Malformed payload. ● critical drop: Unidentified critical payload. ● cookie mismatch: Cookie mismatch. ● invalid cookie: Invalid cookie. ● invalid length: Invalid packet length. ● unknown exchange type: Unknown negotiation mode. ● uncritical drop: Unidentified non-critical payload. ● local address mismatch: The local IP address in IKE negotiation and interface IP address do not match.

Item	Description
	● dynamic peers number reaches limitation: The number of IKE peers reaches the upper limit. ● ipsec tunnel number reaches limitation: The number of IPSec tunnels reaches the upper limit. ● no policy applied on interface: No policy is applied to an interface. ● nat detection fail: NAT detailed failed. ● fragment packet limit: Fragment packets exceed the limit. ● fragment packet reassemble timeout: Fragment packet reassembly times out. ● max transmit reached: Tunnel negotiation fails after the number of IKE packet retransmissions reaches the maximum value. ● no valid local cert: No valid CA/local certificate exists. ● receive phase1 proposal mismatch: The received IKE proposal parameters do not match the local parameters. ● receive phase2 proposal mismatch: The received IPSec proposal parameters do not match the local parameters. ● phase2 proposal mismatch: IPSec proposal parameters on both ends do not match. ● receive flow or peer mismatch: The received security ACL or IKE peer address does not match the local one. ● (peer local or tunnel local or interface) address mismatch: The peer's local IP address, local tunnel IP address or interface IP address does not match the local one. ● remote auth method mismatch: The peer authentication method does not match. ● proc auth payload fail(pre-share-key): Failed to process the authentication payload during pre-shared key authentication. ● recv peer auth fail notification: An authentication failure notification from the peer end is received. ● recv peer auth fail notification(pre-share-key): An authentication failure notification from the peer end is received during pre-shared key authentication. ● proc and auth ID payload fail(pre-share-key): The peer ID fails to be authenticated during pre-shared key authentication.

10.3.5 display ike global config

Function

The **display ike global config** command displays global IKE configurations.

Format

display ike global config

Parameters

None.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run this command to view global IKE configurations, such as the local name used in IKE negotiation, interval for sending heartbeat packets, timeout interval of heartbeat packets, and interval for sending NAT keepalive packets.

Example

# Display global IKE configurations.

```
<HUAWEI> display ike global config
IKE Global Config:
----------------------------------------------------------------
  IKE local-name                   : huawei
  IKE heartbeat-timer interval     : 30
  IKE heartbeat-timer timeout      : 100
  IKE nat-keepalive-timer interval : 52   IKEv1 phase1-phase2 sa dependent : enable   IKE
DSCP                         : -   IKEv2 initial-contact            : enable   IKEv2 delete old child-sa        : enable
----------------------------------------------------------------
```

Table 10-10 Description of the **display ike global config** command output

Item	Description
IKE Global Config	Global IKE configurations.
IKE local-name	Local peer name used in IKE negotiation. This parameter can be configured using the **ike local-name** command. If the **ike local-name** command is not run, the device name configured using the **sysname** command is used for IKE negotiation.

Item	Description
IKE heartbeat-timer interval	Interval (in seconds) at which a device sends heartbeat packets through an IKE SA. This parameter is configured using the **ike heartbeat-timer interval** command.
IKE heartbeat-timer timeout	Timeout period (in seconds) of sending heartbeat packets through an IKE SA. This parameter is configured using the **ike heartbeat-timer timeout** command.
IKE nat-keepalive-timer interval	Interval (in seconds) at which a device sends NAT keepalive packets through an IKE SA. This parameter is configured using the **ike nat-keepalive-timer interval** command.
IKEv1 phase1-phase2 sa dependent	Dependency between an IPSec SA and an IKE SA during IKEv1 negotiation is enabled. ● enable ● disable This function is configured using the **ikev1 phase1-phase2 sa dependent** command.
IKE DSCP	Global DSCP value of IKE packets. This parameter can be configured using the **ike dscp** command.
IKEv2 initial-contact	Whether the first IKE_AUTH request message carries the INITIAL_CONTACT notification payload. ● enable ● disable This function is configured using the **ikev2 initial-contact enable** command.
IKEv2 delete old child-sa	Whether to enable the function of instructing the peer device to delete the old child SA: ● enable ● disable This function is configured using the **ikev2 delete old child-sa enable** command.

10.3.6 display ike offline-info

Function

The **display ike offline-info** command displays information about deleted IPSec tunnels established through IKE negotiation.

Format

display ike offline-info [**peer** *remote-address*]

Parameters

Parameter	Description	Value
peer *remote-address*	Displays information about deleted IPSec tunnels with a specified remote IP address and established through IKE negotiation.	The value is in dotted decimal notation.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The command output contains the possible causes and time of the latest 200 IPSec tunnel deletions.

Example

Display information about deleted IPSec tunnels established through IKE negotiation.

```
<HUAWEI> display ike offline-info

  Current info Num :2
  Ike offline information:
---------------------------------------------------------------------------
  peer             offline-reason             version     offline-time
---------------------------------------------------------------------------
  2.1.1.2          dpd timeout                 v2         2017-02-18 02:12:39
  2.1.1.2          dpd timeout                 v2         2017-02-18 01:17:06
---------------------------------------------------------------------------
```

Table 10-11 Description of the **display ike offline-info** command output

Item	Description
Current info Num	Current number of information records.
Ike offline information	Information about IPSec tunnels established through IKE negotiation have been deleted.
peer	Peer IP address of a deleted IPSec tunnel.

Item	Description
offline-reason	Causes for deletion of IPSec tunnels established through IKE negotiation: ● dpd timeout: Dead peer detection (DPD) times out. ● peer request: The remote end has sent a message, asking the local end to tear down the tunnel. ● config modify or manual offline: An SA is deleted due to configuration modification or an SA is manually deleted. ● phase1 hard expiry: Hard lifetime expires in phase 1 (no new SA negotiation success message is received). ● phase2 hard expiry: Hard lifetime expires in phase 2. ● heartbeat timeout: heartbeat detection times out. ● modecfg address soft expiry: The IP address lease applied by the remote end from the server expires. ● re-auth timeout: An SA is deleted due to reauthentication timeout. ● aaa cut user: The AAA module disconnects users. ● hard expiry triggered by port mismatch: A hard timeout occurs due to mismatch NAT port number. ● spi conflict: An SPI conflict occurs. ● phase1 sa replace: The new IKE SA replaces the old IKE SA. ● phase2 sa replace: The new IPSec SA replaces the old IPsec SA. ● receive invalid spi notify: The device receives an invalid SPI notification. ● dns resolution status change: DNS resolution status changes. ● ikev1 phase1-phase2 sa dependent offline: The device deletes the associated IPSec SA when deleting an IKEv1 SA. ● exchange timeout: Packet interaction timeout.
version	IKE version.
offline-time	IPSec tunnel deletion time.

10.3.7 display ike sa

Function

The **display ike sa** command displays information about SAs established through IKE negotiation.

Format

display ike sa [**remote** *ipv4-address*]

display ike sa [**remote-id-type** *remote-id-type*] **remote-id** *remote-id*

display ike sa verbose [**remote** *ipv4-address* | **connection-id** *connection-id* | [**remote-id-type** *remote-id-type*] **remote-id** *remote-id*]

Parameters

Parameter	Description	Value
remote *ipv4-address*	Specifies the IPv4 address of the remote peer.	The value is in dotted decimal notation.
remote-id-type *remote-id-type*	Specifies a remote ID type.	The remote ID type can be ip, key-id, fqdn, or user-fqdn.
remote-id *remote-id*	Specifies the remote ID.	The remote ID must be an existing one.
verbose	Displays detailed information about SAs. **NOTE** If only this parameter is specified (other parameters are not specified), the command displays detailed information about all SAs.	-
connection-id *connection-id*	Specifies the connection ID of an SA.	The value is an integer that ranges from 1 to 4294967295.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display ike sa** command to check the following SA information: connection ID, peer IP address, VPN instance name, SA phase, remote ID type, remote ID, and SA status.

NOTE

After an IPSec tunnel is established successfully, the **display ike sa** command does not display the latest local ID or remote ID until the IPSec tunnel is re-negotiated if the local ID or remote ID is modified.

Example

# Display IKE SAs and IPSec SAs.

```
<HUAWEI> display ike sa
IKE SA information :
    Conn-ID       Peer           VPN   Flag(s)   Phase   RemoteType  RemoteID
  -------------------------------------------------------------------------------
    117477244     10.100.1.1/4500 vrf1  RD|M      v2:2    IP         10.100.1.1
    117477242     10.100.1.1/4500 vrf1  RD|M      v2:1    IP         10.100.1.1

   Number of IKE SA : 2
  -------------------------------------------------------------------------------

  Flag Description:
  RD--READY   ST--STAYALIVE   RL--REPLACED   FD--FADING   TO--TIMEOUT
  HRT--HEARTBEAT   LKG--LAST KNOWN GOOD SEQ NO.   BCK--BACKED UP
  M--ACTIVE   S--STANDBY   A--ALONE  NEG--NEGOTIATING
```

Table 10-12 Description of the **display ike sa** command output

Item	Description
IKE SA information	Configuration of SAs.
Conn-ID	Connection ID of an SA.
Peer	IP address and UDP port number of the peer.
VPN	VPN instance bound to the interface where the IPSec policy was applied to.

Item	Description
Flag(s)	SA status: ● RD--READY: The SA has been established successfully. ● ST--STAYALIVE: This end is the initiator of tunnel negotiation. ● RL--REPLACED: This SA has been replaced by a new one and will be deleted after a period of time. ● FD--FADING: A soft timeout has occurred, but the SA is still in use. The SA will be deleted when the hard lifetime expires. ● TO--TIMEOUT: This SA has not received any heartbeat packet after the last heartbeat timeout. The SA will be deleted if it still does not receive any heartbeat packet till the next heartbeat timeout. ● HRT--HEARTBEAT: The local IKE SA sends heartbeat packets. ● LKG--LAST KNOWN GOOD SEQ NO: It is the last known sequence number. ● BCK--BACKED UP: The SA is backed up. ● M--ACTIVE: The IPSec policy group is in active state. ● S--STANDBY: The IPSec policy group is in standby state. ● A--ALONE: The IPSec policy group is not backed up. ● NEG--NEGOTIATING: The devices are negotiating an SA. ● Empty: IKE SA negotiation is being performed because the settings at the two ends of the tunnel are inconsistent.
Phase	Phases of the SA: ● v1:1 or v2:1: v1 and v2 are IKE versions. The digit 1 indicates the phase during which a security channel, that is IKE SA, is established. ● v1:2 or v2:2: v1 and v2 are IKE versions. The digit 2 indicates the phase during which a security service, that is IPSec SA, is negotiated.
RemoteType	Remote ID type.
RemoteID	Remote ID.

# Display detailed information about established IKE SAs and IPSec SAs when the peers use IKEv1 to negotiate IPSec SAs.

```
<HUAWEI> display ike sa verbose remote 10.100.1.1
-----------------------------------------------
Ike Sa phase   : 2
Establish Time : 2017-02-08 13:10:29
```

```
PortCfg Index  : 0x448
IKE Peer Name  : _resv_ikev1__1
Connection Id  : 26
Version        : v1
Flow VPN       :
Peer VPN       :
-----------------------------------------------
Initiator Cookie        : 0x33d7a5bbf8ad12bb
Responder Cookie        : 0xf311b3991d739d38
Local Address           : 10.1.1.1/500
Remote Address          : 10.100.1.1/500
PFS                     :
Flags                   : RD|ST|A
-----------------------------------------------

-----------------------------------------------
Ike Sa phase   : 1
Establish Time : 2017-02-07 20:57:48
PortCfg Index  : 0x448
IKE Peer Name  : _resv_ikev1__1
Connection Id  : 7
Version        : v1
Exchange Mode  : Aggressive
Flow VPN       :
Peer VPN       :
-----------------------------------------------
Initiator Cookie              : 0x33d7a5bbf8ad12bb
Responder Cookie              : 0xf311b3991d739d38
Local Address                 : 10.1.1.1/500
Remote Address                : 10.100.1.1/500
Encryption Algorithm          : 3DES-CBC
Authentication Algorithm      : SHA1
Authentication Method         : Pre-Shared key
DPD Capability                : Yes
DPD Enable                    : Yes
DPD Message Learning Enable   : Yes
DPD Message Format            : Seq-Notify-Hash
Reference Counter             : 0
Flags                         : RD|ST|A
Local Id Type                 : IP
local Id                      : 10.1.1.1
Remote Id Type                : IP
Remote Id                     : 10.1.1.2
DH Group                      : 2
NAT Traversal Version         : RFC3947
SA Remaining Soft Timeout (sec):100 SA Remaining Hard Timeout (sec):200
-----------------------------------------------

  Number of IKE SA : 2
-----------------------------------------------

  Flag Description:
  RD--READY   ST--STAYALIVE   RL--REPLACED   FD--FADING   TO--TIMEOUT
  HRT--HEARTBEAT   LKG--LAST KNOWN GOOD SEQ NO.   BCK--BACKED UP
  M--ACTIVE   S--STANDBY   A--ALONE  NEG--NEGOTIATING
```

# Display detailed information about established IKE SAs and IPSec SAs when the peers use IKEv2 to negotiate IPSec SAs.

```
<HUAWEI> display ike sa verbose remote 10.100.1.1
-----------------------------------------------
Ike Sa phase   : 2
Establish Time : 2017-02-20 22:07:57
PortCfg Index  : 0x98
IKE Peer Name  : _resv_ikev2__1
Connection Id  : 4
Version        : v2
Flow VPN       :
Peer VPN       :
-----------------------------------------------
```

```
Initiator Cookie        : 0x039b87ea4e1e91b2
Responder Cookie        : 0xdedd86121d2038d7
Local Address           : 10.1.1.1/500
Remote Address          : 10.100.1.1/4500
PFS                     :
Flags                   : RD|ST|A
------------------------------------------------

------------------------------------------------
Ike Sa phase   : 1
Establish Time : 2017-02-20 22:07:57
PortCfg Index  : 0x98
IKE Peer Name  : _resv_ikev2__1
Connection Id  : 3
Version        : v2
Flow VPN       :
Peer VPN       :
------------------------------------------------
Initiator Cookie                      : 0x039b87ea4e1e91b2
Responder Cookie                      : 0xdedd86121d2038d7
Local Address                         : 10.1.1.1/500
Remote Address                        : 10.100.1.1/4500
Encryption Algorithm                  : 3DES-CBC
Authentication Method                 : Pre-Shared key
Integrity Algorithm                   : hmac-sha1-96
Prf Algorithm                         : hmac-sha1
DPD Capability                        : Yes
DPD Enable                            : Yes
Reference Counter                     : 1
Flags                                 : RD|ST|A
Local Id Type                         : IP
Local Id                              : huawei1Remote Id Type                         : IP
Remote Id                             : huawei
DH Group                              : 14
Re-authentication remaining time (sec) : -
SA Remaining Soft Timeout (sec)        :100
SA Remaining Hard Timeout (sec)        :200
------------------------------------------------

  Number of IKE SA : 2
------------------------------------------------

  Flag Description:
  RD--READY   ST--STAYALIVE   RL--REPLACED   FD--FADING   TO--TIMEOUT
  HRT--HEARTBEAT   LKG--LAST KNOWN GOOD SEQ NO.   BCK--BACKED UP
  M--ACTIVE   S--STANDBY   A--ALONE  NEG--NEGOTIATING
```

Table 10-13 Description of the **display ike sa verbose** command output

Item	Description
Ike Sa phase	Phases of the SA: ● 1: IKE peers establish an IPSec tunnel. An IKE SA is established in this phase. ● 2: IKE peers negotiate security services. An IPSec SA is established in this phase.
Establish Time	Time when the SA was created.
PortCfg Index	Index of the interface where the IPSec policy was applied to.
IKE Peer Name	IKE peer name.

Item	Description
Connection Id	Connection ID of an SA.
Version	IKE version of the IKE peer: ● v1: IKEv1 is enabled. ● v2: IKEv2 is enabled. ● v1v2: Both IKEv1 and IKEv2 are enabled.
Exchange Mode	Negotiation mode of the IKEv1 phase 1. ● Main: main mode. ● Aggressive: aggressive mode.
Flow VPN	VPN to which the data flow belongs.
Peer VPN	VPN to which the peer belongs.
Initiator Cookie	Cookie of the initiator.
Responder Cookie	Cookie of the responder.
Local Address	Local IP address of an IPSec tunnel.
Remote Address	Remote IP address and UDP port number of an IPSec tunnel.
Encryption Algorithm	Encryption algorithm in the IKE proposal.
Authentication Algorithm	Authentication algorithm in the IKE proposal.
Authentication Method	Authentication method in the IKE proposal.
Integrity Algorithm	Integrity algorithm used in an IKEv2 proposal.
Prf Algorithm	Pseudo-random function (PRF) used in an IKEv2 proposal.
DPD Capability	Whether DPD capability is successfully negotiated. ● yes ● no
DPD Enable	Whether the DPD function is enabled. ● yes ● no
DPD Message Learning Enable	Whether automatic learning of the payload sequence of DPD packets is enabled. ● Yes ● No To configure the automatic learning function, run the **dpd msg notify-hash-sequence learning** command.

Item	Description
DPD Message Format	Sequence of the payload in DPD packets. ● Seq-Notify-Hash ● Seq-Hash-Notify
Reference Counter	Number of IPSec SAs negotiated by the IKE SA.
PFS	Perfect Forward Secrecy (PFS) when the local end initiates negotiation.
Flags	SA status: ● RD--READY: The SA has been established successfully. ● ST--STAYALIVE: This end is the initiator of tunnel negotiation. ● RL--REPLACED: This SA has been replaced by a new one and will be deleted after a period of time. ● FD--FADING: A soft timeout has occurred, but the SA is still in use. The SA will be deleted when the hard lifetime expires. ● TO--TIMEOUT: This SA has not received any heartbeat packet after the last heartbeat timeout. The SA will be deleted if it still does not receive any heartbeat packet till the next heartbeat timeout. ● HRT--HEARTBEAT: The local IKE SA sends heartbeat packets. ● LKG--LAST KNOWN GOOD SEQ NO: It is the last known sequence number. ● BCK--BACKED UP: The SA is backed up. ● M--ACTIVE: The IPSec policy group is in active state. ● S--STANDBY: The IPSec policy group is in standby state. ● A--ALONE: The IPSec policy group is not backed up. ● NEG--NEGOTIATING: The devices are negotiating an SA. ● Empty: IKE SA negotiation is being performed because the settings at the two ends of the tunnel are inconsistent.
Local Id Type	Local ID type.
Local Id	Local ID for IKE negotiation.
Remote Id Type	Remote ID type.
Remote Id	Remote ID for IKE negotiation.
DH Group	DH group in the IKE proposal.

Item	Description
NAT Traversal Version	Version of NAT traversal. ● draft-ietf-ipsec-nat-t-ike-00 ● draft-ietf-ipsec-nat-t-ike-02 ● RFC3947
Re-authentication remaining time (sec)	Remaining time for IKEv2 to initiate re-authentication, in seconds.
SA Remaining Soft Timeout (sec)	Soft remaining lifetime of an IKE SA, in seconds.
SA Remaining Hard Timeout (sec)	Hard remaining lifetime of an IKE SA, in seconds.
Number of IKE SA	Total number of IKE SAs and IPSec SAs.

10.3.8 display ike statistics

Function

The **display ike statistics** command displays IKE statistics.

Format

display ike statistics { **v1** | **v2** }

Parameters

Parameter	Description	Value
v1	Displays IKEv1 statistics.	-
v2	Displays IKEv2 statistics.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

When a fault occurs on the IPSec tunnel that is established through IKE negotiation, you can check statistics about IKE peers, IKE SAs, and DPD packets to diagnose and locate the fault.

Example

# Display IKEv1 statistics.

```
<HUAWEI> display ike statistics v1
--------------------------------------------------------------------------------
 IKE V1 statistics information

 Number of total peers                      : 7
 Maximum of total peers in history          : 0
 Begin time of total peers                  : 2015-04-08 21:23:10
 Maximum time of total peers                : 2015-04-08 21:23:10
 Number of proposals                        : 4
 Number of established V1 phase 1 SAs       : 0
 Number of established V1 phase 2 SAs       : 0
 Number of total V1 phase 1 SAs             : 0
 Number of total V1 phase 2 SAs             : 0
 Number of total SAs                        : 0
 Maximum of V1 phase 1 SAs in history       : 0
 Begin time of V1 phase 1 SAs               : 2015-04-08 21:23:10
 Maximum time of V1 phase 1 SAs             : 2015-04-08 21:23:10
 Maximum of V1 phase 2 SAs in history       : 0
 Begin time of V1 phase 2 SAs               : 2015-04-08 21:23:10
 Maximum time of V1 phase 2 SAs             : 2015-04-08 21:23:10
 Maximum of total SAs in history            : 0
 Begin time of total SAs                    : 2015-04-08 21:23:10
 Maximum time of total SAs                  : 2015-04-08 21:23:10
 Number of messages in V1 fast queue        : 0
 Number of messages in V1 slow queue        : 0
 Number of DPD request sent                 : 0
 Number of DPD ack received                 : 0
 Number of DPD request received             : 0
 Number of DPD ack sent                     : 0
 Number of DPD request receive dropped      : 0
 Number of DPD ack receive dropped          : 0
--------------------------------------------------------------------------------
```

# Display IKEv2 statistics.

```
<HUAWEI> display ike statistics v2
--------------------------------------------------------------------------------
 IKE V2 statistics information

 Number of total peers                      : 0
 Maximum of total peers in history          : 0
 Begin time of total peers                  : 2015-04-08 21:23:10
 Maximum time of total peers                : 2015-04-08 21:23:10
 Number of proposals                        : 4
 Number of established V2 phase 1 SAs       : 0
 Number of established V2 phase 2 SAs       : 0
 Number of total V2 phase 1 SAs             : 0
 Number of total V2 phase 2 SAs             : 0
 Number of total SAs                        : 0
 Maximum of V2 phase 1 SAs in history       : 0
 Begin time of V2 phase 1 SAs               : 2015-04-08 21:23:10
 Maximum time of V2 phase 1 SAs             : 2015-04-08 21:23:10
 Maximum of V2 phase 2 SAs in history       : 0
 Begin time of V2 phase 2 SAs               : 2015-04-08 21:23:10
 Maximum time of V2 phase 2 SAs             : 2015-04-08 21:23:10
 Maximum of total SAs in history            : 0
 Begin time of total SAs                    : 2015-04-08 21:23:10
```

```
Maximum time of total SAs                    : 2015-04-08 21:23:10
Number of messages in V2 fast queue          : 0
Number of messages in V2 slow queue          : 0
Number of DPD request sent                   : 0
Number of DPD ack received                   : 0
Number of DPD request received               : 0
Number of DPD ack sent                       : 0
Number of DPD request receive dropped        : 0
Number of DPD ack receive dropped            : 0
--------------------------------------------------------------------------------
```

Table 10-14 Description of the **display ike statistics** command output

Item	Description
IKE V1 statistics information	IKEv1 statistics.
IKE V2 statistics information	IKEv2 statistics.
Number of total peers	Total number of peers.
Maximum of total peers in history	Historical maximum number of IKE peers.
Begin time of total peers	Time when the system started to count the number of IKE peers.
Maximum time of total peers	Time when the total number of IKE peers reached the maximum value.
Number of proposals	Number of IKE proposals.
Number of established V1/V2 phase 1 SAs	Total number of IKE SAs that have been established successfully.
Number of established V1/V2 phase 2 SAs	Total number of IPSec SAs that have been established successfully.
Number of total V1/V2 phase 1 SAs	Total number of IKE SAs.
Number of total V1/V2 phase 2 SAs	Total number of IPSec SAs.
Number of total SAs	Total number of SAs.
Maximum of V1/V2 phase 1 SAs in history	Maximum number of IKE SAs in the history.
Begin time of V1/V2 phase 1 SAs	Time when the system started to count the number of IKE SAs.

Item	Description
Maximum time of V1/V2 phase 1 SAs	Time when the total number of IKE SAs reaches the maximum value.
Maximum of V1/V2 phase 2 SAs in history	Maximum number of IPSec SAs in the history.
Begin time of V1/V2 phase 2 SAs	Time when the system started to count the number of IPSec SAs.
Maximum time of V1/V2 phase 2 SAs	Time when the total number of IPSec SAs reached the maximum value.
Maximum of total SAs in history	Maximum number of total SAs in the history.
Begin time of total SAs	Time when the system started to count the total number of SAs.
Maximum time of total SAs	Time when the total number of SAs reached the maximum value.
Number of messages in V1/V2 fast queue	Number of IKE messages in high-priority queues.
Number of messages in V1/V2 slow queue	Number of IKE messages in low-priority queues.
Number of DPD request sent	Number of DPD request packets sent from the local end.
Number of DPD ack received	Number of DPD ack packets received by the local end.
Number of DPD request received	Number of DPD request packets received by the local end.
Number of DPD ack sent	Number of DPD ack packets sent from the local end.
Number of DPD request receive dropped	Number of received DPD request packets that are dropped.
Number of DPD ack receive dropped	Number of received DPD response packets that are dropped.

10.3.9 display ikev2 statistics

Function

The **display ikev2 statistics** command displays statistics on IPSec tunnels negotiated using IKEv2.

Format

display ikev2 statistics { **error** | **notify-info** | **packet** | **sa** }

Parameters

Parameter	Description	Value
error	Displays error statistics on IPSec tunnels negotiated using IKEv2.	-
notify-info	Displays notification message statistics on IPSec tunnels negotiated using IKEv2.	-
packet	Displays packet statistics on IPSec tunnels negotiated using IKEv2.	-
sa	Displays SA statistics on IPSec tunnels negotiated using IKEv2.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run this command to view error, packet, SA, and notification message statistics on IPSec tunnels negotiated using IKEv2.

Example

# Display error statistics on IPSec tunnels negotiated using IKEv2.

```
<HUAWEI> display ikev2 statistics error

Error statistics:
--------------------------------------------------------------------------------
```

```
Config error:
Version error          :0
Peer address can not match with any ike peer config              :0
Phase1 proposal mismatch :0          Phase2 proposal or pfs mismatch:0
Responder dh mismatch    :0          Initiator dh mismatch          :0
Flow mismatch           :1
ID can not match with any ike peer config                         :0
Construct local id fail                                          :0
Authentication fail (may be pre-shared-key error)                 :0
Peer's flow netmask range is too wide                            :0
-------------------------------------------------------------------------------
Packet or payload error:
Invalid length          :0
Message-id unordered    :0
Unknown exchange type   :0
Invalid cookie          :6
Shortpacket             :0
Malformed message       :4
Malformed payload       :0
Rekey, not find old child:0          Rekey, old child close         :14
Exchange-type or role(initiator or responder) mismatch             :0
Unexpected critical payload, drop                                 :0
Unexpected uncritical payload, ignore                             :0
-------------------------------------------------------------------------------
Maybe ddos attack:
Responder request IKEV2_COOKIE                                    :0
Responder receive invalid cookie for IKEV2_COOKIE request         :0
Responder receive no cookie for IKEV2_COOKIE request              :0
-------------------------------------------------------------------------------
System abnormal:
Fail decrypt            :0          Fail encrypt                  :0
Fail integrity check    :0
No memory, fail send packet                                       :0
No memory, fail process packet                                    :0
-------------------------------------------------------------------------------
System limited:
First packet speed limited :0            License limited         :0
-------------------------------------------------------------------------------
```

Table 10-15 Description of the **display ikev2 statistics error** command output

Item	Description
Error statistics	Error statistics.
Config error	Configurations are incorrect.
Version error	The IKE version does not match.
Peer address can not match with any ike peer config	The corresponding IKE peer is not found based on the peer address.
Phase1 proposal mismatch	The phase 1 IPSec proposal does not match.
Phase2 proposal or pfs mismatch	The phase 2 IPSec proposal or PFS does not match.

Item	Description
Responder dh mismatch	DH group match on the responder failed. (If a matching DH group is available in the algorithm list of the initiator, the responder will send an information message to the initiator to instruct the initiator to start negotiation using the matching DH group. If the initiator accepts the information message, the negotiation succeeds.)
Initiator dh mismatch	DH group match on the initiator failed. (The initiator failed to process the message requesting a matching DH group.)
Flow mismatch	The data flow does not match.
ID can not match with any ike peer config	The peer ID does not match that configured in the IKE peer.
Construct local id fail	Local ID construction failed.
Authentication fail (may be pre-shared-key error)	Authentication failed. The possible cause is that the pre-shared key does not match.
Peer's flow netmask range is too wide	The mask length of the peer flow is too large.
Packet or payload error	Incorrect packet or payload.
Invalid length	Invalid length.
Message-id unordered	Message ID out of order.
Unknown exchange type	Unknown exchange type.
Invalid cookie	Invalid cookie: ● The corresponding SA does not exist in the received IKEv2 message that does not trigger negotiation. ● The cookie in the IKEv2 message that triggers negotiation is 0.
Shortpacket	The packet is too short.
Malformed message	Invalid message.
Malformed payload	Invalid payload.
Rekey, not find old child	The old IPSec SA is not found for re-negotiation.
Rekey, old child close	The old IPSec SA is offline for re-negotiation.

Item	Description
Exchange-type or role(initiator or responder) mismatch	The exchange type or role (initiator or responder) does not match.
Unexpected critical payload, drop	The unidentified key payload is dropped.
Unexpected uncritical payload, ignore	The unidentified key payload is ignored.
Maybe ddos attack	Maybe DDoS attacks occur.
Responder request IKEV2_COOKIE	The device requests a cookie when the SA in negotiation status exceeds the threshold.
Responder receive invalid cookie for IKEV2_COOKIE request	The received cookie is invalid.
Responder receive no cookie for IKEV2_COOKIE request	No cookie is received.
System abnormal	The system is abnormal.
Fail decrypt	Decryption failed.
Fail encrypt	Encryption failed.
Fail integrity check	Integrity check failed.
No memory, fail send packet	Packet sending failed due to insufficient memory.
No memory, fail process packet	Packet parsing failed due to insufficient memory.
System limited	System restriction.
First packet speed limited	The rate of the first packet is limited.
License limited	License restriction.

# Display notification message statistics on IPSec tunnels negotiated using IKEv2.

```
<HUAWEI> display ikev2 statistics notify-info

Ikev2 notification statistics:
------------------------------------------------------------------------------
Notification:
INVALID_IKE_SPI notification                send:0          receive:0
```

```
INVALID_MAJOR_VERSION notification          send:0          receive:0
INVALID_SYNTAX notification                 send:0          receive:0
INVALID_IPSEC_SPI notification              send:0          receive:0
INVALID_KE_PAYLOAD notification             send:0          receive:0
SINGLE_PAIR_REQUIRED notification           send:0          receive:0
NO_ADDITIONAL_SA notification               send:0          receive:0
TS_UNACCEPTABLE notification                send:0          receive:0
INVALID_IPSEC_SELECTORS notification        send:0          receive:0
INITIAL_CONTACT payload                     send:0          receive:0
SET_WINDOW_SIZE payload                     send:0          receive:0
NAT_DETECTION_SOURCE_IP payload             send:0          receive:0
NAT_DETECTION_DESTINATION_IP payload        send:0          receive:0
USE_TRANSPORT_MODE notification             send:0          receive:0
REKEY_SA notification                       send:0          receive:0
ESP_TFC_PADDING_NOT_SUPPORTED payload       send:0          receive:0
AUTH_LIFETIME payload                       send:0          receive:0
REDIRECT payload                            send:0          receive:0
DELETE_OLD_CHILDSA notification             send:0          receive:0
DSCP payload                                send:0          receive:0
IKEV2_FRAGMENTATION_SUPPORTED payload       send:0          receive:0
------------------------------------------------------------------------------
```

Table 10-16 Description of the **display ikev2 statistics notify-info** command output

Item	Description
Ikev2 notification statistics	IKEv2 notification message statistics.
Notification	IKEv2 notification message.
INVALID_IKE_SPI notification	Invalid IKE SPI notification message.
INVALID_MAJOR_VERSION notification	Invalid Major version number notification message.
INVALID_SYNTAX notification	Invalid syntax notification message.
INVALID_IPSEC_SPI notification	Invalid IPSec SPI notification message.
INVALID_KE_PAYLOAD notification	Incorrect KE payload.
SINGLE_PAIR_REQUIRED notification	Single_Pair_Required notification message.
NO_ADDITIONAL_SA notification	No additional SA notification message.
TS_UNACCEPTABLE notification	Invalid TS payload.
INVALID_IPSEC_SELECTORS notification	Invalid IPSec Selectors notification message.
INITIAL_CONTACT payload	Initial_Contact notification message.

Item	Description
SET_WINDOW_SIZE payload	Set_Window_Size notification message.
NAT_DETECTION_SOURCE_IP payload	NAT source IP notification message.
NAT_DETECTION_DESTINATION_IP payload	NAT destination IP notification message.
USE_TRANSPORT_MODE notification	Transport mode notification message.
REKEY_SA notification	SA re-negotiation notification message.
ESP_TFC_PADDING_NOT_SUPPORTED payload	ESP_TFC_Padding_Not_Supported notification message.
AUTH_LIFETIME payload	Auth_Lifetime notification message.
REDIRECT payload	Redirection notification message.
DELETE_OLD_CHILDSA notification	Delete_Old_ChildSa notification message.
DSCP payload	DSCP notification message.
IKEV2_FRAGMENTATION_SUPPORTED payload	IKEV2_FRAGMENTATION_SUPPORTED notify payload message.
send	Number of sent messages.
receive	Number of received messages.

# Display packet statistics on IPSec tunnels negotiated using IKEv2.

```
<HUAWEI> display ikev2 statistics packet

Packet statistics:
-------------------------------------------------------------------------------
Ike_init request  send   :0           Ike_init request   recv   :0
Ike_init response recv   :0           Ike_init response  send   :0
Ike_auth request  send   :0           Ike_auth request   recv   :0
Ike_auth response recv   :0           Ike_auth response  send   :0
Create_child req  send   :0           Create_child req   recv   :0
Create_child resp recv   :0           Create_child resp  send   :0
Ike_info request  send   :0           Ike_info request   recv   :0
Ike_info response recv   :0           Ike_info response  send   :0
Del_info request  send   :0           Del_info request   recv   :0
Del_info response recv   :0           Del_info response  send   :0
DPD_info request  send   :0           DPD_info request   recv   :0
DPD_info response recv   :0           DPD_info response  send   :0
DPD_info req recv drop   :0           DPD_info resp recv drop   :0
Fragment message  send   :0           Fragment message   recv   :0
Fragment packet   send   :0           Fragment packet    recv   :0

Ike_init request resend  :0
Ike_auth request resend  :0
Create_child req resend  :0
Ike_info request resend  :0
-------------------------------------------------------------------------------
```

Table 10-17 Description of the **display ikev2 statistics packet** command output

Item	Description
Packet statistics	IPSec packet statistics.
Ike_init request send	Number of sent IKE SA initialization exchange (ike_init) request packets.
Ike_init request recv	Number of received ike_init request packets.
Ike_init response recv	Number of received ike_init response packets.
Ike_init response send	Number of sent ike_init response packets.
Ike_auth request send	Number of sent IKE authentication exchange (ike_auth) request packets.
Ike_auth request recv	Number of received ike_auth request packets.
Ike_auth response recv	Number of received ike_auth response packets.
Ike_auth response send	Number of sent ike_auth response packets.
Create_child req send	Number of sent IPSec SA for sub-tunnel creation (create_child) request packets.
Create_child req recv	Number of received create_child request packets.
Create_child resp recv	Number of received create_child response packets.
Create_child resp send	Number of sent create_child response packets.
Ike_info request send	Number of sent IKE notification exchange (ike_info) request packets.
Ike_info request recv	Number of received ike_info request packets.
Ike_info response recv	Number of received ike_info response packets.
Ike_info response send	Number of sent ike_info response packets.

Item	Description
Del_info request send	Number of sent tunnel information deletion (del_info) request packets.
Del_info request recv	Number of received del_info request packets.
Del_info response recv	Number of received del_info response packets.
Del_info response send	Number of sent del_info response packets.
Dpd_info request send	Number of sent DPD information (dpd_info) request packets.
Dpd_info request recv	Number of received dpd_info request packets.
Dpd_info response recv	Number of received dpd_info response packets.
Dpd_info response send	Number of sent dpd_info response packets.
Dpd_info req recv drop	Number of received dpd_info request packets that are dropped.
Dpd_info resp recv drop	Number of received dpd_info response packets that are dropped.
Fragment message send	Number of sent fragment messages.
Fragment message recv	Number of received fragment messages.
Fragment packet send	Number of sent fragment packets.
Fragment packet recv	Number of received fragment packets.
Ike_init request resend	Number of retransmitted ike_init requests.
Ike_auth request resend	Number of retransmitted ike_auth requests.
Create_child req resend	Number of retransmitted create_child requests.
Ike_info request resend	Number of retransmitted ike_info requests.

# Display SA statistics on IPSec tunnels negotiated using IKEv2.

```
<HUAWEI> display ikev2 statistics sa

Sa establish and offline statistic:
------------------------------------------------------------------------------
Establish:
Initiator request phase1 negotiation                         :33
Initiator request phase2 negotiation                         :16
Initiator request and success phase1 negotiation               :10
Initiator request and success phase2 negotiation               :41
Responder response phase1 negotiation                         :0
Responder response phase2 negotiation                         :0
Responder response and success phase1 negotiation               :0
Responder response and success phase2 negotiation               :0
Offline:
Receive delete info      :1          Config modify            :0
Manual reset             :1          Dpd timeout              :0
Phase1 hardware expire   :0          Phase2 hardware expire   :0
Phase1 replace           :0          Phase2 replace           :0
Aaa cut user             :0          Reauth timeout           :0
Flow overlap             :0          IP address syn failed    :0
Port mismatch            :0          Kick old SA              :0
CPU table updated        :0          SPI conflict             :0
EAP delete old sa        :0          Hash gene adjusted       :0
------------------------------------------------------------------------------
```

Table 10-18 Description of the **display ikev2 statistics sa** command output

Item	Description
Sa establish and offline statistic	SA establishment and deletion information.
Establish	Statistics on established IPSec tunnels.
Initiator request phase1 negotiation	Number of times that the initiator requests phase 1 negotiation.
Initiator request phase2 negotiation	Number of times that the initiator requests phase 2 negotiation.
Initiator request and success phase1 negotiation	Number of times that the initiator succeeds in requesting phase 1 negotiation.
Initiator request and success phase2 negotiation	Number of times that the initiator succeeds in requesting phase 2 negotiation.
Responder response phase1 negotiation	Number of times that the responder responds to phase 1 negotiation.
Responder response phase2 negotiation	Number of times that the responder responds to phase 2 negotiation.
Responder response and success phase1 negotiation	Number of times that the responder succeeds in responding to phase 1 negotiation.
Responder response and success phase2 negotiation	Number of times that the responder succeeds in responding to phase 2 negotiation.

Item	Description
Offline	Statistics on deleted IPSec tunnels.
Receive delete info	Number of times that the device receives tunnel deletion messages.
Config modify	Number of times that the tunnel is deleted by modifying the configuration.
Manual reset	Number of times that the tunnel is deleted manually.
Phase1 hardware expire	Number of times that the phase 1 tunnel is deleted due to hard timeout.
Phase2 hardware expire	Number of times that the phase 2 tunnel is deleted due to hard timeout.
Phase1 replace	Number of phase 1 tunnel re-negotiation times.
Phase2 replace	Number of phase 2 tunnel re-negotiation times.
Aaa cut user	Number of tunnel deletion times caused by forced user offline.
Dpd timeout	Number of tunnel deletion times caused by DPD timeout.
Reauth timeout	Number of tunnel deletion times caused by re-authentication timeout.
Flow overlap	Number of tunnel deletion times caused by the conflict between the IP address in the encrypted flow and remote IP address.
IP address syn failed	Number of tunnel deletion times caused by the failure to synchronize IP addresses.
Port mismatch	Number of tunnel deletion times caused by the UDP port mismatch.
Kick old SA	Number of tunnel deletion times caused by a flow conflict.
CPU table updated	Number of tunnel deletion times caused by a CPU table update.
SPI conflict	Number of tunnel deletion times caused by an SPI conflict.
EAP delete old sa	Number of times the device deletes the old SA during EAP authentication.
Hash gene adjusted	Number of tunnel deletion times caused by hash factor adjustment.

10.3.10 display ipsec efficient-vpn

Function

The **display ipsec efficient-vpn** command displays Efficient VPN policy information.

Format

display ipsec efficient-vpn [**brief** | **capability** | **name** *efficient-vpn-name*]

Parameters

Parameter	Description	Value
brief	Displays brief information about Efficient VPN policies.	-
capability	Displays the IPSec configuration supported by an Efficient VPN policy.	-
name *efficient-vpn-name*	Displays information about a specified Efficient VPN policy.	The value is an existing Efficient VPN policy name.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After the Efficient VPN policy is configured, you can run this command to know the configuration information of the Efficient VPN policy, such as the name, interface, authentication method, IKE version, DH algorithm, and PFS algorithm of the Efficient VPN.

Example

# Display brief information about Efficient VPN policies.

```
<HUAWEI> display ipsec efficient-vpn brief
 Total number of IPSec efficient-vpn: 1

 Efficient-vpn name       Efficient-vpn mode
 ------------------------------------------
 v1                     client
```

# Display information about the Efficient VPN policy named **easyvpn_1**.

```
<HUAWEI> display ipsec efficient-vpn name easyvpn_1
===========================================IPSec efficient-vpn name: easyvpn_1
Using interface          : Vlanif27
===========================================
 IPSec Efficient-vpn Mode  : 1 (1:Client 2:Network 3:Network-plus)
 ACL Number                :
 Auth Method               : 8 (8:PSK)
 VPN name                  : wbh
 Local ID Type             : 11 (1:IP 2:Name 3:User-fqdn 11:Key-id)
 IKE Version               : 2 (1:IKEv1 2:IKEv2)
 Remote Address            : 10.10.10.1
 Pre Shared Key Cipher     : ******
 DH Group                  : DH group 14
 PFS Type                  : DH group 14 Remote Name               :
 Re-auth interval          : 400 seconds
 Anti-replay window size   : 0
 Service-scheme name       : ser
 DPD message  type         : seq-notify-hash
 DPD message  learning     : enable
 Interface loopback        : LoopBack0
 Interface loopback IP     : 1.1.1.1/32
```

Table 10-19 Description of the **display ipsec efficient-vpn** command output

Item	Description
Total number of IPSec efficient-vpn	Total number of the Efficient VPN policy.
Efficient-vpn name/IPSec Efficient-vpn Name	Name of the Efficient VPN policy. To configure an Efficient VPN policy, run the **ipsec efficient-vpn (system view)** command.
Using interface	Interface to which an Efficient VPN policy is applied.
Efficient-vpn mode/IPSec Efficient-vpn Mode	Mode used by the Efficient VPN policy. ● 1: client ● 2: network ● 3: network-plus To configure an Efficient VPN policy, run the **ipsec efficient-vpn (system view)** command.
ACL Number	ACL used by the Efficient VPN policy. To configure an ACL referenced by an Efficient VPN policy, run the **security acl** command.
Auth Method	Authentication method used by the Efficient VPN policy is pre-shared key authentication (8).
VPN name	Name of the VPN instance bound to the Efficient VPN policy. To bind a VPN instance to an Efficient VPN policy, run the **sa binding vpn-instance (Efficient VPN policy view)** command.

Item	Description
Local ID Type	Local ID type in IKE negotiation. ● 1: IP ● 2: Name ● 3: User-fqdn ● 11: Key-id To set the local ID type, run the **local-id-type** command.
IKE Version	Configured IKE version: ● 1: IKEv1 ● 2: IKEv2
Remote Address	IP address of the remote IKE peer. To configure the remote IP address, run the **remote-address** command.
Pre Shared Key Cipher	Pre-shared key. To configure a pre-shared key, run the **pre-shared-key** (Efficient VPN policy view) command.
DH Group	DH group used in IKE negotiation. To specify a DH group, run the **dh** command.
PFS Type	Perfect Forward Secrecy (PFS) used in IKE negotiation. To specify a PFS, run the **pfs** command.
Remote Name	Remote name used in IKE negotiation.
Re-auth interval	IKEv2 re-authentication interval. To configure an IKEv2 re-authentication interval, run the **re-authentication interval** command.
Anti-replay window size	IPSec anti-replay window size. This field is available only when the IPSec anti-replay function is enabled. To set the IPSec anti-replay window size, run the **anti-replay window** command. When the value is 0, the IPSec anti-replay function is enabled in the system view. To enable this function, run the **ipsec anti-replay enable** command.
Service-scheme name	Name of the bound service scheme. To configure the name of the bound service scheme, run the **service-scheme** command.

Item	Description
DPD message type	Sequence of the payload in DPD packets. ● seq-notify-hash ● seq-hash-notify To configure the sequence of the payload, run the **dpd msg** command.
DPD message learning	Whether automatic learning of the payload sequence of DPD packets is enabled. ● enable ● disable To configure the automatic learning function, run the **dpd msg notify-hash-sequence learning** command.
Interface loopback	Number of the loopback interface. The loopback interface is dynamically created on the remote device and is used to establish an IPSec tunnel with the Efficient VPN server.
Interface loopback IP	IP address of the loopback interface, which is allocated by the Efficient VPN server to the remote device.

# Display the IPSec configuration supported by an Efficient VPN policy.

```
<HUAWEI> display ipsec efficient-vpn capability

  IKEv1 Global Supported Algorithms
--------------------------------------------------------
  Supported DH Groups:
    DH_GROUP1 | DH_GROUP2 | DH_GROUP5 | DH_GROUP14 | DH_GROUP19 | DH_GROUP20 |
DH_GROUP21
  Supported Encryption Algorithms:
    DES | 3DES | AES128 | AES192 | AES256
  Supported Authentication Algorithms:
    MD5 | SHA1 | SHA2-256 | SHA2-384 | SHA2-512
  Supported Authentication Methods:
    Pre Shared Key

  IKEv2 Global Supported Algorithms
--------------------------------------------------------
  Supported DH Groups:
    DH_GROUP1 | DH_GROUP2 | DH_GROUP5 | DH_GROUP14 | DH_GROUP19 | DH_GROUP20 |
DH_GROUP21
  Supported Encryption Algorithms:
    DES | 3DES | AES128 | AES192 | AES256
  Supported Integrity Algorithms:
    MD5 | SHA1 | AES-XCBC-96 | SHA2-256 | SHA2-384 | SHA2-512
  Supported PRF:
    PRF-MD5 | PRF-SHA1 | PRF-AES-XCBC-128 | PRF-SHA2-256 | PRF-SHA2-384 |
    PRF-SHA2-512

  IPSEC Global Supported Algorithms
--------------------------------------------------------
  Supported Security Protocols:
    ESP
```

```
Supported Encapsulation Modes:
  TUNNEL
Supported Authentication Algorithms:
  MD5 | SHA1 | SHA256 | SHA384 | SHA512
Supported Encryption Algorithms:
  DES | 3DES | AES128 | AES192 | AES256
```

NOTE

- The MD5 and SHA-1 authentication algorithms have security risks; therefore, you are advised to use SHA-2 preferentially.
- The DES and 3DES encryption algorithms have security risks; therefore, you are advised to use AES preferentially.
- The PRF-MD5 and PRF-SHA1 algorithms have security risks; therefore, you are advised to use PRF-AES-XCBC-128 or SHA-2 preferentially.

Table 10-20 Description of the **display ipsec efficient-vpn capability** command output

Item	Description
IKEv1 Global Supported Algorithms	Supported algorithms when IKEv1 is specified in the Efficient VPN policy. The server can use only the supported algorithms to negotiate with the remote device.
Supported DH Groups	Supported DH groups when IKEv1 or IKEv2 is used.
Supported Encryption Algorithms	Supported encryption algorithms when IKEv1 or IKEv2 is used.
Supported Authentication Algorithms	Supported authentication algorithms when IKEv1 is used. To configure an authentication algorithm on the server.
Supported Authentication Methods	Supported authentication algorithms when IKEv1 is used: Pre Shared Key (pre-shared key authentication).
IKEv2 Global Supported Algorithms	Supported algorithms when IKEv2 is specified in the Efficient VPN policy. The server can use only the supported algorithms to negotiate with the remote device.
Supported Integrity Algorithms	Supported integrity algorithms when IKEv2 is used. To configure an integrity algorithm on the server.
Supported PRF	Supported PRF algorithms when IKEv2 is used.
IPSEC Global Supported Algorithms	Algorithms supported by the system.
Supported Security Protocols	Security protocol supported by IPSec: ESP.

Item	Description
Supported Encapsulation Modes	Encapsulation mode supported by IPSec: tunnel mode.
Supported Authentication Algorithms	Authentication algorithm supported by IPSec.
Supported Encryption Algorithms	Encryption algorithm supported by IPSec.

10.3.11 display ipsec global config

Function

The **display ipsec global config** command displays IPSec global configurations.

Format

display ipsec global config

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

To view IPSec global configurations, run the **display ipsec global config** command. The global configurations include the global SA lifetime and whether the anti-replay function is enabled.

Example

# Display IPSec global configurations.

```
<HUAWEI> display ipsec global config
IPSec Global Config:
----------------------------------------------------------------
  IPSec sa global-duration time-based(seconds)        : 3600
  IPSec sa global-duration traffic-based(kbytes)      : 1843200
  IPSec anti-replay                                   : enable
----------------------------------------------------------------
```

Table 10-21 Description of the **display ipsec global config** command output

Item	Description
IPSec Global Config	IPSec global configurations.
IPSec sa global-duration time-based(seconds)	Time-based global SA lifetime, in seconds. To set the time-based global SA lifetime, run the **ipsec sa global-duration time-based** command.
IPSec sa global-duration traffic-based(kbytes)	Traffic-based global SA lifetime, in kilobytes. To set the traffic-based global SA lifetime, run the **ipsec sa global-duration traffic-based** command.
IPSec anti-replay	Whether the anti-replay function is enabled. To configure the anti-replay function, run the **ipsec anti-replay enable** command.

10.3.12 display ipsec interface brief

Function

The **display ipsec interface brief** command displays IPSec policies bound to an interface.

Format

display ipsec interface brief

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After an IPSec policy is bound to an interface, you can run this command to view information about the bound IPSec policy, such as the policy name and interface to which the policy is bound.

Example

# Display IPSec policies bound to an interface.

```
<HUAWEI> display ipsec interface brief
------------------------------------------------
```

```
IPSec policy        : evpn_client
Using interface     : Vlanif100
IPSec policy number : -
IPSec policy Type   : efficient-vpn
------------------------------------------------
```

Table 10-22 Description of the **display ipsec interface brief** command output

Item	Description
IPSec policy	Sequence number of the IPSec policy bound to the interface. Name of the IPSec policy bound to an interface. To apply an IPSec policy to an interface, run the **ipsec efficient-vpn (interface view)** command.
Using interface	Interface to which an IPSec policy is applied.
IPSec policy number	Sequence number of the IPSec policy bound to the interface.
IPSec policy Type	Type of the IPSec policy bound to an interface.

10.3.13 display ipsec history record

Function

The **display ipsec history record** command displays history information about IPSec tunnels.

Format

display ipsec history record [**remote-address** *remote-address*]

Parameters

Parameter	Description	Value
remote-address *remote-address*	Displays history information about the IPSec tunnel with the specified remote IP address.	The value is in dotted decimal notation.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display ipsec history record** command to view the reason and time of the last teardown of the IPSec tunnel.

Example

# Display history information about IPSec tunnels.

```
<HUAWEI> display ipsec history record
IPSec history record:
Current record number: 1
===============================
Interface              : Vlanif100
remote-address         : 2.1.1.1
remote-port            : 500
VPN instance           : huawei
flow-source            : 10.1.1.1/255.255.255.255
flow-destination       : 10.2.2.2/255.255.255.255
last-offline-reason    : peer request
last-offline-time      : 2017-07-17 20:25:31
offline-times-in-24Hour: 1
```

Table 10-23 Description of the **display ipsec history record** command output

Item	Description
IPSec history record	Display history information about IPSec tunnels.
Current record number	Current record number of the teardown of the IPSec tunnel.
Interface	Interface to which an IPSec policy is applied.
remote-address	Remote IP address of an IPSec tunnel.
remote-port	Remote UDP port number.
VPN instance	Name of a VPN instance.
flow-source	Source address segment of data flows.
flow-destination	Destination address segment of data flows.

Item	Description
last-offline-reason	Reason of the last teardown of an IPSec tunnel. ● dpd timeout: Dead peer detection (DPD) times out. ● peer request: The remote end has sent a message, asking the local end to tear down the tunnel. ● config modify or manual offline: An SA is deleted due to configuration modification or an SA is manually deleted. ● phase1 hard expiry: Hard lifetime expires in phase 1 (no new SA negotiation success message is received). ● phase2 hard expiry: Hard lifetime expires in phase 2. ● heartbeat timeout: heartbeat detection times out. ● modecfg address soft expiry: The IP address lease applied by the remote end from the server expires. ● re-auth timeout: An SA is deleted due to reauthentication timeout. ● aaa cut user: The AAA module disconnects users. ● hard expiry triggered by port mismatch: A hard timeout occurs due to mismatch NAT port number. ● spi conflict: An SPI conflict occurs. ● phase1 sa replace: The new IKE SA replaces the old IKE SA. ● phase2 sa replace: The new IPSec SA replaces the old IPsec SA. ● receive invalid spi notify: The device receives an invalid SPI notification. ● dns resolution status change: DNS resolution status changes. ● ikev1 phase1-phase2 sa dependent offline: The device deletes the associated IPSec SA when deleting an IKEv1 SA. ● exchange timeout: Packet interaction timeout.
last-offline-time	Last time an IPSec tunnel was torn down.
offline-times-in-24Hour	Number of times an IPSec tunnel was torn down within 24 hours.

10.3.14 display ipsec sa efficient-vpn

Function

The **display ipsec sa efficient-vpn** command displays IPSec SA information.

Format

display ipsec sa efficient-vpn *efficient-vpn-name*

Parameters

Parameter	Description	Value
efficient-vpn-name	Displays SA information of an Efficient VPN policy with a specified name.	The value is an existing Efficient VPN policy name.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run this command to check Efficient VPN SA information, such as the local and remote addresses of IPSec tunnels, source and destination addresses of data flows, and SA lifetime.

Example

# Display information about the IPSec SA of Efficient VPN policy.

```
<HUAWEI> display ipsec sa efficient-vpn evpn

ipsec sa information:

===============================
Interface: Vlanif20
===============================


  -----------------------------
  IPSec efficient-vpn name: "evpn"
  Mode                 : EFFICIENTVPN-CLIENT MODE
  -----------------------------
    Connection ID     : 268435456
    Tunnel index      : 4026531842
    Encapsulation mode: Tunnel
    Holding time      : 0d 0h 4m 29s
    Tunnel local      : 10.10.10.1/500
    Tunnel remote     : 10.2.1.2/500
    Flow source       : 10.10.10.6/255.255.255.255 0/0
    Flow destination  : 0.0.0.0/0.0.0.0 0/0
    Flow dscp         : af11

    [Outbound ESP SAs]
      SPI: 2703436139 (0xa123296b)
      Proposal: ESP-ENCRYPT-3DES-192 ESP-AUTH-SHA1
      SA remaining key soft duration (kilobytes/sec): 4666163/2960
      SA remaining key hard duration (kilobytes/sec): 5242880/3355
      Max sent sequence-number: 0
      UDP encapsulation used for NAT traversal: N
      SA encrypted packets (number/bytes): 0/0
```

```
[Inbound ESP SAs]
  SPI: 2303751342 (0x895074ae)
  Proposal: ESP-ENCRYPT-3DES-192 ESP-AUTH-SHA1
  SA remaining key soft duration (kilobytes/sec): 4666163/2960
  SA remaining key hard duration (kilobytes/sec): 5242880/3355
  Max received sequence-number: 0
  UDP encapsulation used for NAT traversal: N
  SA decrypted packets (number/bytes): 0/0
  Anti-replay : Enable
  Anti-replay window size: 1024
```

Table 10-24 Description of the **display ipsec sa efficient-vpn** command output

Item	Description
ipsec sa information	Information about the IPSec SA.
Interface	Interface to which the Efficient VPN policy is applied.
IPSec efficient-vpn name	Name of the Efficient VPN policy. To configure the Efficient VPN policy name, run the **ipsec efficient-vpn** command in the system view.
Mode	Mode in which an Efficient VPN policy is created.
Connection ID	ID of the IPSec SA connection.
Tunnel index	Tunnel index.
Encapsulation mode	Encapsulation mode in an IPSec proposal.
Holding time	Time elapsed since an IPSec tunnel was created.
Tunnel local	IP address and NAT traversal port of the local interface. To configure the IP address of the local interface, run the **tunnel local** command.
Tunnel remote	IP address and NAT traversal port of the remote interface. To configure the IP address of the remote interface, run the **remote-address** command in the Efficient VPN policy view.
Flow source	Source IP address segment of the data flow sent from the local end and the protocol number and port number of the ACL.
Flow destination	Destination IP address segment of the data flow sent from the local end and the protocol number and port number of the ACL.
Flow dscp	DSCP value of the data flow sent from the local end.
Outbound ESP SAs	Outbound IPSec SA information using ESP.
SPI	SPI of an SA.
Proposal	IPSec proposal.

Item	Description
SA remaining key soft duration (kilobytes/sec)	Remaining soft lifetime of an IPSec SA, in kilobytes or seconds.
SA remaining key hard duration (kilobytes/sec)	Remaining hard lifetime of an IPSec SA, in kilobytes or seconds. To set the SA lifetime, run the **ipsec sa global-duration** command.
Max sent sequence-number	Maximum sequence number of sent packets. The sequence number increases during communication and is used for anti-replay.
UDP encapsulation used for NAT traversal	Whether NAT traversal is enabled: ● Y ● N
SA encrypted packets (number/bytes)	Number of packets that are successfully encrypted using the IPSec SA.
Inbound ESP SAs	Inbound IPSec SA information using ESP.
Max received sequence-number	Maximum sequence number of received packets.
SA decrypted packets (number/bytes)	Number of packets that are successfully decrypted using the IPSec SA.
Anti-replay	Whether the anti-replay function is enabled for an IPSec tunnel: ● Enable ● disable To configure the anti-replay function for an IPSec tunnel, run the **ipsec anti-replay enable** command.
Anti-replay window size	IPSec anti-replay window size. This field is valid only when the IPSec anti-replay function is enabled. To set the IPSec anti-replay window size, run the **anti-replay window** or **ipsec anti-replay window** command.

10.3.15 display ipsec packet statistics

Function

The **display ipsec packet statistics** command displays IPSec packet statistics.

Format

display ipsec packet statistics

Parameters

None.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

You can run the **display ipsec packet statistics** command to view IPSec packet statistics, including statistics about incoming or outgoing packets that are protected, statistics about encrypted and decrypted packets, detailed statistics about discarded packets that are protected, and statistics about IKE negotiation related packets. The IPSec packet statistics facilitate IPSec fault diagnosis and maintenance.

Precautions

The **display ipsec packet statistics** command only displays the number of plaintext bytes.

Example

# Display statistics about all IPSec packets.

```
<HUAWEI> display ipsec packet statistics
 IPSec statistics information:
 Number of IPSec tunnels: 1
 Number of standby IPSec tunnels: 0
 the security packet statistics:
   input/output security packets: 0/0
   input/output security bytes: 0/0
   input/output dropped security packets: 0/0
   the encrypt packet statistics:
     send chip: 0, recv chip: 0, send err: 0
     local cpu: 0, other cpu: 0, recv other cpu: 0
     intact packet: 0, first slice: 0, after slice: 0
   the decrypt packet statistics:
     send chip: 0, recv chip: 0, send err: 0
     local cpu: 0, other cpu: 0, recv other cpu: 0
     reass  first slice: 0, after slice: 0
   dropped security packet detail:
     can not find SA: 0, wrong SA: 0
     authentication: 0, replay: 0
     front recheck: 0, after recheck: 0
     change cpu enc: 0, dec change cpu: 0
     fib search: 0, output l3: 0
     flow err: 0, slice err: 0, byte limit: 0
  negotiate about packet statistics:
```

```
IKE fwd packet ok: 0, err: 0
IKE ctrl packet inbound ok: 0, outbound ok: 0
SoftExpr: 0, HardExpr: 0, DPDOper: 0
trigger ok: 0, switch sa: 0, sync sa: 0
recv IKE nat keepalive: 0, IKE input: 0
```

Table 10-25 Description of the **display ipsec packet statistics** command output

Item	Description
IPSec statistics information	Statistics about IPSec packets.
Number of IPSec tunnels	Number of the IPSec tunnels.
Number of standby IPSec tunnels	Number of the standby IPSec tunnels.
the security packet statistics	Statistics about packets that are protected.
input/output security packets	Number of incoming or outgoing packets that are protected.
input/output security bytes	Number of incoming or outgoing bytes that are protected.
input/output dropped security packets	Number of discarded incoming or outgoing packets that are protected.
the encrypt packet statistics	Statistics about encrypted packets.
send chip	Number of packets sent to the hardware for encryption and decryption.
recv chip	Number of packets encrypted and decrypted by hardware.
send err	Number of packets that fail to be sent to hardware for encryption and decryption.
local cpu	Number of packets encrypted and decrypted by the local CPU.
other cpu	Number of packets forwarded to another CPU for encryption and decryption.
recv other cpu	Number of packets received from another CPU for encryption and decryption.
intact packet	Number of non-fragmented encrypted packets.
first slice	Number of initial fragmented packets.
after slice	Number of non-initial fragmented packets.

Item	Description
the decrypt packet statistics	Statistics about decrypted packets.
reass first slice	Number of initial packets that are reassembled.
after slice	Number of non-initial packets that are reassembled.
dropped security packet detail	Detailed statistics about discarded packets that are protected.
can not find SA	Number of packets for which SAs are not found.
wrong SA	Number of packets with invalid SAs.
authentication	Number of packets that fail to be authenticated.
replay	Number of discarded packets due to replay check.
front recheck	Number of discarded packets due to IPSec pre-check.
after recheck	Number of discarded packets due to IPSec post-check.
change cpu enc	Number of encrypted packets that fail to be forwarded.
dec change cpu	Number of decrypted packets that fail to be forwarded.
fib search	Number of encrypted packets that are discarded due to route searching failure.
output l3	Number of encrypted packets that fail to be sent.
flow err	Number of packets discarded because negotiation is triggered.
slice err	Number of IPSec packets that fail to be fragmented.
byte limit	Number of discarded packets due to traffic limit.
negotiate about packet statistics	Statistics about IKE negotiation packets.
IKE fwd packet ok	Number of IKE packets sent to the IKE process.

Item	Description
err	Number of IKE packets that fail to be sent to the IKE process.
IKE ctrl packet inbound ok	Number of IKE packets received by the control plane.
outbound ok	Number of IKE packets sent by the control plane.
SoftExpr	Number of traffic soft timeouts.
HardExpr	Number of traffic hard timeouts.
DPDOper	Number of times DPD is performed in on-demand DPD mode.
trigger ok	Number of times that negotiation is triggered.
switch sa	Number of times the local device receives data encrypted with the new SA and instructs the IKE process to replace the SA.
sync sa	Number of times the active device notifies the IKE process that the SA 3-tuple (remote address, SPI, protocol ID) does not exist on the standby device.
recv IKE nat keepalive	Number of received IKE nat keepalive packets.
IKE input	Number of received IKE packets.

10.3.16 display ipsec statistics tunnel-number

Function

The **display ipsec statistics tunnel-number** command displays the number of IPSec tunnels.

Format

display ipsec statistics tunnel-number

Parameters

None.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run this command to check the number of IPSec tunnels.

Example

# Display the number of IPSec tunnels.

```
<HUAWEI> display ipsec statistics tunnel-number
  IPSec tunnel totals: 0
  IPSec tunnel specifications: 4000
```

Table 10-26 Description of the **display ipsec statistics tunnel-number** command output

Item	Description
IPSec tunnel totals	Number of IPSec tunnels.
IPSec tunnel specifications	IPSec tunnel specifications.

10.3.17 dpd msg

Function

The **dpd msg** command configures the payload sequence of DPD packets on the specified IKE peer.

The **undo dpd msg** command restores the default payload sequence of DPD packets on the specified IKE peer.

By default, the payload sequence of DPD packets on an IKE peer is **seq-notify-hash**.

Format

dpd msg { **seq-hash-notify** | **seq-notify-hash** }

undo dpd msg

Parameters

Parameter	Description	Value
seq-hash-notify	Indicates that in a DPD packet, the hash payload is before the notify payload.	-
seq-notify-hash	Indicates that in a DPD packet, the notify payload is before the hash payload.	-

Views

Efficient VPN policy view

Default Level

2: Configuration level

Usage Guidelines

DPD packets carrying the notify payload and hash payload are exchanged bidirectionally. The notify payload sent by the initiator carries an R-U-THERE message equivalent to a Hello packet, and the notify payload sent by the responder carries an R-U-THERE-ACK message equivalent to an ACK packet.

The payload sequence of DPD packets sent by different devices may be different. IKE peers on both ends must send DPD packets with the same payload sequence; otherwise, DPD does not take effect. In this case, run the **dpd msg** command to set the same payload sequence of DPD packets on both ends.

Precautions

This command applies only when an IKE peer uses IKEv1.

Example

# Set the payload sequence of DPD packets to **hash-notify**.

```
<HUAWEI> system-view
[HUAWEI] ipsec efficient-vpn evpn mode client
[HUAWEI-ipsec-efficient-vpn-evpn] dpd msg seq-hash-notify
```

10.3.18 dpd msg notify-hash-sequence learning

Function

The **dpd msg notify-hash-sequence learning** command enables automatic learning of the payload sequence of DPD packets.

The **undo dpd msg notify-hash-sequence learning** command disables automatic learning of the payload sequence of DPD packets.

By default, automatic learning of the payload sequence of DPD packets is enabled.

Format

dpd msg notify-hash-sequence learning

undo dpd msg notify-hash-sequence learning

Parameters

None

Views

Efficient VPN policy view

Default Level

2: Configuration level

Usage Guidelines

When DPD is used to detect the IKEv1 peer status, the payload sequence of DPD packets on both ends must be consistent. Otherwise, DPD does not take effect, and even the IPSec tunnel between both ends flaps.

If the local end does not know the payload sequence of DPD packets sent from the remote end, run the **dpd msg notify-hash-sequence learning** command on the local end to enable automatic learning of the payload sequence of DPD packets. When the local end receives a DPD packet from the remote end, the local end learns the payload sequence of the DPD packet and sends a DPD packet in the same payload sequence.

Example

# Enable automatic learning of the payload sequence of DPD packets.

```
<HUAWEI> system-view
[HUAWEI] ipsec efficient-vpn evpn mode client
[HUAWEI-ipsec-efficient-vpn-evpn] dpd msg notify-hash-sequence learning
```

10.3.19 ike dscp

Function

The **ike dscp** command sets a global DSCP priority of IKE packets.

The **undo ike dscp** command cancels the DSCP priority configuration.

By default, the global DSCP priority of IKE packets is 0.

Format

ike dscp *dscp-value*

undo ike dscp

Parameters

Parameter	Description	Value
dscp-value	Specifies the global DSCP priority of IKE packets.	The value can be an integer or a string of characters. That is, the value can be an integer that ranges from 0 to 63, or a string of AF11 to AF13, AF21 to AF23, AF31 to AF33, AF41 to AF43, CS1 to CS7, EF, or default.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

IKE packets are used for IKE SA and IPSec SA negotiation or DPD. When IKE packets are lost during transmission, IPSec SAs may fail to be negotiated. As a result, packets that need to be protected by IPSec are not protected. The DSCP priority of IKE packets can be improved so that IKE packets are processed preferentially. IKE packet transmission reliability is therefore improved.

To configure the DSCP priority for IKE packets of all IKE peers, run this command.

Example

# Set a global DSCP priority of IKE packets to CS2.

```
<HUAWEI> system-view
[HUAWEI] ike dscp cs2
```

10.3.20 ike heartbeat

Function

The **ike heartbeat** command sets heartbeat parameters.

The **undo ike heartbeat** command restores the default configuration.

By default, a heartbeat packet uses old type sequence number mechanism and does not carry the SPI list.

Format

ike heartbeat { **seq-num** { **new** | **old** } | **spi-list** }

undo ike heartbeat { **seq-num** | **spi-list** }

Parameters

Parameter	Description	Value
seq-num { **new** | **old** }	Configures the sequence number mechanism for heartbeat packets. ● **new**: The sequence number mechanism conforms to draft-ietf-ipsec-heartbeats-00.txt. ● **old**: The sequence number mechanism conforms to the standard that before draft-ietf-ipsec-heartbeats-00.txt emerges.	-
spi-list	Configures heartbeat packets to carry the SPI list.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In IPSec communication, if the local end becomes faulty and the remote end does not detect the fault because of system failures, the remote end still sends IPSec packets to the local end, causing traffic loss. Heartbeat detection solves this problem. After heartbeat detection is enabled, the local end periodically sends detection packets to the remote end. If the remote end does not receive packets after the heartbeat timer expires, the remote end considers the local end faulty. IKE can send heartbeat packets to detect IKE peer faults and maintain the IKE SA link status.

Precautions

The two ends must use the same heartbeat parameters.

If you run the **ike heartbeat** { **seq-num** { **new** | **old** } | **spi-list** } command multiple times, only the latest configuration takes effect.

Example

# Configure the sequence number mechanism for heartbeat packets to **new**.

```
<HUAWEI> system-view
[HUAWEI] ike heartbeat seq-num new
```

10.3.21 ike heartbeat-timer interval

Function

The **ike heartbeat-timer interval** command sets the interval for sending heartbeat packets through an IKE SA.

The **undo ike heartbeat-timer interval** command cancels the configuration.

By default, an IKE SA does not send heartbeat packets.

Format

ike heartbeat-timer interval *interval*

undo ike heartbeat-timer interval

Parameters

Parameter	Description	Value
interval	Specifies the interval for sending heartbeat packets through an IKE SA.	The value is an integer that ranges from 20 to 28800, in seconds.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After heartbeat detection is enabled, the local end periodically sends detection packets to the remote end. If the remote end does not receive packets after the heartbeat timer expires, the remote end considers the local end faulty. IKE can send heartbeat packets to detect IKE peer faults and maintain the IKE SA link status. This command sets the interval for sending heartbeat packets through an IKE SA.

The interval at which heartbeat packets are sent (configured using the **ike heartbeat-timer timeout** command) at the local end must be used with the timeout interval of heartbeat packets (configured using the **ike heartbeat-timer timeout** command) at the remote end. If the remote end does not receive any heartbeat packet within the timeout interval, it deletes the IKE SA with a timeout tag along with its corresponding IPSec SA. If the IKE SA does not have a timeout tag, it is marked as timeout.

Precautions

When the **ike heartbeat-timer interval** command is configured at one end, the **ike heartbeat-timer timeout** command must be used at the other end.

The timeout interval of heartbeat packets must be longer than the interval at which heartbeat packets are sent. On a network, packet loss seldom occurs more than three consecutive times. Therefore, it is recommended that the timeout interval of heartbeat packets be three times the interval at which heartbeat packets are sent.

Example

# Set the interval for sending heartbeat packets to 20 seconds.

```
<HUAWEI> system-view
[HUAWEI] ike heartbeat-timer interval 20
```

10.3.22 ike heartbeat-timer timeout

Function

The **ike heartbeat-timer timeout** command sets the timeout interval during which an IKE SA waits for a heartbeat packet.

The **undo ike heartbeat-timer timeout** command cancels the configuration.

By default, the timeout interval during which an IKE SA waits for a heartbeat packet is not configured.

Format

ike heartbeat-timer timeout *seconds*

undo ike heartbeat-timer timeout

Parameters

Parameter	Description	Value
seconds	Specifies the timeout interval during which an IKE SA waits for a heartbeat packet.	The value is an integer that ranges from 30 to 28800, in seconds.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After heartbeat detection is enabled, the local end periodically sends detection packets to the remote end. If the remote end does not receive packets after the heartbeat timer expires, the remote end considers the local end faulty. IKE can send heartbeat packets to detect IKE peer faults and maintain the IKE SA link status. This command sets the timeout interval during which an IKE SA waits for a heartbeat packet.

Precautions

When the **ike heartbeat-timer interval** command is configured at one end, the **ike heartbeat-timer timeout** command must be used at the other end.

The timeout interval of heartbeat packets must be longer than the interval at which heartbeat packets are sent. On a network, packet loss seldom occurs more than three consecutive times. Therefore, it is recommended that the timeout interval of heartbeat packets be three times the interval at which heartbeat packets are sent.

Example

# Set the timeout interval during which an IKE SA waits for a heartbeat packet to 60 seconds.

```
<HUAWEI> system-view
[HUAWEI] ike heartbeat-timer timeout 60
```

10.3.23 ike local-name

Function

The **ike local-name** command configures the local name for IKE negotiation.

The **undo ike local-name** command deletes the local name for IKE negotiation.

By default, no local name is configured for IKE negotiation.

Format

ike local-name *local-name*

undo ike local-name

Parameters

Parameter	Description	Value
local-name	Specifies a local name for IKE negotiation.	The value is a string of 1 to 255 case-sensitive characters without question marks (?).

Views

System view

Default Level

2: Configuration level

Usage Guidelines

When identity authentication, If the ID type of an IKE peer is fully qualified domain name (FQDN), or USER-FQDN, the IKE peer uses the name for identity authentication. In this case, you need to run the **ike local-name** command to configure the local name.

Example

# Set the local ID for IKE negotiation to **Huawei**.

```
<HUAWEI> system-view
[HUAWEI] ike local-name Huawei
```

10.3.24 ike nat-keepalive-timer interval

Function

The **ike nat-keepalive-timer interval** command configures the interval for sending NAT Keepalive packets.

The **undo ike nat-keepalive-timer interval** command restores the default setting.

By default, the interval for sending NAT Keepalive packets is 20 seconds.

Format

ike nat-keepalive-timer interval *interval*

undo ike nat-keepalive-timer interval

Parameters

Parameter	Description	Value
interval	Specifies the interval for sending NAT Keepalive packets.	The value is an integer that ranges from 5 to 300, in seconds.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

When an NAT gateway exists between two IKE peers, to prevent NAT entries from being aged, the device on the private network side of the NAT gateway sends NAT Keepalive packets to its peer at a certain interval to maintain the NAT session.

Example

# Configure the interval for sending NAT Keepalive packets to 30 seconds.

```
<HUAWEI> system-view
[HUAWEI] ike nat-keepalive-timer interval 30
```

10.3.25 ikev1 phase1-phase2 sa dependent

Function

The **ikev1 phase1-phase2 sa dependent** command enables dependency between IPSec SA and IKE SA during IKEv1 negotiation.

The **undo ikev1 phase1-phase2 sa dependent** command cancels dependency between IPSec SA and IKE SA during IKEv1 negotiation.

By default, no dependency exists between IPSec SA and IKE SA during IKEv1 negotiation.

Format

ikev1 phase1-phase2 sa dependent

undo ikev1 phase1-phase2 sa dependent

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

During IKEv1 negotiation, an IKE SA is established during phase 1, and an IPSec SA is established during phase 2. By default, no dependency exists between IPSec SA and IKE SA, that is, the two SAs can be deleted separately. If the IKE SA is deleted but the corresponding IPSec SA still exists, traffic forwarding will be effected. To prevent this problem, you can run this command to enable dependency between IPSec SA and IKE SA.

Prerequisites

Before running this command, you need to install the weak encryption algorithm plug-in and run the **version 1** command in the IKE peer view to enable IKEv1. Otherwise, the command configuration does not take effect. For details about how to install the WEAKEA plug-in, see "WEAKEA Configuration" in the *CLI-based Configuration Guide*.

Example

# Enable dependency between IPSec SA and IKE SA during IKEv1 negotiation.

```
<HUAWEI> system-view
[HUAWEI] ikev1 phase1-phase2 sa dependent
```

10.3.26 ikev2 delete old child-sa enable

Function

The **ikev2 delete old child-sa enable** command enables the function of instructing the peer device to delete the old child SA.

The **undo ikev2 delete old child-sa enable** command disables the function of instructing the peer device to delete the old child SA.

By default, the function of instructing the peer device to delete the old child SA is enabled.

Format

ikev2 delete old child-sa enable

undo ikev2 delete old child-sa enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

In an IKEv2 scenario, when the local device deletes the child SA and initiates IKEv2 negotiation to the peer device again, the default negotiation message carries the IKEV2_NOTIFY_DELETE_OLD_CHILDSA payload, instructing the peer device to delete the old child SA. If the peer device does not support the processing of this payload, IKEv2 negotiation between the two ends fails. To prevent this problem, run the **undo ikev2 delete old child-sa enable** command on the local device to disable it from instructing the peer device to delete the old child SA so that the IKEv2 negotiation message does not carry this payload.

Example

# Enable the function of instructing the peer device to delete the old child SA.

```
<HUAWEI> system-view
[HUAWEI] ikev2 delete old child-sa enable
```

10.3.27 ikev2 initial-contact enable

Function

The **ikev2 initial-contact enable** command enables the device to send the INITIAL_CONTACT notify payload in the first IKE_AUTH request.

The **undo ikev2 initial-contact enable** command disables the device from sending the INITIAL_CONTACT notify payload in the first IKE_AUTH request.

By default, the device is disabled to send the INITIAL_CONTACT notify payload in the first IKE_AUTH request.

Format

ikev2 initial-contact enable

undo ikev2 initial-contact enable

Parameters

None

Views

System View

Default Level

2: Configuration level

Usage Guidelines

The INITIAL_CONTACT notify payload asserts that an IKE SA is the only active IKE SA between a pair of IKE peers. By default, the device will delete the old IKE SA without the INITIAL_CONTACT notify payload after the new IKE SA is created. When the remote end requires the INITIAL_CONTACT notify payload to delete the old IKE SA, configure this command.

When the local device restarts or expects to use the current IKE SA for establishing an IPSec tunnel only, run this command to enable the device to send the INITIAL_CONTACT notify payload in the first IKE_AUTH request so that the remote device deletes the old IKE SA.

Example

# Enable the device to send the INITIAL_CONTACT notify payload in the first IKE_AUTH request.

```
<HUAWEI> system-view
[HUAWEI] ikev2 initial-contact enable
```

10.3.28 ipsec anti-replay enable

Function

The **ipsec anti-replay enable** command enables the anti-replay function globally.

The **undo ipsec anti-replay enable** command disables the anti-replay function globally.

By default, the anti-replay function is enabled globally.

Format

ipsec anti-replay enable

undo ipsec anti-replay enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Replayed packets refer to the packets that have been processed by the device. IPSec uses the sliding window (anti-replay window) to detect replayed packets. AH and ESP packet headers carry 32-bit sequence numbers. The sequence numbers carried in the AH or ESP packet headers of the same SA are in ascending order. If the sequence number of an authenticated packet is the same as that of a decapsulated packet or the sequence number is outside the sliding window, the packet is considered a replayed packet.

Decapsulating replayed packets consumes many resources and makes system performance deteriorate. Therefore, attackers may use replayed packets to initiate a DoS attack. After the anti-replay function is enabled, the system discards replayed packets to save system resources.

Precautions

In some situations, for example, network congestion occurs or QoS is performed for packets, the sequence numbers of some service data packets may be different from those in common data packets. The device that has IPSec anti-replay enabled considers the packets replayed and discards them. You can disable global IPSec anti-replay to prevent packets from being discarded incorrectly or adjust the IPSec anti-replay window size to meet service requirements.

Example

# Enable the anti-replay function globally.

```
<HUAWEI> system-view
[HUAWEI] ipsec anti-replay enable
```

10.3.29 ipsec anti-replay window

Function

The **ipsec anti-replay window** command sets the global IPSec anti-replay window size.

The **undo ipsec anti-replay window** command restores the default global IPSec anti-replay window size.

By default, the global IPSec anti-replay window size is 1024 bits.

Format

ipsec anti-replay window *window-size*

undo ipsec anti-replay window

Parameters

Parameter	Description	Value
window-size	Specifies the global IPSec anti-replay window size.	The value can be 32, 64, 128, 256, 512, or 1024, in bits.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In some situations, for example, network congestion occurs or QoS is performed for packets, the sequence numbers of some service data packets may be unusual. The device that has IPSec anti-replay enabled considers the packets replayed and discards them. To prevent packets from being discarded incorrectly, you can disable global IPSec anti-replay or adjust the IPSec anti-replay window size to meet service requirements.

Prerequisites

The anti-replay function has been enabled. By default, the anti-replay function is enabled (through **ipsec anti-reply enable** command).

Precautions

When both **anti-replay window** and **ipsec anti-replay window** are used, the **anti-replay window** command takes effect. When **anti-replay window** is not configured, the **ipsec anti-replay window** command takes effect.

Example

# Set the global IPSec anti-replay window size to 128 bits.

```
<HUAWEI> system-view
[HUAWEI] ipsec anti-replay window 128
```

10.3.30 ipsec efficient-vpn (interface view)

Function

The **ipsec efficient-vpn** command binds an Efficient VPN policy to an interface.

The **undo ipsec efficient-vpn** command deletes the Efficient VPN policy from an interface.

By default, no Efficient VPN policy is applied to an interface.

Format

ipsec efficient-vpn *efficient-vpn-name*

undo ipsec efficient-vpn

Parameters

Parameter	Description	Value
efficient-vpn-name	Specifies the name of an Efficient VPN policy.	The value is an existing Efficient VPN policy name.

Views

VLANIF interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When many branches and traveling staff connect to the headquarters over IPSec tunnels, similar or duplicate IPSec configurations and other network resource configurations must be configured on the branch and headquarters gateways. The Efficient VPN solution uses centralized IPSec configurations on the headquarters gateway and simplified IPSec configuration on each branch gateway. This solution reduces the manual configuration workload, and facilitates IPSec VPN configuration and maintenance.

Prerequisites

An Efficient VPN policy has been created using the **ipsec efficient-vpn (system view)** command.

Precautions

If an Efficient VPN policy is used to establish an IPSec tunnel between the enterprise branch and headquarters, apply the Efficient VPN policy to the branch gateway and use an IPSec policy template on the headquarters gateway to create an IPSec policy.

Example

# Apply the Efficient VPN policy named **evpn** to **VLANIF10**.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 10
[HUAWEI-Vlanif10] ipsec efficient-vpn evpn
```

10.3.31 ipsec efficient-vpn (system view)

Function

The **ipsec efficient-vpn** command creates an IPSec Efficient VPN policy and displays the IPSec Efficient VPN policy view.

The **undo ipsec efficient-vpn** command deletes an IPSec Efficient VPN policy.

By default, no IPSec Efficient VPN policy is created in the system.

Format

ipsec efficient-vpn *efficient-vpn-name* [**mode** { **client** | **network** | **network-plus** }]

undo ipsec efficient-vpn *efficient-vpn-name*

Parameters

Parameter	Description	Value
efficient-vpn-name	Specifies the name of an Efficient VPN policy.	The value is a string of 1 to 12 case-sensitive characters without question marks (?) or spaces.
mode	Specifies the mode of the Efficient VPN policy.	-
client	Indicates the client mode.	-
network	Indicates the network mode.	-
network-plus	Indicates the network-plus mode.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When many branches and traveling staff connect to the headquarters over IPSec tunnels, similar or duplicate IPSec configurations and other network resource configurations must be configured on the branch and headquarters gateways. The Efficient VPN solution uses centralized IPSec configurations on the headquarters gateway and simplified IPSec configuration on each branch gateway. This solution reduces the manual configuration workload, and facilitates IPSec VPN configuration and maintenance.

The Efficient VPN policy has the following modes:

- Client mode

  When a remote device requests an IP address from the Efficient VPN server, a loopback interface is dynamically created on the remote device and the IP address obtained from the server is assigned to the loopback interface. The remote device uses this IP address to establish an IPSec tunnel with the headquarters.

  The client mode applies to scenarios where small-scale branches connect to the headquarters network through private networks. In client mode, devices connected to the Efficient VPN server or remote devices can use the same IP address. However, the number of devices allowed depends on the number of IP addresses assigned by the Efficient VPN server.

- Network mode

  In network mode, a remote device does not apply to the Efficient VPN server for an IP address. Instead, the remote device uses the original IP address to establish an IPSec tunnel with the headquarters.

  The network mode applies to scenarios where IP addresses of the headquarters and branches are planned uniformly. Ensure that IP addresses do not conflict.

- Network-plus mode

  Compared with the network mode, the remote device applies to the Efficient VPN server for an IP address in network-plus mode. IP addresses of branches and headquarters are configured beforehand. A remote device applies to the Efficient VPN server for an IP address. The Efficient VPN server uses the IP address to perform ping, Telnet, or other management and maintenance operations on the remote device.

Follow-up Procedure

Configure negotiation parameters of Efficient VPN in the Efficient VPN policy view, and use the **ipsec efficient-vpn (interface view)** command to bind the Efficient VPN policy to an interface.

Example

# Create the Efficient VPN policy named **vpn1** in client mode.

```
<HUAWEI> system-view
[HUAWEI] ipsec efficient-vpn vpn1 mode client
[HUAWEI-ipsec-efficient-vpn-vpn1]
```

10.3.32 ipsec sa global-duration

Function

The **ipsec sa global-duration** command sets the global hard lifetime of IPSec SAs.

The **undo ipsec sa global-duration** command restores the default global hard lifetime of IPSec SAs.

By default, the global time-based SA hard lifetime is 3600 seconds and the global traffic-based SA hard lifetime is 1843200 Kbytes.

Format

ipsec sa global-duration { **time-based** *interval* | **traffic-based** *size* }

undo ipsec sa global-duration { **time-based** | **traffic-based** }

Parameters

Parameter	Description	Value
time-based *interval*	Specifies the time-based global IPSec SA hard lifetime. When a large number of IPSec tunnels are established between two devices, you are advised to set the global IPSec SA hard lifetime to a value larger than or equivalent to 1800s.	It is an integer that ranges from 30 to 604800, in seconds.
traffic-based *size*	Specifies the traffic-based global IPSec SA hard lifetime. It is recommended that the traffic volume be equal to or larger than the size of IPSec traffic forwarded in 1 hour.	The value is 0 or an integer from 256 to 200000000, in Kbytes. ● IKEv1 for IPSec negotiation: If the traffic hard lifetime is set to 0 on either device, both the local and remote devices disable the traffic timeout function. ● IKEv2 for IPSec negotiation: If the traffic hard lifetime is set to 0 on either device, the local device disables the traffic timeout function.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

For a dynamic SA, configure the SA hard lifetime so that the SA can be updated in real time, reducing the crash risk and improving security.

There are two methods to measure the lifetime:

- Time-based lifetime

  The period from when an SA is set up to when the SA is expired.

- Traffic-based lifetime

  The maximum volume of traffic that this SA can process.

The lifetime is classified as follows:

- Hard lifetime: specifies the lifetime of an IPSec SA.

  When two devices negotiate an IPSec SA, the actual hard lifetime is the smaller of the two values configured on the two devices.

- Soft lifetime: specifies the time after which a new IPSec SA is negotiated so that the new IPSec SA will be ready before the hard lifetime of the original IPSec SA expires.

  Table 10-27 lists the default soft lifetime values.

Table 10-27 Soft lifetime values

Soft Lifetime Type	Description
Time-based soft lifetime (soft timeout period)	The value is 70% of the actual hard lifetime (hard timeout period).
Traffic-based soft lifetime (soft timeout traffic)	● For IKEv1, the value is 70% of the actual hard lifetime (hard timeout traffic). ● For IKEv2, the value is 65% to 75% of the actual hard lifetime (hard timeout traffic) plus or minus a random value.

Before an IPSec SA becomes invalid, IKE negotiates a new IPSec SA for the remote end. The remote end uses the new IPSec SA to protect IPSec communication immediately after the new IPSec SA is negotiated. If service traffic is transmitted, the original IPSec SA is deleted immediately. If no service traffic is transmitted, the original IPSec SA will be deleted after 10s or the hard lifetime expires.

If the time-based lifetime and traffic-based lifetime are both set for an IPSec SA, the IPSec SA becomes invalid when either lifetime expires.

Precautions

During IKEv1 negotiation:

- The responder cannot initiate IPSec SA renegotiation after the IPSec SA soft lifetime expires.
- The initiator cannot initiate IPSec SA renegotiation when its IKE SA is deleted and the IPSec SA soft lifetime expires.

During IKEv2 negotiation, the initiator or responder cannot initiate IPSec SA renegotiation if the IKE SA is deleted and the IPSec SA soft lifetime expires.

Example

# Set the time-based global SA hard lifetime to 7200s.

```
<HUAWEI> system-view
[HUAWEI] ipsec sa global-duration time-based 7200
```

# Set the traffic-based global SA hard lifetime to 10 MB.

```
<HUAWEI> system-view
[HUAWEI] ipsec sa global-duration traffic-based 10240
```

10.3.33 local-id-type

Function

The **local-id-type** command sets the type of the local ID used in IKE negotiation.

The **undo local-id-type** command restores the default type of the local ID used in IKE negotiation.

By default, the local ID type used by IKE negotiation is IP.

Format

local-id-type { **fqdn** | **ip** | **key-id** | **user-fqdn** }

undo local-id-type

Parameters

Parameter	Description	Value
fqdn	Specifies the name as the local ID.	-
ip	Specifies the IP address as the local ID.	-
key-id	Specifies the key-id as the local ID.	-
user-fqdn	Specifies the USER-FQDN as the local ID.	-

Views

Efficient VPN policy view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Identity authentication is a protection mechanism for IKE negotiation. The device ensures security by confirming identities of communication parties. IKE peers can use different types. This command configures the type of the local ID of an IKE peer.

Precautions

- The local ID type can be different from the remote ID type. You can use commands to specify the local and remote ID types.
- For pre-shared key authentication, the local ID type on the local end must be the same as the remote ID type on the remote end, and the local ID on the local end must be the same as the remote ID on the remote end.

Different authentication methods support different ID types, as shown in **Table 10-28**.

Table 10-28 Relationship between local IKE ID types, local ID, and authentication methods

Authentication Method	IP	FQDN	USER-FQDN	key-id
pre-share	Supported The IP address is the local IP address used for IKE negotiation by default.	Supported The ID specified by the **ike local-name** command, indicating that all peers on the device use this ID for identity authentication.	Supported The ID specified by the **ike local-name** command, indicating that all peers on the device use this ID for identity authentication.	Supported This parameter is often used when the device using the Efficient VPN policy functions as a remote end to communicate with Cisco devices.

Example

# Set the local ID type of Efficient VPN to FQDN.

```
<HUAWEI> system-view
[HUAWEI] ipsec efficient-vpn evpn mode client
[HUAWEI-ipsec-efficient-vpn-evpn] local-id-type fqdn
```

10.3.34 pfs

Function

The **pfs** command enables PFS when the local end initiates IPSec tunnel negotiation.

The **undo pfs** command disables PFS when the local end initiates IPSec tunnel negotiation.

By default, PFS is not used when the local end initiates IPSec tunnel negotiation.

Format

pfs { **dh-group14** | **dh-group19** | **dh-group20** | **dh-group21** }

undo pfs

Parameters

Parameter	Description	Value
dh-group14	Uses the 2048-bit DH group.	-
dh-group19	Uses the 256-bit Elliptic Curve Groups modulo a Prime (ECP) DH group.	-
dh-group20	Uses the 384-bit ECP DH group.	-
dh-group21	Uses the 521-bit ECP DH group.	-

Views

Efficient VPN policy view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the local end initiates negotiation, there is an additional DH exchange in IKEv1 phase 2 or IKEv2 CREATE_CHILD_SA exchange. The additional DH exchange ensures security of the IPSec SA key and improves communication security.

Precautions

The system software does not support the **dh-group1**, **dh-group2**, and **dh-group5** parameters. To use these DH groups, you need to install the WEAKEA plug-in. For higher security purposes, you are advised to specify other DH groups.

For details about how to install the WEAKEA plug-in, see "WEAKEA Configuration" in the *CLI-based Configuration Guide*.

Example

# Enable the PFS feature in the IPSec Efficient VPN policy **evpn**.

```
<HUAWEI> system-view
[HUAWEI] ipsec efficient-vpn evpn mode client
[HUAWEI-ipsec-efficient-vpn-evpn] pfs dh-group14
```

10.3.35 pre-shared-key (Efficient VPN policy view)

Function

The **pre-shared-key** command configures the pre-shared key used by IKE peers to perform pre-shared key authentication.

The **undo pre-shared-key** command deletes the pre-shared key used by IKE peers to perform pre-shared key authentication.

By default, the pre-shared key used by IKE peers to perform pre-shared key authentication is not configured.

Format

pre-shared-key cipher *key*

undo pre-shared-key

Parameters

Parameter	Description	Value
cipher	Indicates the pre-shared key in cipher text. You can enter a pre-shared key in plain text or cipher text, but the pre-shared key is displayed in cipher text in the configuration file.	-
key	Specifies the pre-shared key used by IKE peers to perform pre-shared key authentication.	The value is a string of case-sensitive characters without spaces. A plaintext key contains 1 to 128 characters, and a ciphertext key contains 48 to 188 characters. If the character string is enclosed in double quotation marks (" "), the character string can contain spaces. **NOTE** For security purposes, it is recommended that the pre-shared key contain at least three types of lowercase letters, uppercase letters, digits, and special characters and contain at least 8 characters.

Views

Efficient VPN policy view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

During IKE negotiation, IPSec can use pre-shared key authentication to verify identities of communication parties. After pre-shared key authentication is configured, the initiator encrypts data using the pre-shared key before transmitting the data, and the receiver decrypts the data using the same pre-shared key. If the receiver succeeds in data decryption, the initiator passes the identity verification.

Precautions

Both ends of IKE negotiation must be configured with the same pre-shared key.

Example

# Configure pre-shared key authentication in the Efficient VPN policy **evpn** and set the pre-shared key to YsHsjx_202206 in cipher text.

```
<HUAWEI> system-view
[HUAWEI] ipsec efficient-vpn evpn mode client
[HUAWEI-ipsec-efficient-vpn-evpn] pre-shared-key cipher YsHsjx_202206
```

10.3.36 re-authentication interval

Function

The **re-authentication interval** command sets the IKEv2 re-authentication interval.

The **undo re-authentication interval** command cancels the configuration.

By default, the device does not perform IKEv2 re-authentication.

Format

re-authentication interval *interval*

undo re-authentication interval

Parameters

Parameter	Description	Value
interval	Specifies the IKEv2 re-authentication interval. When about 70% of the time interval has elapsed, the device initiates IKEv2 re-authentication.	The value is an integer that ranges from 60 to 604800, in seconds.

Views

Efficient VPN policy view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In the remote access scenario, third-party attacks may occur during communications of peers. To improve IPSec network security, you can run this command to enable the peers to periodically re-authenticate each other.

Precautions

Only IKEv2 supports re-authentication.

Example

# Set the re-authentication interval to 400 seconds in the IPSec Efficient VPN policy.

```
<HUAWEI> system-view
[HUAWEI] ipsec efficient-vpn evpn mode client
[HUAWEI-ipsec-efficient-vpn-evpn] re-authentication interval 400
```

10.3.37 remote-address (Efficient VPN policy view)

Function

The **remote-address** command configures an IP address or domain name for the remote IKE peer during IKE negotiation.

The **undo remote-address** command deletes an IP address or domain name for the remote IKE peer during IKE negotiation.

By default, no IP address or domain name is configured for the remote IKE peer during IKE negotiation.

Format

remote-address { *ip-address* | **host-name** *host-name* } { **v1** | **v2** }

undo remote-address [*ip-address* | **host-name** *host-name*]

NOTE

The **v1** parameter is supported only when the WEAKEA plug-in is installed. For details about how to install the WEAKEA plug-in, see "WEAKEA Configuration" in the *CLI-based Configuration Guide*.

Parameters

Parameter	Description	Value
ip-address	Specifies the IP address of the remote IKE peer.	The value is in dotted decimal notation.
host-name *host-name*	Specifies the domain name of the remote IKE peer.	The value is an existing remote IKE peer domain name.
v1	Indicates that both ends use IKEv1.	-
v2	Indicates that both ends use IKEv2.	-

Views

Efficient VPN policy view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **remote-address** command configures an IP address or domain name for the remote IKE peer in an Efficient VPN policy. If the domain name is configured for the remote IKE peer, the IP address of the remote IKE peer is obtained in either of the following modes:

- Static mode: The IP address of the remote IKE peer is obtained based on the mapping between the domain name and IP address.
- Dynamic mode: The IP address of the remote IKE peer is obtained from the DNS server.

To improve network reliability, two devices can be deployed at the headquarters to connect to the branch gateway. In an Efficient VPN solution, two IP addresses or domain names of the remote IKE peer can be configured on the branch gateway. The branch gateway first attempts to use the first configured IP address or domain name to establish an IKE connection with the headquarters gateway. If establishing an IKE connection fails, the branch gateway uses the second IP address or domain name to establish an IKE connection.

Precautions

When you configure IP addresses or domain names for two remote IKE peers, ensure that the value type of **remote-address** and the IKE version are respectively the same. Generally, only one device is deployed at the headquarters to connect to the branch gateway. Therefore, only one remote address is configured.

Example

# Assign the IP addresses 10.1.1.1 and 10.1.2.1 to the remote peer in the Efficient VPN policy view.

```
<HUAWEI> system-view
[HUAWEI] ipsec efficient-vpn evpn mode client
[HUAWEI-ipsec-efficient-vpn-evpn] remote-address 10.1.1.1 v2
[HUAWEI-ipsec-efficient-vpn-evpn] remote-address 10.1.2.1 v2
```

# Set the domain name of the remote peer to **mypeer** in the Efficient VPN policy view.

```
<HUAWEI> system-view
[HUAWEI] ipsec efficient-vpn evpn mode client
[HUAWEI-ipsec-efficient-vpn-evpn] remote-address host-name mypeer v2
```

10.3.38 remote-id

Function

The **remote-id** command specifies the remote ID for IKE negotiation.

The **undo remote-id** command deletes the remote ID for IKE negotiation.

By default, the remote ID for IKE negotiation is not configured.

Format

remote-id *id*

undo remote-id

Parameters

Parameter	Description	Value
id	Specifies the remote ID.	The value is a string of 1 to 255 case-sensitive characters including special characters, such as the exclamation point (!), at sign (@), number sign (#), dollar sign ($), and percent (%).

Views

Efficient VPN policy view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If the remote ID type of the IKE peer is FQDN or USER-FQDN, you can run this command to set a value for the remote ID.

If the remote ID type of the IKE peer is DN, FQDN, or USER-FQDN, you can run this command to set a value for the remote ID.

During IKE negotiation, you can run the **remote-id** commands to configure the remote ID for authentication.

Precautions

- In IKEv1, the configured remote ID is used to authenticate only the peer.
- In IKEv2, the configured remote ID can be sent to the peer to check whether the local name of the peer is the same as this remote ID.

Example

# Set the remote peer name to **Huawei** in the Efficient VPN policy view.

```
<HUAWEI> system-view
[HUAWEI] ipsec efficient-vpn name mode client
[HUAWEI-ipsec-efficient-vpn-name] remote-id Huawei
```

10.3.39 reset ike error-info

Function

The **reset ike error-info** command clears information about IPSec tunnel negotiation failures using IKE.

Format

reset ike error-info

Parameters

None.

Views

User view

Default Level

3: Management level

Usage Guidelines

NOTICE

Statistics cannot be restored after being cleared.

You can run the **display ike error-info** command to view information about IPSec tunnel negotiation failures using IKE.

Example

# Clear information about IPSec tunnel negotiation failures using IKE.

```
<HUAWEI> reset ike error-info
```

10.3.40 reset ike offline-info

Function

The **reset ike offline-info** command clears information about deleted IPSec tunnels established through IKE negotiation.

Format

reset ike offline-info

Parameters

None.

Views

User view

Default Level

3: Management level

Usage Guidelines

NOTICE

Statistics cannot be restored after being cleared.

You can run the **display ike offline-info** command to check the reasons why IPSec tunnels established through IKE negotiation have been deleted.

Example

# Clear information about deleted IPSec tunnels established using IKE negotiation.

```
<HUAWEI> reset ike offline-info
```

10.3.41 reset ike sa

Function

The **reset ike sa** command clears information about SAs established through IKE negotiation.

Format

reset ike sa [**conn-id** *conn-id* | **remote** *ipv4-address*]

Parameters

Parameter	Description	Value
conn-id *conn-id*	Specifies the connection ID of an SA.	The value is an integer that ranges from 1 to 4294967295.
remote *ipv4-address*	Specifies the IPv4 address of the remote end.	The value is in dotted decimal notation.

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To clear an IPSec tunnel established through IKE negotiation, run the **reset ike sa** command to clear the IKE SA that is used to negotiate the IPSec tunnel.

There are two types of SAs established by IKE negotiation: IKE SAs in phase 1 and IPSec SAs in phase 2. IKE SAs in phase 1 are used for IKE negotiation. Under the protection of these IKE SAs, IPSec SAs in phase 2 are used to protect data flows.

- If the specified *conn-id* parameter corresponds to an IKE SA in phase 1, IKE peers do not automatically negotiate an IKE SA after the IKE SA is cleared. The IKE peers re-negotiate an IKE SA in phase 1 only when data flows match ACL rules in the IPSec policy again.
- If the specified *conn-id* parameter corresponds to an IPSec SA in phase 2, either of the following will occur:

  - Automatic triggering mode: The IKE peers re-negotiate an IPSec SA in phase 2 under the protection of the IKE SA in phase 1 after the IPSec SA is cleared.
  - Traffic-based triggering mode: The IKE peers do not automatically negotiate an IPSec SA after the IPSec SA is cleared. They re-negotiate an IPSec SA in phase 2 under the protection of the IKE SA in phase 1 only when data flows match ACL rules in the IPSec policy again.
- If the *conn-id* parameter is not specified, all IKE SAs in phase 1 are cleared, and IKE negotiation process is similar to that described above.

Precautions

After dependency between IPSec SA and IKE SA during IKEv1 negotiation is disabled using the **undo ikev1 phase1-phase2 sa dependent** command, running the **reset ike sa** *conn-id* command to delete an IKE SA will also delete the corresponding IPSec SA.

Example

# Clear IKE SAs in both phases.

```
<HUAWEI> reset ike sa
```

10.3.42 reset ike statistics

Function

The **reset ike statistics** command clears IKE statistics.

Format

reset ike statistics

Parameters

None.

Views

User view

Default Level

3: Management level

Usage Guidelines

NOTICE

Statistics cannot be restored after being cleared.

To diagnose and locate faults of IPSec tunnels established using IKE, you can collect IKE statistics in a given period of time. You can run the **reset ike statistics** command to clear historical IKE statistics before starting statistics collection. You can then run the **display ike statistics** command to check IKE statistics.

Example

# Clear IKE statistics.

```
<HUAWEI> reset ike statistics
```

10.3.43 reset ipsec history record

Function

The **reset ipsec history record** command clears history information about IPSec tunnels.

Format

reset ipsec history record

Parameters

None.

Views

User view

Default Level

3: Management level

Usage Guidelines

NOTICE

Statistics cannot be restored once being cleared.

You can run the **display ipsec history record** command to view history information about the current IPSec tunnel.

Example

# Clear history information about IPSec tunnels.

```
<HUAWEI> reset ipsec history record
```

10.3.44 reset ipsec sa

Function

The **reset ipsec sa** command deletes IPSec SAs.

Format

reset ipsec sa [**remote** *ipv4-address* | **parameters** *ipv4-address* **esp** *spi* | **efficient-vpn** *efficient-vpn-name*]

Parameters

Parameter	Description	Value
remote *ipv4-address*	Specifies the IPv4 address of the remote end.	The value is in dotted decimal notation.
parameters *ipv4-address* **esp** *spi*	Specifies the three elements that uniquely identify an IPSec SA. The three elements are *ipv4-address* (destination address), *protocol* (ESP), and Security Parameter Index (SPI). To reset an SA, the three elements must be specified.	The three elements are described as follows: ● *ipv4-address*: IPv4 address. ● *protocol*: ESP. ● *spi*: an integer that ranges from 256 to 4294967295.
efficient-vpn *efficient-vpn-name*	Specifies the name of an Efficient VPN policy.	The value is an existing Efficient VPN policy name.

Views

User view

Default Level

3: Management level

Usage Guidelines

When you run the **reset ipsec sa** command to delete IPSec SAs, note the following points:

- If no parameter is specified, all IPSec SAs are deleted.
- If **parameters** is specified, the IPSec SAs in two directions are deleted simultaneously.
- To delete IPSec SAs established through IKE negotiation, you must run the **reset ipsec sa** and **reset ike sa** commands in sequence. Otherwise, IPSec SAs established through IKE negotiation fail to be deleted. After the IPSec SAs are deleted, IKE peers re-negotiate IPSec SAs only when packets trigger IKE negotiation.

Example

# Delete the IPSec SA created through Efficient VPN policy **evpn**.

```
<HUAWEI> reset ipsec sa efficient-vpn evpn
```

10.3.45 reset ipsec packet statistics

Function

The **reset ipsec packet statistics** command deletes statistics about IPSec packets.

Format

reset ipsec packet statistics

Parameters

None.

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

Before collecting statistics about IPSec packets within a given period of time, run this command to delete existing statistics.

Precautions

The deleted statistics about IPSec packets cannot be restored. Exercise caution when you run this command.

Example

# Delete statistics about all IPSec packets.

```
<HUAWEI> reset ipsec packet statistics
```

10.3.46 sa binding vpn-instance (Efficient VPN policy view)

Function

The **sa binding vpn-instance** command binds a VPN instance to an IPSec tunnel.

The **undo sa binding vpn-instance** command unbinds a VPN instance from an IPSec tunnel.

By default, no VPN instance is bound to an IPSec tunnel.

Format

sa binding vpn-instance *vpn-instance-name*

undo sa binding vpn-instance

Parameters

Parameter	Description	Value
vpn-instance-name	Specifies the name of the VPN instance bound to an IPSec tunnel.	The value is an existing VPN instance name.

Views

Efficient VPN policy view

Default Level

2: Configuration level

Usage Guidelines

Applicable environment

On an VPN with small VPN sites, if CEs and PEs are connected through the Internet but not leased lines, hosts connected to a CE can access resources on another VPN site only through the insecure Internet. To enhance access security, these hosts can connect to the backbone network of the VPN through an IPSec tunnel.

This command specifies the VPN that the remote end of the IPSec tunnel belongs to. The tunnel initiator then can obtain the outbound interface and send packets through the outbound interface.

Prerequisites

A VPN instance has been created using the **ip vpn-instance** command.

A route distinguisher (RD) for the VPN instance has been configured using the **route-distinguisher** command.

Example

# Bind the VPN instance **vpna** to the Efficient VPN policy **evpn**.

```
<HUAWEI> system-view
[HUAWEI] ip vpn-instance vpna
[HUAWEI-vpn-instance-vpna] ipv4-family
[HUAWEI-vpn-instance-vpna-af-ipv4] route-distinguisher 100:1
[HUAWEI-vpn-instance-vpna-af-ipv4] vpn-target 100:100
[HUAWEI-vpn-instance-vpna-af-ipv4] quit
```

```
[HUAWEI-vpn-instance-vpna] quit
[HUAWEI] ipsec efficient-vpn evpn mode client
[HUAWEI-ipsec-efficient-vpn-evpn] sa binding vpn-instance vpna
```

10.3.47 security acl

Function

The **security acl** command specifies an ACL to be referenced in an IPSec policy or IPSec policy template.

The **undo security acl** command cancels the configuration.

By default, an IPSec policy or IPSec policy template does not reference an ACL.

Format

security acl *acl-number*

undo security acl

Parameters

Parameter	Description	Value
acl-number	Specifies the number of an ACL.	The value is an integer that ranges from 3000 to 3999.

Views

Efficient VPN policy view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **security acl** command references an ACL that defines data flows to be protected by IPSec. In practice, you need to configure rules in an ACL to define data flows to be protected and apply the ACL to an IPSec policy to protect the data flows.

When an IPSec policy is created using an IPSec policy template, you can determine whether to define data flows to be protected by IPSec on the responder.

- If data flows to be protected by IPSec are not specified on the responder, the responder accepts the range of data flows to be protected by IPSec defined on the initiator.
- If data flows to be protected by IPSec are specified on the responder, the configuration on the responder must mirror that on the initiator or the range

of protected data flows on the responder must contain the range of protected data flows on the initiator.

Precautions

To reference an ACL in an IPSec policy, ensure that rules must be configured in this ACL view and the number of rules configured in this ACL view does not exceed 32. Otherwise, this ACL cannot be referenced in this IPSec policy.

Example

# Reference ACL 3101 in an Efficient VPN policy.

```
<HUAWEI> system-view
[HUAWEI] acl number 3101
[HUAWEI-acl-adv-3101] rule permit tcp source 10.1.1.1 0.0.0.0 destination 10.1.1.2 0.0.0.0
[HUAWEI-acl-adv-3101] quit
[HUAWEI] ipsec efficient-vpn name mode network
[HUAWEI-ipsec-efficient-vpn-name] security acl 3101
```

10.3.48 service-scheme (Efficient VPN policy view)

Function

The **service-scheme** command configures a server-end service scheme in an Efficient VPN policy.

The **undo service-scheme** command deletes a server-end service scheme from an Efficient VPN policy.

By default, no server-end service scheme is configured in an Efficient VPN policy.

Format

service-scheme *service-scheme-name*

undo service-scheme

Parameters

Parameter	Description	Value
service-scheme-name	Specifies the name of a service scheme on the server end.	The service scheme name must already exist.

Views

Efficient VPN policy view

Default Level

2: Configuration level

Usage Guidelines

In an Efficient VPN scenario, the customer wants to deploy network resources including the DNS domain name, DNS server address, WINS server address, and IP addresses on the server end (headquarters gateway). The server end pushes network resource information to remote ends (branch gateways) to simplify configuration and maintenance of network resources on them.

Remote ends are authorized based on network resource information pushed by the server end or the server-end AAA service scheme specified in an Efficient VPN policy. To use the AAA service scheme, run the **service-scheme** command to configure a server-end service scheme in an Efficient VPN policy and run the **local-id-type** command to specify the **key-id** parameter. Otherwise, the configuration does not take effect.

Example

# Configure the server-end service scheme **service** in an Efficient VPN policy.

```
<HUAWEI> system-view
[HUAWEI] ipsec efficient-vpn name mode network
[HUAWEI-ipsec-efficient-vpn-name] service-scheme service
```

10.3.49 tunnel local

Function

The **tunnel local** command specifies the local address of an IPSec tunnel.

The **undo tunnel local** command cancels the configuration.

By default, no local IP address is configured for the IPSec tunnel.

Format

tunnel local { *ipv4-address* | **applied-interface** }

undo tunnel local

Parameters

Parameter	Description	Value
ipv4-address	Specifies an IPv4 address for the local end of an IPSec tunnel.	The value is in dotted decimal notation.
applied-interface	Indicates the primary IP address of the IPSec-enabled interface is used as the local address of an IPSec tunnel.	-

Views

Efficient VPN policy view

Default Level

2: Configuration level

Usage Guidelines

You can run this command to specify a start point for an IPSec tunnel.

You do not need to configure an IP address for the local end of an IPSec tunnel. During SA negotiation, the device will select a proper address based on route information. The local address needs to be configured in the following situations:

- If the IP address of the interface to which an IPSec policy is applied varies or is unknown, run the **tunnel local** *ipv4-address* command to specify the IP address of another interface (such as the loopback interface) on the device as the IP address for the local end of an IPSec tunnel. Otherwise, run the **tunnel local applied-interface** command to specify the IP address of the interface to which an IPSec policy is applied as the local address of an IPSec tunnel.
- If the interface to which an IPSec policy is applied has multiple IP addresses (one primary IP address and several secondary IP addresses), run the **tunnel local** *ipv4-address* command to specify one of these IP addresses as the IP address for the local end of an IPSec tunnel. Otherwise, run the **tunnel local applied-interface** command to specify the primary IP address of the interface as the local address of an IPSec tunnel.
- If equal-cost routes exist between the local and remote ends, run the **tunnel local** command to specify a local IP address for an IPSec tunnel.

Example

# Set the primary IP address of the interface to which the Efficient VPN policy in IKE negotiation mode is applied as the local IP address of the IPSec tunnel.

```
<HUAWEI> system-view
[HUAWEI] ipsec efficient-vpn name mode network
[HUAWEI-ipsec-efficient-vpn-name] tunnel local applied-interface
```

10.4 BGP/MPLS IP VPN Configuration Commands

10.4.1 Command Support

- Only the following switch models support working as a PE:

  S5731-H, S5731S-H, S5732-H, S5731-S, S6730-S, S6720-EI, S6720S-EI, S6730S-H, and S6730-H
- S1720GW-E and S1720GWR-E switches support working as an MCE. All models of S300, S500, S2700, S5700, and S6700 series switches (except the S5731-L and S5731S-L) support working as an MCE.

10.4.2 apply tunnel-policy (tunnel-selector view)

Function

The **apply tunnel-policy** command applies a tunnel policy to routes filtered by the **if-match** clause.

The **undo apply tunnel-policy** command cancels the setting.

By default, no tunnel policy is configured for filtered routes.

Format

apply tunnel-policy *tunnel-policy-name*

undo apply tunnel-policy

Parameters

Parameter	Description	Value
tunnel-policy-name	Specifies the name of a tunnel policy to be applied to the routes that match the **if-match** clause.	The value is a string of 1 to 39 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Views

Tunnel selector view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In BGP/MPLS IP VPN networking, by default, LSPs are selected for VPNv4 and BGP labeled routes without performing load balancing. If you want to select other types of tunnels or configure load balancing for VPNv4 or BGP labeled routes, run the **apply tunnel-policy** command to apply a tunnel policy. The **apply tunnel-policy** command can be used in the following situations:

- The RR on the backbone network of a VPN needs to apply a tunnel policy to VPNv4 routes learned from PEs.

If you want to apply a tunnel policy to only specific VPNv4 or BGP labeled routes in the situations mentioned above, first use the **if-match** clause to filter routes. The **if-match** commands that can be used are listed below:

- **if-match ip next-hop (tunnel-selector view)**

  The command filters IPv4 routes by next hop.
- **if-match ipv6 next-hop (tunnel-selector view)**

  The command filters IPv6 routes by next hop.
- **if-match rd-filter**

  The command filters routes by RD.

Prerequisite

The **tunnel-selector** command is run to create a tunnel selector; **if-match** clauses are configured as needed.

Follow-up Procedure

If the tunnel policy specified in the **apply tunnel-policy** command does not exist in the system, run the **tunnel-policy** command to create the tunnel policy.

Example

# Select policy1 for the VPN routes that are filtered by RD in the tunnel selector view.

```
<HUAWEI> system-view
[HUAWEI] tunnel-policy policy1
[HUAWEI-tunnel-policy-policy1] tunnel select-seq cr-lsp lsp load-balance-number 1
[HUAWEI-tunnel-policy-policy1] quit
[HUAWEI] tunnel-selector tps permit node 10
[HUAWEI-tunnel-selector] if-match rd-filter 1
[HUAWEI-tunnel-selector] apply tunnel-policy policy1
```

10.4.3 apply-label per-instance

Function

The **apply-label per-instance** command sets the label allocation mode to one label per instance. In this mode, all the routes of the VPN instance address family destined for the remote PE are assigned the same label.

The **undo apply-label per-instance** command restores the default configuration.

By default, the VPN instance address family assigns the same label to all routes to be sent to the peer PE.

Format

apply-label per-instance

undo apply-label per-instance

Parameters

None

Views

VPN instance view, VPN instance IPv4 address family view, VPN instance IPv6 address family view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In BGP/MPLS IP VPN networking, if VPN routes on PE are numerous but MPLS label resources are insufficient, the **apply-label per-instance** command can be run to minimize MPLS label consumption on PE.

When a large number of routes of the VPN instance IPv4 address family need to apply for labels, the **apply-label per-instance** command saves label resources of PEs and lowers the requirements for PE capacities.

By default, the system applies for a label for each route in a VPN instance enabled with the IPv4 or IPv6 address family. After the **apply-label per-instance** command is run in the IPv4 or IPv6 address family view of the VPN instance, the routes of the VPN instance enabled with the corresponding address family will be allocated the same label. For example, a PE is configured with two VPN instances that have 20000 routes in total. By default, 20000 MPLS labels will be allocated to the routes. If the **apply-label per-instance** command is run, only two MPLS labels will be allocated to the routes.

You can run the **display fib statistics** command to check the number of VPN routes.

Prerequisites

1. The **ip vpn-instance** command has been executed to create a VPN instance and enter the VPN instance view.
2. The **ipv4-family** or **ipv6-family** command has been executed to enter the IPv4 or IPv6 VPN instance address family view.
3. The **route distinguisher** command has been executed to set the RD of the VPN instance.

Precautions

The change of the label allocation mode leads to the re-advertising of VPN routes. The services may be interrupted temporarily. Therefore, use the **apply-label per-instance** and **undo apply-label per-instance** commands with caution.

NOTE

If there are a large number of VPN routes in the system, frequently executing this command will cause flapping of many routes. Route flapping results in a high CPU usage but does not affect real-time services in the system.

Example

# Assign one label to all routes of the IPv4 address family of the VPN instance named vpn1.

```
<HUAWEI> system-view
[HUAWEI] ip vpn-instance vpn1
[HUAWEI-vpn-instance-vpn1] ipv4-family
[HUAWEI-vpn-instance-vpn1-af-ipv4] route-distinguisher 100:1
[HUAWEI-vpn-instance-vpn1-af-ipv4] apply-label per-instance
```

10.4.4 apply-label per-nexthop

Function

The **apply-label per-nexthop** command enables the ASBR to allocate labels for IPv4 VPN routes or IPv6 VPN routes based on the next hop.

The **undo apply-label per-nexthop** command disables the ASBR from allocating labels for IPv4 VPN routes or IPv6 VPN routes based on the next hop.

By default, next-hop-based label allocation for VPN routes is disabled on the ASBR, and a label is allocated to each VPN instance.

Format

apply-label per-nexthop

undo apply-label per-nexthop

Parameters

None

Views

BGP-VPNv4 address family view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In inter-AS VPN Option B or HoVPN networking, if MPLS label resources on the ASBR or SPE are insufficient for the advertised VPNv4 or VPNv6 routes to use, the **apply-label per-nexthop** command can be run to minimize MPLS label consumption on the ASBR or SPE.

By default, the ASBR or SPE allocates a label to each VPNv4 or VPNv6 route when advertising it to an MP-BGP peer. If the **apply-label per-nexthop** command is run, the ASBR or SPE will allocate one label to all the routes with the same next hop and outgoing label. To make the routes learned from the same next hop have the same outgoing label, run the **apply-label per-instance** command on the PE. Otherwise, the effect of the **apply-label per-nexthop** command will be affected.

Configuration Impact

After next-hop-based label allocation is enabled or disabled, the label allocated by the ASBR to a route changes, which leads to a transient loss of VPN packets.

Example

# In the BGP-VPNv4 view, enable the ASBR to allocate labels to IPv4 VPN routes based on the next hop.

```
<HUAWEI> system-view
[HUAWEI] bgp 100
[HUAWEI-bgp] ipv4-family vpnv4
[HUAWEI-bgp-af-vpnv4] apply-label per-nexthop
```

10.4.5 apply-label per-route

Function

The **apply-label per-route** command enables the one-label-per-route mode. The VPN instance address family assigns a unique label to each route to be sent to the peer PE.

The **undo apply-label per-route** command disables the one-label-per-route mode.

By default, the VPN instance address family assigns the same label to all routes to be sent to the peer PE.

Format

apply-label per-route

undo apply-label per-route

Parameters

None

Views

VPN instance view, VPN instance IPv4 address family view, VPN instance IPv6 address family view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If you want to change the label allocation mode from one-label-per-instance to one-label-per-route, run the **apply-label per-route** command.

Prerequisite

The **route-distinguisher** command is run to configure an RD for the VPN instance enabled with the IPv4 or IPv6 address family.

Configuration Impact

The change of the label allocation mode leads to the re-advertising of VPN routes. The services may be interrupted temporarily. Exercise caution when running the **apply-label per-route** or **undo apply-label per-route** command.

The **apply-label per-instance** and **apply-label per-route** commands are mutually exclusive. If both commands are run, the latest configuration overrides the previous one.

Example

# Enable the one-label-per-route mode for routes of **vpn1**.

```
<HUAWEI> system-view
[HUAWEI] ip vpn-instance vpn1
[HUAWEI-vpn-instance-vpn1] ipv4-family
[HUAWEI-vpn-instance-vpn1-af-ipv4] route-distinguisher 100:1
[HUAWEI-vpn-instance-vpn1-af-ipv4] apply-label per-route
```

10.4.6 arp vpn-cross enable

Function

The **arp vpn-cross enable** command enables direct ARP entry delivery for mutual access between local VPNs.

The **undo arp vpn-cross enable** command disables direct ARP entry delivery for mutual access between local VPNs.

By default, direct ARP entry delivery is disabled for mutual access between local VPNs.

NOTE

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

Format

arp vpn-cross enable

undo arp vpn-cross enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The initial traffic between two local VPNs triggers ARP Miss messages and ARP learning. If a PE device fails to timely process the ARP Miss messages due to some reasons, mutual access traffic between the VPNs cannot be transmitted.

After direct ARP entry delivery is enabled on the PE device, the PE device delivers ARP entries before the mutual access traffic triggers ARP Miss messages and ARP learning. This ensures normal traffic transmission between local VPNs.

Precautions

ARP entry delivery before triggering of ARP Miss messages and ARP learning consumes ARP entries. Configure this command only when required.

Example

# Enable direct ARP entry delivery for mutual access between local VPNs.

```
<HUAWEI> system-view
[HUAWEI] arp vpn-cross enable
Warning: After this function is enabled, a large number of ARP entries will be occupied.
```

10.4.7 as-number

Function

The **as-number** command configures an AS number for a VPN instance.

The **undo as-number** command restores the default setting.

By default, a VPN instance uses the AS number of BGP.

Format

as-number { *as-number-plain* | *as-number-dot* }

undo as-number

Parameters

Parameter	Description	Value
as-number-plain	Integral AS number	The value is an integer ranging from 1 to 4294967295.
as-number-dot	AS number in dotted notation	The value is in the format of *x.y*, where *x* and *y* are integers that range from 1 to 65535 and from 0 to 65535, respectively.

Views

BGP-VPN instance IPv4 address family view, BGP-VPN instance IPv6 address family view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

During network transfer or service identification, a device needs to be simulated as multiple BGP devices logically. In this case, you can run the **as-number** command to configure an AS number for each VPN instance.

After the **as-number** command is used:

- BGP peer relationships in the VPN instance are established by using the configured AS number.
- The configured AS number is used to generate the aggregator attribute during route aggregation.
- When advertising routes to an EBGP peer, the local device carries the AS number configured in the VPN instance.

Prerequisites

If a BGP peer or a BGP peer group is configured in the VPN instance, you need to delete the configuration of the BGP peer or peer group before configuring or deleting an AS number.

Precautions

A VPN instance configured with an AS number cannot be configured with BGP confederation. Conversely, a VPN instance configured with BGP confederation cannot be configured with an AS number.

NOTE

The AS number configured in the BGP-VPN instance view cannot be the same as the AS number configured in the BGP view.

Example

# Set the AS number of the VPN instance named **vpna** to 65001.

```
<HUAWEI> system-view
[HUAWEI] bgp 100
[HUAWEI-bgp] ipv4-family vpn-instance vpna
[HUAWEI-bgp-vpna] as-number 65001
```

10.4.8 auto-frr

Function

The **auto-frr** command enables BGP Auto FRR.

The **undo auto-frr** command disables BGP Auto FRR.

By default, BGP Auto FRR is disabled.

Format

auto-frr

undo auto-frr

Parameters

None

Views

BGP-VPN instance IPv4 address family view, BGP-VPN instance IPv6 address family view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

This function is applicable to networks that require a low packet loss ratio and a short delay.

Using BGP Auto FRR together with BFD is recommended. They can rapidly detect a link fault and switch traffic to a standby link if a fault occurs.

Example

# Enable BGP Auto FRR for unicast routes.

```
<HUAWEI> system-view
[HUAWEI] bgp 100
[HUAWEI-bgp] ipv4-family vpn-instance vpna
[HUAWEI-bgp-vpna] auto-frr
```

10.4.9 auto-frr (BGP-VPNv4 address family view)

Function

The **auto-frr** command enables VPNv4 FRR.

The **undo auto-frr** command restores the default configuration.

By default, VPNv4 FRR is disabled.

Format

auto-frr

undo auto-frr

Parameters

None.

Views

BGP-VPNv4 address family view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Running the **auto-frr** command in the BGP-VPNv4 address family view enables VPNv4 FRR and improves network reliability. After VPNv4 FRR is configured, traffic can be switched to the backup LSP (Label Switched Path) immediately after the primary LSP to which a VPNv4 route recurses becomes faulty. VPNv4 FRR applies to HVPN scenarios.

- In an HVPN scenario, VPNv4 FRR is deployed on SPEs.

Prerequisites

BGP has been enabled.

Precautions

If used with BFD, VPNv4 FRR can rapidly detect link faults and switch services to the standby link for transmission.

Do not configure the **apply-label per-nexthop** command in the BGP-VPNv4 address family view if VPNv4 FRR is enabled, or VPNv4 FRR will fail to take effect.

If the **auto-frr** command is configured in the BGP-VPNv4 address family view, the **bestroute nexthop-resolved tunnel** command must also be configured, so that packets will not get lost during traffic switchback.

Example

# Enable VPNv4 FRR.

```
<HUAWEI> system-view
[HUAWEI] bgp 100
[HUAWEI-bgp] ipv4-family vpnv4
[HUAWEI-bgp-af-vpnv4] auto-frr
```

10.4.10 description (VPN instance view)

Function

The **description** command specifies the description of the current VPN instance.

The **undo description** command deletes the description of the current VPN instance.

By default, no description is specified for a VPN instance.

Format

description *description-information*

undo description

Parameters

Parameter	Description	Value
description-information	Specifies the description of a VPN instance.	The value is a string of 1 to 242 case-sensitive characters with spaces.

Views

VPN instance view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To record the purpose of creating a VPN instance and the CEs with which the VPN instance is associated, you can run the **description** command to specify the description of the VPN instance.

To check the description of a VPN instance, run the **display ip vpn-instance** command.

Precautions

If you run the **description** command several times, the latest configuration overrides the previous configurations.

Example

# Specify the description of a VPN instance named vpn1.

```
<HUAWEI> system-view
[HUAWEI] ip vpn-instance vpn1
[HUAWEI-vpn-instance-vpn1] description OnlyForAB
```

10.4.11 description (tunnel interface view)

Function

The **description** command sets the description of the current tunnel interface.

The **undo description** command deletes the description of the current tunnel interface.

By default, a tunnel interface does not have a description.

Format

description *text*

undo description

Parameters

Parameter	Description	Value
text	Specifies the description of a tunnel interface.	The value is a string of 1 to 242 case-sensitive characters, with spaces supported.

Views

Tunnel interface view

Default Level

2: Configuration level

Usage Guidelines

After using the **interface tunnel** command to create a tunnel interface, you can run the **description** command to configure a description of the tunnel interface to facilitate later query.

To check the description of a tunnel interface, run the **display this interface** command in the tunnel interface view or the **display interface tunnel** command.

Example

# Configure the description of Tunnel 1.

```
<HUAWEI> system-view
[HUAWEI] interface tunnel 1
[HUAWEI-Tunnel1] description This is a tunnel from 10.1.1.1 to 10.2.2.2
```

# Delete the description of Tunnel 1.

```
<HUAWEI> system-view
[HUAWEI] interface tunnel 1
[HUAWEI-Tunnel1] undo description
```

10.4.12 description (tunnel-policy view)

Function

The **description** command configures the description of the current tunnel policy.

The **undo description** command cancels the setting.

By default, a tunnel policy does not have a description.

Format

description *description-information*

undo description

Parameters

Parameter	Description	Value
description-information	Specifies the description of the tunnel policy.	The value is a string of 1 to 80 case-sensitive characters with spaces.

Views

Tunnel policy view

Default Level

2: Configuration level

Usage Guidelines

After using the **tunnel-policy** command to create a tunnel policy, you can run the **description** command to configure a description of the tunnel policy to facilitate later query.

To check tunnel policy configurations, run the **display tunnel-policy-config** command.

Example

# Configure the description of the tunnel policy named test1.

```
<HUAWEI> system-view
[HUAWEI] tunnel-policy test1
[HUAWEI-tunnel-policy-test1] description two TE tunnels are used
```

10.4.13 destination

Function

The **destination** command specifies the destination IP address of a tunnel interface.

The **undo destination** command deletes the destination IP address of a tunnel interface.

By default, no destination address is configured.

Format

destination [**vpn-instance** *vpn-instance-name*] *dest-ip-address*

undo destination

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Specifies the name of the VPN instance that the destination address of a tunnel belongs to. When the tunnel interface uses GRE, you can specify **vpn-instance** *vpn-instance-name*.	The value is the name of an existing VPN instance.
dest-ip-address	Specifies the destination IP address of a tunnel interface.	The IPv4 address is in dotted decimal notation. The IPv6 address is a 32-digit hexadecimal number, in the format X:X:X:X:X:X:X:X.

Views

Tunnel interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When configuring a GRE, MPLS TE, IPv4 over IPv6 tunnel or manual IPv6 over IPv4 tunnel, create a tunnel interface. After a tunnel interface is created, run the **destination** command to specify the destination IP address for the tunnel interface.

When using the **destination** command on a PE to specify the destination address of a GRE tunnel bound for a CE, you need to set **vpn-instance** *vpn-instance-name* in the command to specify the name of the VPN instance to which the destination address belongs.

Prerequisites

A tunnel interface has been created using the **interface tunnel** command, and the encapsulation mode is set to GRE, MPLS TE, IPv4 over IPv6 or IPv6 over IPv4 of manual mode using the **tunnel-protocol** command.

Precautions

Two tunnel interfaces with the same encapsulation mode, source address, and destination address cannot be configured simultaneously.

You can configure a main interface working in Layer 3 mode as the source tunnel interface.

On the GRE, MPLS TE, IPv4 over IPv6 tunnel or manual IPv6 over IPv4 tunnel, the destination address of the local tunnel interface is the source address of the remote tunnel interface, and the source address of the local tunnel interface is the destination address of the remote tunnel interface.

Example

# Establish a manual IPv6 over IPv4 tunnel between VLANIF 10 at 10.1.1.1 on switch HUAWEI1 and VLANIF 20 at 10.2.1.1 on switch HUAWEI2.

```
<HUAWEI1> system-view
[HUAWEI1] interface tunnel 1
[HUAWEI1-Tunnel1] tunnel-protocol ipv6-ipv4
[HUAWEI1-Tunnel1] source 10.1.1.1
[HUAWEI1-Tunnel1] destination 10.2.1.1
<HUAWEI2> system-view
[HUAWEI2] interface tunnel 1
[HUAWEI2-Tunnel1] tunnel-protocol ipv6-ipv4
[HUAWEI2-Tunnel1] source 10.2.1.1
[HUAWEI2-Tunnel1] destination 10.1.1.1
```

# Set the destination address of the GRE tunnel Tunnel1 to 10.1.1.1 that belongs to vpn1.

```
<HUAWEI> system-view
[HUAWEI] ip vpn-instance vpn1
[HUAWEI-vpn-instance-vpn1] ipv4-family
[HUAWEI-vpn-instance-vpn1-af-ipv4] route-distinguisher 100:1
[HUAWEI-vpn-instance-vpn1-af-ipv4] quit
[HUAWEI-vpn-instance-vpn1] quit
[HUAWEI] interface tunnel 1
[HUAWEI-Tunnel1] tunnel-protocol gre
[HUAWEI-Tunnel1] destination vpn-instance vpn1 10.1.1.1
```

10.4.14 display default-parameter l3vpn

Function

The **display default-parameter l3vpn** command displays the default configuration of L3VPN during initialization.

Format

display default-parameter l3vpn

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Scenario

You can run this command to check the default configuration of L3VPN during initialization, for example, default label allocation mode in a VPN instance.

Precautions

This command displays only the default configuration of L3VPN during initialization. The command output shows the default configuration of L3VPN during initialization even when the default configuration is changed.

Example

# Display the default configuration of L3VPN during initialization.

```
<HUAWEI> display default-parameter l3vpn
 Apply label mode         :
    IPv4-family           : label per instance
    IPv6-family           : label per instance
```

Table 10-29 Description of the display default-parameter l3vpn command output

Item	Description
Apply label mode	Default label allocation mode.
IPv4-family	IPv4 address family.
IPv6-family	IPv6 address family.
label per instance	The default label allocation mode is label per instance.

10.4.15 display ip prefix-limit statistics

Function

The **display ip prefix-limit statistics** command displays the statistics of the prefix limits of VPN instances.

Format

display ip prefix-limit { **all-vpn-instance** | **vpn-instance** *vpn-instance-name* } **statistics**

Parameters

Parameter	Description	Value
all-vpn-instance	Indicates all VPN instances.	-
vpn-instance *vpn-instance-name*	Specifies the name of a VPN instance.	The value is the name of an existing VPN instance.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display ip prefix-limit statistics** command to view the number of times that a protocol re-adds or deletes routes according to the prefix limit of a specified VPN instance.

Example

# Display the statistics of the prefix limits of all VPN instances.

```
<HUAWEI> display ip prefix-limit all-vpn-instance statistics
-------------------------------------------------------------------------------
VPN instance name: vrf1
          DenyAdd TryAddInDelState NotifyDelAll NotifyDelFinish NotifyAddRoute
DIRECT        0             0            0              0              0
STATIC        0             0            0              0              0
UNR           0             0            0              0              0
OSPF          0             0            0              0              0
IS-IS         0             0            0              0              0
RIP           0             0            0              0              0
BGP           0             0            0              0              0
MSR           0             0            0              0              0
-------------------------------------------------------------------------------
VPN instance name: vrf2
          DenyAdd TryAddInDelState NotifyDelAll NotifyDelFinish NotifyAddRoute
DIRECT        0             0            0              0              0
STATIC        0             0            0              0              0
UNR           0             0            0              0              0
OSPF          0             0            0              0              0
IS-IS         0             0            0              0              0
RIP           0             0            0              0              0
BGP           0             0            0              0              0
MSR           0             0            0              0              0
```

# Display the statistics of the prefix limit of the VPN instance named **vrf1**.

```
<HUAWEI> display ip prefix-limit vpn-instance vrf1 statistics
-------------------------------------------------------------------------------
VPN instance name: vrf2
          DenyAdd TryAddInDelState NotifyDelAll NotifyDelFinish NotifyAddRoute
DIRECT        0             0            0              0              0
STATIC        0             0            0              0              0
UNR           0             0            0              0              0
OSPF          0             0            0              0              0
IS-IS         0             0            0              0              0
RIP           0             0            0              0              0
BGP           0             0            0              0              0
MSR           0             0            0              0              0
```

Table 10-30 Description of the display ip prefix-limit statistics command output

Item	Description
DenyAdd	Number of routes that the protocol fails to add to the RIB because of the prefix limit.
TryAddInDelState	Number of routes that the protocol fails to add to the RIB because the RIB is in the process of deleting routes.
NotifyDelAll	Number of times that the RIB notifies the protocol of deleting routes when the prefix limit is decreased.
NotifyDelFinish	Number of times that the protocol notifies the RIB of completion of deleting routes.
NotifyAddRoute	Number of times that the RIB notifies the protocol of re-adding routes.

10.4.16 display ipv6 prefix-limit statistics

Function

The **display ipv6 prefix-limit statistics** command displays the statistics of the prefix limits of IPv6 VPN instances.

Format

display ipv6 prefix-limit { **all-vpn-instance** | **vpn-instance** *vpn-instance-name* } **statistics**

Parameters

Parameter	Description	Value
all-vpn-instance	Indicates all IPv6 VPN instances.	-
vpn-instance *vpn-instance-name*	Specifies the name of an IPv6 VPN instance.	The value is the name of an existing IPv6 VPN instance.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display ipv6 prefix-limit statistics** command to view the number of times that a protocol re-adds or deletes routes according to the prefix limit of a specified IPv6 VPN instance.

Example

# Display the statistics of the prefix limits of all IPv6 VPN instances.

```
<HUAWEI> display ipv6 prefix-limit all-vpn-instance statistics
------------------------------------------------------------------------------
IPv6 VPN instance name: vrf1
         DenyAdd TryAddInDelState NotifyDelAll NotifyDelFinish NotifyAddRoute
DIRECT        0              0           0              0             0
STATIC        0              0           0              0             0
UNR           0              0           0              0             0
OSPFv3        0              0           0              0             0
IS-IS         0              0           0              0             0
RIPng         0              0           0              0             0
BGP           0              0           0              0             0
------------------------------------------------------------------------------
IPv6 VPN instance name: vrf2
         DenyAdd TryAddInDelState NotifyDelAll NotifyDelFinish NotifyAddRoute
DIRECT        0              0           0              0             0
STATIC        0              0           0              0             0
UNR           0              0           0              0             0
OSPFv3        0              0           0              0             0
IS-IS         0              0           0              0             0
RIPng         0              0           0              0             0
BGP           0              0           0              0             0
```

# Display the statistics of the prefix limit of the IPv6 VPN instance named **vrf1**.

```
<HUAWEI> display ipv6 prefix-limit vpn-instance vrf1 statistics
------------------------------------------------------------------------------
IPv6 VPN instance name: vrf1
         DenyAdd TryAddInDelState NotifyDelAll NotifyDelFinish NotifyAddRoute
DIRECT        0              0           0              0             0
STATIC        0              0           0              0             0
UNR           0              0           0              0             0
OSPFv3        0              0           0              0             0
IS-IS         0              0           0              0             0
RIPng         0              0           0              0             0
BGP           0              0           0              0             0
```

Table 10-31 Description of the display ipv6 prefix-limit statistics command output

Item	Description
DenyAdd	Number of routes that the protocol fails to add to the RIB because of the prefix limit.
TryAddInDelState	Number of routes that the protocol fails to add to the RIB because the RIB is in the process of deleting routes.
NotifyDelAll	Number of times that the RIB notifies the protocol of deleting routes when the prefix limit is decreased.
NotifyDelFinish	Number of times that the protocol notifies the RIB of completion of deleting routes.

Item	Description
NotifyAddRoute	Number of times that the RIB notifies the protocol of re-adding routes.

10.4.17 display ip vpn-instance

Function

The **display ip vpn-instance** command displays configurations of VPN instances.

Format

display ip vpn-instance [**verbose**] [*vpn-instance-name*]

display ip vpn-instance [*vpn-instance-name*] **interface**

display ip vpn-instance [*vpn-instance-name*] **tunnel-info**

Parameters

Parameter	Description	Value
verbose	Displays detailed information about VPN instances.	-
vpn-instance-name	Specifies the name of a VPN instance.	The value is the name of an existing VPN instance.
interface	Displays information about the interfaces bound to the VPN instance.	-
tunnel-info	Displays information about the LSP associated with the VPN instance.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

If you want to check the configurations of VPN instances, interfaces bound to them, and LSPs associated with them, run the **display ip vpn-instance** command.

Since VPN instances support both IPv4 and IPv6 address families, the **display ip vpn-instance** command displays the information of different address families separately.

If *vpn-instance-name* is not specified, the **display ip vpn-instance** command displays information about all configured VPN instances on the device.

If **interface** is specified, the display ip vpn-instance command displays all interfaces bound to the specified VPN instance.

If **tunnel-info** is specified, the **display ip vpn-instance** command displays information about the LSPs to which the routes of the VPN instance enabled with the IPv4 or IPv6 address family recurse (in other words, information about the LSPs between PEs). If the tunnels between PEs are not LSPs, the **display ip vpn-instance** command does not display tunnel information.

Precautions

If the VPN instance to be displayed is not created, the system prompts that the VPN instance does not exist.

Example

# Display brief information about all VPN instances.

```
<HUAWEI> display ip vpn-instance
 Total VPN-Instances configured      : 2
 Total IPv4 VPN-Instances configured : 2
 Total IPv6 VPN-Instances configured : 0

  VPN-Instance Name               RD                    Address-family
  vpn1
  vpna                            100:1                 IPv4
  vpnb                            100:2                 IPv4
```

Table 10-32 Description of the display ip vpn-instance command output

Item	Description
Total VPN-Instances configured	Total number of VPN instances configured on the local end.
Total IPv4 VPN-Instances configured	Total number of locally configured VPN instances for which IPv4 address families are enabled.
Total IPv6 VPN-Instances configured	Total number of locally configured VPN instances for which IPv6 address families are enabled.
VPN-Instance Name	Name of the VPN instance.
RD	RD of the VPN instance IPv4 address family or IPv6 address family.

Item	Description
Address-family	Address family enabled for the VPN instance. The address family can be: ● Null, if no address family is enabled. ● IPv4, if only the IPv4 address family is enabled. ● IPv6, if only the IPv6 address family is enabled.

# Display detailed information about all VPN instances.

```
<HUAWEI> display ip vpn-instance verbose
 Total VPN-Instances configured      : 1
 Total IPv4 VPN-Instances configured : 1
 Total IPv6 VPN-Instances configured : 1

 VPN-Instance Name and ID : vpna, 6
  Description : vpna-1
  Service ID : 12
  Interfaces : Vlanif10
 Address family ipv4
  Create date : 2013-03-06 15:20:43+08:00
  Up time : 6 days, 04 hours, 41 minutes and 57 seconds
  Route Distinguisher : 100:1
  Export VPN Targets :  1:1
  Import VPN Targets :  1:1
  Label Policy : label per instance
  Per-Instance Label : 1024
  IP FRR Route Policy : 20
  VPN FRR Route Policy : 12
  Import Route Policy : 10
  Export Route Policy : 20
  Tunnel Policy : bindTE
  Maximum Routes Limit : 2000
  Threshold Routes Limit : 80%
  Maximum Prefixes Limit : 1024
  Threshold Prefixes Limit : 50%
  Install Mode : route-unchanged
  Log Interval : 10
 Address family ipv6
  Create date : 2013-03-06 15:20:43+08:00
  Up time : 6 days, 04 hours, 41 minutes and 57 seconds
  Log Interval : 5
```

Table 10-33 Description of the display ip vpn-instance verbose command output

Item	Description
Total VPN-Instances configured	Total number of VPN instances configured on the local end.
Total IPv4 VPN-Instances configured	Total number of locally configured VPN instances for which IPv4 address families are enabled.

Item	Description
Total IPv6 VPN-Instances configured	Total number of locally configured VPN instances for which IPv6 address families are enabled.
VPN-Instance Name and ID	Name and ID of the VPN instance. The ID is assigned by the system, which facilitates indexing.
Description	Description of the VPN instance. This field is displayed in the command output only when the **description (VPN instance view)**command is used.
Service ID	Service ID of the VPN instance. This item is displayed only after the **service-id (VPN instance view)** command is run in the VPN instance view.
Interfaces	Interfaces bound to the VPN instance. This field is displayed only after the **ip binding vpn-instance** command is configured on these interfaces.
Address family ipv4	Information about the IPv4 address family enabled for the VPN instance.
Address family ipv6	Information about the IPv6 address family enabled for the VPN instance.
Create date	Time when the VPN instance is created.
Up time	Period during which the VPN instance maintains in the Up state.
Route Distinguisher	RD of the VPN instance IPv4 address family or IPv6 address family. To specify an RD, run the **route-distinguisher** command.
Export VPN Targets	Route Target list in the outbound direction. To set the VPN target, run the **vpn-target** command.
Import VPN Targets	Route Target list in the inbound direction. To set the VPN target, run the **vpn-target** command.

Item	Description
Label Policy	Label policy: ● label per instance: indicates that the same label is allocated to routes of a VPN instance. This field is displayed in the command output only when the **apply-label per-instance** command is run in the VPN instance view. ● label per route: indicates that each route of a VPN instance is assigned a label.
Per-Instance Label	Label value used when all VPN routes of the VPN instance address family share one label. This field is displayed only after the **apply-label per-instance** command is run in the VPN instance address family view.
IP FRR Route Policy	IP FRR route policy used for the address family. This item is displayed only after the **ip frr** command is run in the VPN instance IPv4 address family view.
VPN FRR Route Policy	VPN FRR route policy used for the address family. This item is displayed only after the **vpn frr** command is run in the VPN instance IPv4 address family view.
Import Route Policy	Import Route-Policy applied to the VPN instance. This field is displayed only after the **import route-policy** command is run in the VPN instance address family view.
Export Route Policy	Export Route-Policy applied to the VPN instance. This field is displayed only after the **export route-policy** command is run in the VPN instance address family view.
Tunnel Policy	Tunnel policy applied to the VPN instance. This field is displayed only after the **tnl-policy** command is run in the VPN instance address family view.

Item	Description
Maximum Routes Limit	Maximum number of routes supported by the current address family. This field is displayed only after the **routing-table limit** command is run in the VPN instance address family view.
Threshold Routes Limit	Percentage of the maximum number of routes specified for the current address family. When the maximum number of routes reaches the percentage threshold, an alarm is generated. This field is displayed only after the **routing-table limit** command is run in the VPN instance address family view.
Maximum Prefixes Limit	Maximum number of prefixes supported by the current address family of the VPN instance. This field is displayed only after the **prefix limit** command is run in the VPN instance address family view.
Threshold Prefixes Limit	Percentage of the maximum number of prefixes specified for the current address family of the VPN instance. When the maximum number of prefixes reaches the percentage threshold, an alarm is generated. This field is displayed only after the **prefix limit** command is run in the VPN instance address family view.
Install Mode	Method of processing routes. The **prefix limit** command can be used to specify the route processing method when the threshold is lowered due to the number of route prefixes exceeding the upper threshold. ● If **route-unchanged** is configured, routes in the routing information base (RIB) table remain unchanged. ● If **route-unchanged** is not configured, all routes in the RIB table are deleted and the routes are re-installed in the RIB table.

Item	Description
Log Interval	Interval for displaying log messages when the number of VPN instance routes exceeds the maximum value. The default interval is 5 seconds. The value can be set by the command **limit-log-interval**.

# Display information about the interface bound to the VPN instance named **vrf1**.

```
<HUAWEI> display ip vpn-instance vrf1 interface
 VPN-Instance Name and ID : vrf1, 1
  Interface Number : 1
  Interface list : Vlanif40
```

Table 10-34 Description of the display ip vpn-instance interface command output

Item	Description
Interface Number	Number of interfaces bound to the VPN instance
Interface list	List of interfaces bound to the VPN instance

# Display information about the LSP associated with the vrf1 VPN instance.

```
<HUAWEI> display ip vpn-instance vrf1 tunnel-info
 VPN-Instance Name and ID : vrf1, 1
 Address family ipv4
  Nexthop Address              Tunnel ID
  1.1.1.1                  0x3
 Address family ipv6
  Nexthop Address              Tunnel ID
  1.1.1.1                  0x3
```

Table 10-35 Description of the display ip vpn-instance tunnel-info command output

Item	Description
Nexthop Address	Indicates the next-hop address of the route learned by the VPN instance from the peer PE.
Tunnel ID	Indicates the ID of the LSP corresponding to the next-hop address of the route learned by the VPN instance from the peer PE.

10.4.18 display ip vpn-instance import-vt

Function

The **display ip vpn-instance import-vt** command displays all VPN instances with the specified import vpn-target attribute.

Format

display ip vpn-instance import-vt *ivt-value*

Parameters

Parameter	Description	Value
ivt-value	Specifies the value of the import VPN-target attribute. The forms of VPN targets are as follows: ● 2-byte AS number: 4-byte user-defined number, for example, 1:3. The AS number ranges from 0 to 65535. The user-defined number ranges from 0 to 4294967295. The AS number and the user-defined number cannot both be 0. That is, a VPN target cannot be 0:0. ● IPv4-address: 2-byte user-defined number, for example, 192.168.122.15:1. The IP address ranges from 0.0.0.0 to 255.255.255.255. The user-defined number ranges from 0 to 65535. ● Integral 4-byte AS number:2-byte user-defined number, for example, 65537:3. An AS number ranges from 65536 to 4294967295. A user-defined number ranges from 0 to 65535. The AS number and user-defined number cannot be both 0s. That is, a VPN target cannot be 0:0. ● 4-byte AS number in dotted notation:2-byte user-defined number, for example, 0.0:3 or 0.1:0. A 4-byte AS number in dotted notation is in the format of *x.y*, where *x* and *y* are integers that range from 0 to 65535 and from 0 to 65535, respectively. A user-defined number ranges from 0 to 65535. The AS number and user-defined number cannot be both 0s. That is, a VPN target cannot be 0.0:0.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

If a PE is configured with multiple VPN instances, the **display ip vpn-instance import-vt** command can be run on the PE to check into which VPN instances a VPNv4 route with a specified VPN target can be imported.

The VPN target controls route learning between VPN instances. A VPN target may be either an import VPN target or an export VPN target. An export VPN target is contained in a VPNv4 route to be advertised to a remote MP-BGP peer. Receiving a VPNv4 route, an MP-BGP peer compares the received export VPN target with the local import VPN target to determine whether the VPNv4 route can be added to the routing table of the local VPN instance IPv4 address family.

Precautions

At present, this command cannot be used to view the VPN instance with multiple import VPN-target attributes specified.

Example

# Display the VPN instance with the import VPN-target attribute being 1:1.

```
<HUAWEI> display ip vpn-instance import-vt 1:1
The number of ipv4-family matched the import-vt : 3
 VPN-Instance Name and ID : vrf1, 1
 VPN-Instance Name and ID : vrf4, 5
 VPN-Instance Name and ID : vrf5, 4

The number of ipv6-family matched the import-vt : 2
 VPN-Instance Name and ID : vrf1, 1
 VPN-Instance Name and ID : vrf5, 4
```

Table 10-36 Description of the display ip vpn-instance import-vt command output

Item	Description
The number of ipv4-family matched the import-vt	Number of VPN instances with the specified import VPN-target attribute in the VPN instance IPv4 address family view.
The number of ipv6-family matched the import-vt	Number of VPN instances with the specified import VPN-target attribute in the VPN instance IPv6 address family view.
VPN-Instance Name and ID	Name and ID of the VPN instance.

10.4.19 display interface tunnel

Function

The **display interface tunnel** command displays details of the tunnel interface.

Format

display interface tunnel [*interface-number* | **main**]

Parameters

Parameter	Description	Value
interface-number	Specifies the number of the tunnel interface. If this parameter is not specified, the command displays information about all tunnel interfaces.	The value must be the number a tunnel interface that has been created.
main	Displays status and traffic statistics about main interface. The interface has no sub-interfaces. Status and traffic statistics about the interface are displayed whether you specify the main parameter or not.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

To check status of tunnels or diagnose the fault in these tunnels, run the **display interface tunnel** command. You can run this command to obtain tunnel interface information when configuring tunnels or when locating the fault on these tunnels.

Prerequisites

Before run **display interface tunnel**, please ensure that tunnel interface has been created using the **interface tunnel** command.

Example

# Display the details of the tunnel interface.

```
<HUAWEI> display interface tunnel 1
Tunnel1 current state : UP
Line protocol current state : UP
Last line protocol up time : 2012-11-16 19:16:33 UTC+08:00
Description:
Route Port,The Maximum Transmit Unit is 1500
Internet Address is 10.3.1.2/24
```

```
Encapsulation is TUNNEL, loopback not set
Tunnel source 10.2.1.2 (Vlanif1234), destination 10.2.1.1
Tunnel protocol/transport GRE/IP, key disabled
keepalive enable period 5 retry-times 3
Checksumming of packets disabled
Current system time: 2012-11-16 19:17:39+08:00
Last 300 seconds input rate 16 bits/sec, 0 packets/sec
Last 300 seconds output rate 0 bits/sec, 0 packets/sec
Input:  5 packets, 650 bytes
Output:  0 packets, 0 bytes
    Input bandwidth utilization  :    0%
    Output bandwidth utilization :    0%
```

Table 10-37 Description of the display interface tunnel command output

Item	Description
Tunnel1 current state	Physical layer status of the tunnel interface: ● UP: The interface is in normal state. ● Administratively DOWN: The network administrator executes the **shutdown** command on the interface. After a tunnel interface is created, its physical layer status is Up.
Line protocol current state	Link protocol status: ● UP: The link layer protocol of the tunnel interface works normally. ● Down: The link layer protocol of the tunnel interface is abnormal.
Last line protocol up time	Last time the link layer protocol of the tunnel interface goes UP. **NOTE** This field is displayed only when the link layer protocol status of the tunnel interface is UP.
Description	Description of the tunnel interface.
Route Port	Indicates the Layer 3 interface.
The Maximum Transmit Unit is 1500	MTU of tunnel interfaces, which is 1500 bytes by default. Any packet larger than the MTU is fragmented before being sent. If non-fragmentation is configured, the packet is discarded.
Internet Address is 10.3.1.2/24	IP address of the tunnel interface is 10.3.1.2. The mask is 24 bits, that is, 255.255.255.0.
Encapsulation is TUNNEL,	Encapsulation type of packets on a tunnel interface. Packet encapsulation protects a whole IP packet.
loopback not set	The tunnel interface does not support a loopback test.
Tunnel source 10.2.1.2 (Vlanif1234)	The source address of the tunnel is 10.2.1.2. That is, the IP address of the VLANIF 1234 interface sending packets at the source side is 10.2.1.2.

Item	Description
destination 10.2.1.1	Destination address of the tunnel.
Tunnel protocol/ transport GRE/IP, key disabled	The tunnel encapsulation protocol is the GRE protocol, and the transport protocol is the IP protocol. Encapsulation protocol types of a tunnel are as follows: ● GRE: indicates Generic Routing Encapsulation. ● MPLS: encapsulates packets into MPLS packets. ● IPv6 over IPv4: encapsulates IPv6 packets into IPv4 packets. ● IPv4 over IPv6: encapsulates IPv4 packets into IPv6 packets. ● none: indicates no encapsulation. This is the default mode of the tunnel interface. key disabled: the key word recognition function of GRE is not enabled.
keepalive enable period 5 retry-times 3	The keepalive function of GRE.
Checksumming of packets disabled	The check sum function of GRE is not enabled.
Current system time	Current system time. If the time zone is configured and the daylight saving time is used, the time is in YYYY/MM/DD HH:MM:SS UTC±HH:MM DST format.
Last 300 seconds input rate	Incoming packet rate (bits per second and packets per second) within the last 300 seconds.
Last 300 seconds output rate	Outgoing packet rate (bits per second and packets per second) within the last 300 seconds.
Input	Total number of received packets.
Output	Total number of sent packets.
Input bandwidth utilization : --	Input bandwidth usage.
Output bandwidth utilization : --	Output bandwidth usage.

10.4.20 display l3vpn vpn-list tunnel-policy

Function

The **display l3vpn vpn-list tunnel-policy** command displays all the VPN instances to which a specified tunnel policy is applied.

Format

display l3vpn vpn-list tunnel-policy *tunnel-policy-name*

Parameters

Parameter	Description	Value
tunnel-policy-name	Specifies the name of a tunnel policy.	The value is the name of an existing tunnel policy.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

To have its routes recursing to tunnels, a VPN instance needs to apply a tunnel policy. If the tunnel policy used by a VPN instance is changed or the status of tunnels selected based on the tunnel policy changes, the recursive tunnels may change. The **display l3vpn vpn-list tunnel-policy** command displays all the VPN instances to which a specified tunnel policy is applied. The command output will show the VPN instances that will be affected by changes in the tunnel policy.

Example

# Display the referential relationship between a tunnel policy and a VPN instance.

```
<HUAWEI> display l3vpn vpn-list tunnel-policy p1
Codes: *(Tunnel policy is not configured)
Tunnel Policy Name: p1
Total VPN Instance(s) number: 1
VPN(s) using the tunnel policy:
vrf1
```

Table 10-38 Description of the **display l3vpn vpn-list tunnel-policy** command output

Item	Description
Codes	Comments

Item	Description
Tunnel Policy Name	Name of a tunnel policy
Total VPN Instance(s) number	Number of VPN instances specified with tunnel policies
VPN(s) using the tunnel policy	Name of VPN instances specified with tunnel policies

10.4.21 display mpls label-stack vpn-instance

Function

The **display mpls label-stack vpn-instance** command displays information about L3VPN label stacks.

Format

display mpls label-stack vpn-instance *vpn-instance-name ip-address*

Parameters

Parameter	Description	Value
vpn-instance-name	Specifies the name of a VPN instance.	The value is the name of an existing VPN instance.
ip-address	Specifies a private IPv4 address.	The value is in dotted decimal notation.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

In a non-inter-AS L3VPN scenario, this command allows you to query label stack information on PEs based on VPN instance names and private IP addresses.

Example

# Display label stack information about the VPN instance named **vpna**.

```
<HUAWEI> display mpls label-stack vpn-instance vpna 10.12.12.1
Label-stack  : 1
Level        : 1
Type         : VPN
```

```
Label       : 1033
Level       : 2
Type        : LDP
Label       : 1041
OutInterface : Vlanif100
```

Table 10-39 Description of the **display mpls label-stack vpn-instance** command output

Item	Description
Label-stack	Number of label stacks
Level	Number of labels
Type	Tunnel type
Label	Value of the outgoing label
OutInterface	Outbound interface

10.4.22 display tunnel-info

Function

The **display tunnel-info** command displays the tunnel information.

Format

display tunnel-info { **tunnel-id** *tunnel-id* | **all** | **statistics** [**slots**] }

Parameters

Parameter	Description	Value
tunnel-id *tunnel-id*	Specifies the tunnel ID. If the specified ID does not exist, the system prompts errors.	A hexadecimal integer ranging from 1 to FFFFFFFE.
all	Displays information about all the tunnels.	-
statistics	Displays statistics about all tunnels.	-
slots	Displays tunnel statistics in the order of slots.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The **display tunnel-info all** command displays existing tunnel IDs, tunnel types, destination IP addresses, and Token information about all tunnels.

The **display tunnel-info tunnel-id** *tunnel-id* command displays detailed information about a tunnel when you only know the tunnel ID.

The **display tunnel-info statistics** command displays the number of tunnels configured on the switch.

Example

# View information about the tunnel.

```
<HUAWEI> display tunnel-info tunnel-id 2
Tunnel ID:              0x2
Tunnel Token:            2
Type:                  cr lsp
Destination:            1.1.1.1
Out Slot:              0
Instance ID:            0
Interface:             Tunnel1
Sub Tunnel ID:           0x0
<HUAWEI> display tunnel-info tunnel-id 3
Tunnel ID:              0x3
Tunnel Token:            3
Type:                  lsp
Destination:            10.20.10.10
Out Slot:              0
Instance ID:            0
Out Interface:           Vlanif1024
Out Label:              3
Next Hop:               10.24.10.200
Lsp Index:             2048
<HUAWEI> display tunnel-info tunnel-id 10006
Tunnel ID:              0x10006
Tunnel Token:            2
Type:                  lsp
Destination:            6.6.6.6
Out Slot:              0
Instance ID:            0
Out Interface:           Vlanif15
Lsp Index:             0
SubTunnel Type:            L2VPN QoS Token
```

Table 10-40 Description of the **display tunnel-info tunnel-id** command output

Item	Description
Tunnel ID	Tunnel ID in hexadecimal notation that is assigned by the system.
Tunnel Token	Token value used for MPLS forwarding that is a part of tunnel ID and is assigned by the system.

Item	Description
Type	Type of a tunnel, such as GRE, MPLS LSP, or CR-LSP. The command output varies according to the tunnel type.
Destination	Destination IP address of the tunnel.
Out Slot	Number of the slot that is used when the switch sends packets.
Instance ID	VPN instance ID (0 indicates that a tunnel is a public network tunnel).
Interface	Local tunnel interface.
Sub Tunnel ID	Sub-tunnel ID of VPN QoS in hexadecimal notation that is automatically assigned by the system.
Out Label	Out label value.
Next Hop	Next hop.
Lsp Index	LSP index, which is allocated by MPLS.
Out Interface	Local outbound interface of the tunnel.
SubTunnel Type	Types of tokens of sub-tunnels: ● LDP LSP over TE QoS Token ● LDP LSP QoS Token ● BGP LSP over TE QoS Token ● BGP LSP QoS Token ● Static LSP QoS Token ● CR-LSP over TE QoS Token ● L2VPN over TE QoS Token ● L2VPN QoS Token This field is displayed only for sub-tunnels.

# Display all tunnel information.

```
<HUAWEI> display tunnel-info all
 * -> Allocated VC Token
Tunnel ID            Type                   Destination            Token
----------------------------------------------------------------------
0x10006              lsp                    10.2.1.1               6
```

# Display tunnel statistics.

```
<HUAWEI> display tunnel-info statistics
LSP/32bit LSP :                     0/0
GRE :                               2
CRLSP :                             0
LOCAL IFNET :                       0
MPLS LOCAL IFNET :                  0
VPN QOS LSP :                       0
```

```
Reserved :                              0
Vxlan :                                 0
```

Table 10-41 Description of the **display tunnel-info statistics** command output

Item	Description
LSP/32bit LSP	Number of LSP tunnels created in the system view/Number of LSP tunnels triggered by the route of host with the 32-bit mask address.
GRE	Number of tunnel IDs allocated to the GRE tunnels.
CRLSP	Number of tunnel IDs allocated to the CR-LSP tunnels.
LOCAL IFNET	Number of tunnels used by the VPN internal module.
MPLS LOCAL IFNET	Number of tunnels used by the MPLS internal module.
VPN QOS LSP	Number of the tunnel ID allocated to the LSP used in VPN QoS.
Reserved	Number of the tunnel ID allocated to the product.
Vxlan	Number of tunnel IDs allocated to the Vxlan tunnels.

# Display tunnel statistics in the order of slots.

```
<HUAWEI> display tunnel-info statistics slots
-------------------------------------------------------------------
Slot       LSP     CR      GRE     LCL     MPLS-L  VPN     VXLAN
Num                LSP            IFNET   IFNET   QOS
-------------------------------------------------------------------
0          0       0       0       0       0       0       0
Logic Slot: 0                     Total:  0
```

Table 10-42 Description of the display tunnel-info statistics slots command output

Item	Description
Slot Num	Slot number used by the device to send packets.
LSP	Total LSP tunnels set up by the device.
CR LSP	Number of CR-LSPs created on the device.
GRE	Number of GRE tunnels created on the device.
LCL IFNET	Number of tunnels used by the VPN module.
MPLS-L IFNET	Number of tunnels used by the MPLS module.

Item	Description
VPN QOS	Number of tunnels used for VPN QoS.
VXLAN	Number of VXLAN tunnels created on the device.

10.4.23 display tunnel-policy

Function

The **display tunnel-policy** command displays the configurations of tunnel policies.

Format

display tunnel-policy [*tunnel-policy-name*]

Parameters

Parameter	Description	Value
tunnel-policy-name	Specifies the name of tunnel policy. If *tunnel-policy-name* is specified, information about the specified tunnel policy is displayed.	The value is the name of an existing tunnel policy.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Using the **display tunnel-policy** command, you can check the configured tunnel policy and information about a tunnel policy before applying it.

Example

# Display information about all the tunnel policies.

```
<HUAWEI> display tunnel-policy
Total   tunnel policy num:            3
Sel-Seq tunnel policy num:            1
Binding tunnel policy num:            1
Invalid tunnel policy num:            1

Tunnel Policy Name                Select-Seq                  Load balance No
------------------------------------------------------------------------------------------
po2                          CR-LSP LSP                  3
```

```
Tunnel Policy Name                    Destination      Tunnel Intf       Ignore-dest-check   Down switch
-------------------------------------------------------------------------------------------------------------
po2                             1.1.1.9         Tunnel2           Disable             Enable
```

Table 10-43 Description of the display tunnel-policy command output

Item	Description
Total tunnel policy num	Total number of tunnel policies.
Sel-Seq tunnel policy num	Total number of tunnel policies in select-sequence mode.
Binding tunnel policy num	Total number of tunnel policies in tunnel binding mode.
Invalid tunnel policy num	Total number of invalid tunnel policies.
Tunnel Policy Name	Name of tunnel policies.
Select-Seq	Priorities of tunnel types in descending order.
Load balance No	Number of tunnels for load balancing. The default value is 1.
Destination	Destination IP addresses of the bound tunnels, that is, IP addresses of the peer interfaces that receive packets.
Tunnel Intf	Local tunnel interface of the bound tunnel.
Ignore-dest-check	Check is disabled regardless of whether the destination IP address specified in a tunnel policy is consistent with the actual destination address of the tunnel to be bound to the tunnel policy.
Down switch	Tunnel switch over status: ● Enable indicates that the function is enabled ● Disable indicates that the function is disabled

# Display information about the tunnel policy.

```
<HUAWEI> display tunnel-policy p1
The number of binding:1
Tunnel Policy Name                    Destination      Tunnel Intf       Ignore-dest-check   Down Switch
-------------------------------------------------------------------------------------------------------------
p1                              1.1.1.1         Tunnel2           Disable             Enable
```

Table 10-44 Description of the display tunnel-policy tunnel-policy-name command output

Item	Description
The number of binding	Number of the bound destination addresses.

10.4.24 display tunnel-policy-config

Function

The **display tunnel-policy-config** command displays the configuration of tunnel policies.

Format

display tunnel-policy-config [*tunnel-policy-name*]

Parameters

Parameter	Description	Value
tunnel-policy-name	Indicates the name of the tunnel policy.	The value is the name of an existing tunnel policy.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After tunnel policies are configured, you can view the configuration of a tunnel policy by using the **display tunnel-policy-config** command. If you do not specify the tunnel policy to be displayed, the configurations of all tunnel policies are displayed.

Example

# Display the configurations of all tunnel policies.

```
<HUAWEI> display tunnel-policy-config
#
tunnel-policy whm1
 description 1.1.1.1
#
tunnel-policy whm2
 description 1.1.1.1
 tunnel select-seq cr-lsp lsp load-balance-number 3
#
tunnel-policy whm3
 tunnel binding destination 1.1.1.1 te Tunnel2
#
return
```

# Display the configuration of the tunnel policy named p1.

```
<HUAWEI> display tunnel-policy-config p1
#
tunnel-policy p1
 tunnel select-seq cr-lsp lsp load-balance-number 1
#
return
```

10.4.25 display tunnel-policy subscriber statistics

Function

The **display tunnel-policy subscriber statistics** command displays the number of times a tunnel policy is used by external services.

Format

display tunnel-policy *tunnel-policy-name* **subscriber statistics**

Parameters

Parameter	Description	Value
tunnel-policy-name	Specify the name of a tunnel policy.	The value is the name of an existing tunnel policy.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

A system has many tunnel policies that can be used by different services. The **display tunnel-policy subscriber statistics** command can be used to view the number of times a tunnel policy is used by external services. This prevents the tunnel policy from being deleted mistakenly.

Example

# View the number of times a tunnel policy is used by external services.

```
<HUAWEI> display tunnel-policy nms-vrf-vpna subscriber statistics
The specified tunnel policy does not exist.
Total 0 applications subscribed the tunnel policy.
```

# View the number of times a tunnel policy is used by external services.

```
<HUAWEI> display tunnel-policy nms-vrf-vpna subscriber statistics
Total 200 applications subscribed the tunnel policy.
```

Table 10-45 Description of the **display tunnel-policy subscriber statistics** command output

Item	Description
The specified tunnel policy does not exist. Total 0 applications subscribed the tunnel policy.	The tunnel policy does not exist and is not used by applications.
Total 200 applications subscribed the tunnel policy.	The tunnel policy exists and is used by 200 applications.

10.4.26 display tunnel-selector

Function

The **display tunnel-selector** command displays the configurations of tunnel selectors of a system.

Format

display tunnel-selector [*tunnel-selector-name*]

Parameters

Parameter	Description	Value
tunnel-selector-name	Specifies the name of a tunnel selector.	The value is the name of an existing tunnel selector.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

If *tunnel-selector-name* is not specified in the command, the command displays the configurations of all the tunnel selectors of the system.

Example

# Display information about a tunnel selector named tps.

```
<HUAWEI> display tunnel-selector tps
Tunnel-selector : tps
  permit : 10 (matched counts: 0)
    Match clauses :
      if-match ip next-hop ip-prefix ipv4prefix
    Apply clauses :
      apply tunnel-policy policy1
```

Table 10-46 Description of the **display tunnel-selector** command output

Item	Description
Tunnel-selector	Name of a tunnel selector
permit : 10	Matching mode and number of the node of the tunnel selector
Match clauses	**if-match** clauses
Apply clauses	**apply** causes

10.4.27 export route-policy

Function

The **export route-policy** command associates the current VPN instance address family with an export Route-Policy.

The **undo export route-policy** command disassociates the current VPN instance address family from the export Route-Policy.

By default, the current VPN instance address family is not associated with any export Route-Policy.

Format

export route-policy *policy-name*

undo export route-policy

Parameters

Parameter	Description	Value
policy-name	Specifies the name of the export Route-Policy to be associated with the VPN instance address family.	The name is a string of 1 to 40 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Views

VPN instance view, VPN instance IPv4 address family view, VPN instance IPv6 address family view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can implement a more accurate advertisement of the routes of the VPN instance address family based on the export Route-Policy than that based on the extended community attribute. The export Route-Policy is used to filter the routing information and to set the routing attributes of the routes that pass the filtering.

The **export route-policy** command advertises local routes of the VPN instance address family to other VPN instances address family. The **peer route-policy** command or the **filter-policy** command run in the BGP VPN instance address family view filters routes of the VPN instance address family advertised to or received from CE neighbors.

In local cross scenarios, you can run the **export route-policy** command to filter out locally crossed routes and set the attributes of these routes. Locally crossed routes include both locally imported routes and routes learned from VPN peers.

Prerequisites

The **route-distinguisher** command has been executed to set the RD of the VPN instance.

Precautions

The current VPN instance address family can be associated with only one export Route-Policy. If the **export route-policy** command is run several times, the latest configuration overrides the previous configurations.

If the route policy does not exist, you need to configure the route policy.

Creating a route-policy before it is referenced is recommended. By default, nonexistent route-policies cannot be referenced using the command. If the route-policy nonexistent-config-check disable command is run in the system view and a nonexistent route-policy is referenced using the current command in the VPN instance view or BGP-VPN instance IPv4 address family view, all routes in the VPN instance address family can be crossed to the VPNv4 address family. If the **route-policy nonexistent-config-check disable** command is run in the system view and a nonexistent route-policy is referenced using the current command in the BGP-VPN instance IPv6 address family view, all routes in the BGP-VPN instance IPv6 address family can be crossed to the VPNv6 address family.

Example

# Apply an export Route-Policy named poly-1 to the IPv4 address family of the VPN instance named vrf1.

```
<HUAWEI> system-view
[HUAWEI] ip vpn-instance vrf1
[HUAWEI-vpn-instance-vrf1] ipv4-family
[HUAWEI-vpn-instance-vrf1-af-ipv4] route-distinguisher 100:1
[HUAWEI-vpn-instance-vrf1-af-ipv4] export route-policy poly-1
```

10.4.28 if-match ip next-hop (tunnel-selector view)

Function

The **if-match ip next-hop** command configures route filtering based on the next hop.

The **undo if-match ip next-hop** command cancels the setting.

By default, route filtering based on the next hop is not configured.

Format

if-match ip next-hop { **acl** { *acl-number* | *acl-name* } | **ip-prefix** *ip-prefix-name* }

undo if-match ip next-hop [**acl** { *acl-number* | *acl-name* } | **ip-prefix** *ip-prefix-name*]

Parameters

Parameter	Description	Value
acl *acl-number*	Specifies the number of a basic ACL.	The value is an integer ranging from 2000 to 2999.
acl *acl-name*	Specifies the name of a named ACL.	The value is a string of 1 to 64 case-sensitive characters without spaces. The value must start with a letter.
ip-prefix *ip-prefix-name*	Specifies the name of an IP prefix list.	The name is a string of 1 to 169 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Views

Tunnel selector view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

This command can be run in the tunnel selector view on the SPE in HVPN networking needs to apply a tunnel policy to VPNv4 routes to, for example, have the VPNv4 routes recursing to MPLS TE tunnels.

The **if-match ip next-hop** command is used to apply a tunnel policy to the VPNv4 or BGP-IPv4 labeled routes with a specified next hop, not all VPNv4 or BGP-IPv4 labeled routes.

Either an ACL or IP prefix list can be used to filter routes by next hop.

Prerequisite

The **tunnel-selector** command is run to create a tunnel selector.

An IP prefix list is configured using the **ip ip-prefix** command, or an ACL is configured using the **acl** command in the system view or the **acl name** command to specify the next hop.

Follow-up Procedure

Run the **apply tunnel-policy** command in the tunnel selector view to apply a tunnel policy to the routes that pass the filtering.

Precautions

Creating an ACL before it is referenced is recommended. If a nonexistent ACL is referenced using the command, all routes match the ACL.

Creating an IP prefix list before it is referenced is recommended. By default, nonexistent IP prefix lists cannot be referenced using the command. If the **route-policy nonexistent-config-check disable** command is run in the system view and a nonexistent IP prefix list is referenced using the current command, all routes match the IP prefix list.

Example

# Configure route filtering based on the next hop.

```
<HUAWEI> system-view
[HUAWEI] tunnel-selector abc permit node 10
[HUAWEI-tunnel-selector] if-match ip next-hop acl 2000
```

10.4.29 if-match ip-prefix (tunnel-selector view)

Function

The **if-match ip-prefix** command configures a tunnel selector to use an IP prefix list as a route filtering rule.

The **undo if-match ip-prefix** command restores the default configuration.

By default, a tunnel selector does not use any IP prefix list as a route filtering rule.

Format

if-match ip-prefix *ip-prefix-name*

undo if-match ip-prefix *ip-prefix-name*

Parameters

Parameter	Description	Value
ip-prefix-name	Specifies the name of an IP prefix list.	The name is a string of 1 to 169 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Views

Tunnel-selector view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To enable a device to match routes against a specified IP prefix list and determine whether to permit or deny the routes based on matching results, run the **if-match ip-prefix** command to configure a tunnel selector to use the IP prefix list as a route filtering rule.

The **if-match ip-prefix** command must be used with the **ip ip-prefix** command. For example:

If the **if-match ip-prefix aa** and **ip ip-prefix aa permit 1.1.1.1 32** commands are both configured, BGP routes with IP prefix 1.1.1.1/32 will be permitted.

Prerequisites

A tunnel selector has been configured using the **tunnel-selector** command.

The IPv4 prefix list has been created by running the **ip ip-prefix** command.

Precautions

Routes are filtered by IP prefix. Only routes matching the specified IP prefix list are permitted.

Example

# Configure a tunnel selector to use IP prefix list **p1** as a route filtering rule.

```
<HUAWEI> system-view
[HUAWEI] ip ip-prefix p1 permit 10.0.0.0 8 greater-equal 17 less-equal 18
[HUAWEI] tunnel-selector policy permit node 10
[HUAWEI-tunnel-selector] if-match ip-prefix p1
```

10.4.30 if-match ipv6 next-hop (tunnel-selector view)

Function

The **if-match ipv6 next-hop** command configures the filtering of IPv6 routes based on the next hop.

The **undo if-match ipv6 next-hop** command cancels the setting.

By default, the filtering of IPv6 routes based on the next hop is not configured.

Format

if-match ipv6 next-hop prefix-list *ipv6-prefix-name*

undo if-match ipv6 next-hop prefix-list *ipv6-prefix-name*

Parameters

Parameter	Description	Value
prefix-list *ipv6-prefix-name*	Specifies the name of an IPv6 prefix list.	The name is a string of 1 to 169 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Views

tunnel selector view

Default Level

2: Configuration level

Usage Guidelines

You can run the **if-match ipv6 next-hop** command if it is required to filter IPv6 routes based on the next hop. When you run the **if-match ipv6 next-hop** command in the tunnel selector view, you can use an **apply** clause to apply a tunnel policy to the IPv6 routes filtered based on the next hop.

The next hop can be specified by the IPv6 prefix list.

Example

# Configure filtering of IPv6 routes based on the next hop.

```
<HUAWEI> system-view
[HUAWEI] tunnel-selector abc permit node 10
[HUAWEI-tunnel-selector] if-match ipv6 next-hop prefix-list ipv6prefix
```

10.4.31 import route-policy

Function

The **import route-policy** command associates the current VPN instance address family with an import Route-Policy.

The **undo import route-policy** command disassociates the current VPN instance address family from an import Route-Policy.

By default, the current VPN instance address family is not associated with any import Route-Policy.

Format

import route-policy *policy-name*

undo import route-policy

Parameters

Parameter	Description	Value
policy-name	Specifies the name of the import Route-Policy to be associated with the VPN instance address family.	The name is a string of 1 to 40 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Views

VPN instance view, VPN instance IPv4 address family view, or VPN instance IPv6 address family view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When no import Route-Policy is configured, routes that match the export VPN target attribute of the received routes and the import VPN target attribute of the local VPN instance address family are added to the VPN instance address family.

To control the import of the routes into the VPN instance address family more accurately, you can use the import Route-Policy. The import Route-Policy is used to filter the imported routing information and to set the routing attributes of the routes that pass the filtering.

The **import route-policy** command controls the VPN routes that are cross added to the VPN instance address family. The **peer route-policy** command or the **filter-policy** command run in the BGP VPN instance address family view filters routes of the VPN instance address family advertised to or received from CE neighbors.

Prerequisites

The **route-distinguisher** command has been executed to set the RD of the VPN instance.

Precautions

The current VPN instance address family can be associated with only one import Route-Policy. If the **import route-policy** command is run several times, the latest configuration overrides the previous configurations.

If the route policy to be associated with the VPN instance address family does not exist, you need to configure the route policy.

Creating a route-policy before it is referenced is recommended. By default, nonexistent route-policies cannot be referenced using the command. If the **route-policy nonexistent-config-check disable** command is run in the system view and a nonexistent route-policy is referenced using the current command in the VPN instance view or BGP-VPN instance IPv4 address family view, all routes in the VPNv4 address family can be crossed to the VPN instance address family. If the route-policy nonexistent-config-check disable command is run in the system view and a nonexistent route-policy is referenced using the current command in the BGP-VPN instance IPv6 address family view, all routes in the VPNv6 address family can be crossed to the VPN instance address family.

Example

# Apply an import Route-Policy named poly-1 to the IPv4 address family of the VPN instance named vrf1.

```
<HUAWEI> system-view
[HUAWEI] ip vpn-instance vrf1
[HUAWEI-vpn-instance-vrf1] ipv4-family
[HUAWEI-vpn-instance-vrf1-af-ipv4] route-distinguisher 100:1
[HUAWEI-vpn-instance-vrf1-af-ipv4] import route-policy poly-1
```

10.4.32 ingress-lsp trigger

Function

The **ingress-lsp trigger** command specifies a routing policy to control the creation of ingress LSPs based on BGP labeled routes.

The **undo ingress-lsp trigger** command restores the default setting.

By default, ingress LSPs are created based on all received BGP labeled routes.

NOTE

This command is not supported by the S5731S-S, S6730S-S, and S6735-S.

Format

ingress-lsp trigger route-policy *route-policy-name*

undo ingress-lsp trigger

Parameters

Parameter	Description	Value
route-policy *route-policy-name*	Specifies the name of a routing policy to be used to create ingress LSPs based on BGP labeled routes.	The name is a string of 1 to 40 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Views

BGP view, BGP-IPv4 unicast address family view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In a MAN where the hybrid access mode is used, a large number of BGP labeled routes are used to establish end-to-end LSPs. On certain intermediate nodes where VPN services do not need to be supported, excessive ingress LSPs are created, causing the waste of network resources. In this case, you can run the **ingress-lsp trigger** command to create ingress LSPs based on a routing policy to save network resources.

Precautions

If the **ingress-lsp trigger** command is run more than once, the latest configuration overrides the previous ones.

Creating a route-policy before it is referenced is recommended. By default, nonexistent route-policies cannot be referenced using the command. If the **route-policy nonexistent-config-check disable** command is run in the system view and a nonexistent route-policy is referenced using the current command, ingress LSPs are established for all labeled routes.

Example

# Specify a routing policy named test-policy to control the creation of ingress LSPs based on labeled IPv4 routes.

```
<HUAWEI> system-view
[HUAWEI] bgp 100
[HUAWEI-bgp] ipv4-family unicast
[HUAWEI-bgp-af-ipv4] ingress-lsp trigger route-policy test-policy
```

10.4.33 interface tunnel

Function

The **interface tunnel** command creates a tunnel interface.

The **undo interface tunnel** command deletes the configured tunnel interface.

By default, no tunnel interface is configured.

Format

interface tunnel *interface-number*

undo interface tunnel *interface-number*

Parameters

Parameter	Description	Value
interface-number	Specifies the number of the tunnel interface.	The value is an integer that ranges from 0 to 2047 .

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To forward data over a tunnel, ensure that the tunnel has been created. The system supports the following types of tunnels:

- LSP (Static LSP, BGP LSP, LDP LSP)
- MPLS TE
- GRE

- IPv6 over IPv4
- IPv4 over IPv6

You must use the **interface tunnel** command to create a tunnel interface when creating a tunnel except for LSP tunnels.

Precautions

Tunnel interface numbers are valid on the local device only. You can configure different numbers for the tunnel interfaces on the two ends.

Follow-up Procedure

After a tunnel interface is created, you need to configure an IP address and encapsulation type for the tunnel interface.

To save IP addresses, run the **ip address unnumbered** command to configure the tunnel interface to borrow an IP address of another interface.

The **tunnel-protocol** command configures an encapsulation protocol for the tunnel interface. Then basic configurations are performed based on the encapsulation protocol:

- On an MPLS TE tunnel, run the **destination**, **mpls te tunnel-id**, **mpls te signal-protocol**, and **mpls te commit** commands.
- On the GRE, IPv4 over IPv6 tunnel or manual IPv6 over IPv4 tunnel, run the **source** and **destination** commands.

Example

# Create a tunnel interface.

```
<HUAWEI> system-view
[HUAWEI] interface tunnel 1
[HUAWEI-Tunnel1]
```

10.4.34 ip binding vpn-instance

Function

The **ip binding vpn-instance** command associates an interface on a PE with a VPN instance.

The **undo ip binding vpn-instance** command disables the association between a VPN instance and an interface.

By default, an interface is a public network interface and is not associated with any VPN instance.

Format

ip binding vpn-instance *vpn-instance-name*

undo ip binding vpn-instance *vpn-instance-name*

Parameters

Parameter	Description	Value
vpn-instance-name	Specifies the name of the VPN instance that is associated with the interface.	The value must be an existing VPN instance name.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After a VPN instance is created, you need to associate the PE interface connecting to the VPN with the VPN instance. Then, the interface is used as a private network interface on which a private network address and a private network routing protocol can be configured.

Prerequisites

The **ip vpn-instance** command has been executed to create a VPN instance.

Precautions

Binding an interface to a VPN instance or deleting the binding will result in the deletion of the IP address, Layer 3 features, and IP-related routing protocols of the interface as well as IGMP snooping and MLD snooping configurations of the VLAN to which the interface is added. These features must be re-configured if needed.

An interface cannot be bound to any VPN instance that is not enabled with any address family.

Using the **undo ipv4-family** or **undo ipv6-family** command to disable the IPv4 or IPv6 address family also deletes the IPv4 or IPv6 configurations of the interfaces bound to the VPN instance.

The binding relationship between an interface and a VPN instance with a BFD session bound is removable using the **undo ip binding vpn-instance** command only after the bound BFD session is removed.

Example

# Associate the VLANIF 10 interface with the VPN instance named **vrf1**.

```
<HUAWEI> system-view
[HUAWEI] ip vpn-instance vrf1
[HUAWEI-vpn-instance-vrf1] ipv4-family
[HUAWEI-vpn-instance-vrf1-af-ipv4] route-distinguisher 100:1
[HUAWEI-vpn-instance-vrf1-af-ipv4] quit
[HUAWEI-vpn-instance-vrf1] quit
```

```
[HUAWEI] interface vlanif 10
[HUAWEI-Vlanif10] ip binding vpn-instance vrf1
```

# Associate the GE0/0/1 interface with the VPN instance named **vrf1**.

```
<HUAWEI> system-view
[HUAWEI] ip vpn-instance vrf1
[HUAWEI-vpn-instance-vrf1] ipv4-family
[HUAWEI-vpn-instance-vrf1-af-ipv4] route-distinguisher 100:1
[HUAWEI-vpn-instance-vrf1-af-ipv4] quit
[HUAWEI-vpn-instance-vrf1] quit
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] ip binding vpn-instance vrf1
```

10.4.35 ip frr (VPN instance view)

Function

The **ip frr** command enables IP FRR of a private network in the VPN instance IPv4 address family view.

The **undo ip frr** command disables IP FRR of a private network in the VPN instance IPv4 address family view.

By default, IP FRR of a private network is disabled in the VPN instance IPv4 address family view.

Format

ip frr route-policy *route-policy-name*

undo ip frr

Parameters

Parameter	Description	Value
route-policy *route-policy-name*	Enables IP FRR for the private routes matching the specified route-policy.	The name is a string of 1 to 40 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Views

VPN instance view, VPN instance IPv4 address family view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

With the development of the network, services such as audio, online video, and finance have more requirements for real time. Generally, active/standby links are deployed on the network to ensure service stability.

However, under traditional forwarding modes, when multiple routes to the same destination exist, the system selects the optimal route, which is delivered to FIB table to direct data forwarding. When the optimal link is faulty, the system waits for the completion of route convergence, then selects another optimal route, and then deliver the route to the FIB table. Then the service is recovered. This process leads to a long-time service interruption and cannot meet service requirements.

Using the **ip frr** command, you can enable IP FRR of the private network. IP FRR can specify a backup next hop and a backup interface and set backup forwarding information for IPv4 routes. When the active link is faulty, the system can switch the traffic immediately to the backup link. This process is irrelevant to route convergence and therefore services are interrupted for short time.

Pre-configuration Tasks

You are advised to use the **route-policy** command to create Route-Policy at first, in which the **apply backup-interface** command and the **apply backup-nexthop** command are used to set a backup outbound interface and a backup next hop for IPv4 route of the private network.

The **ip frr** command should be used with the **apply backup-interface** command and the **apply backup-nexthop** command.

- To configure IP FRR for a private network, you need to run the **route-policy** command to create Route-Policy first. Then set a backup outbound interface and next hop for IPv4 routes of the private network using the **apply backup-interface** and **apply backup-nexthop** commands.
- To configure IP+VPN hybrid FRR, you need to run the **route-policy** command to create Route-Policy first. Then set a backup next hop for IPv4 routes of the private network using the **apply backup-nexthop** command.

NOTE

The differences between the IP FRR configuration and IP+VPN hybrid FRR configuration is as follows:

- If the backup next hop and the backup outgoing interface are specified at the same time, the configurations are for IP FRR.
- If only the backup next hop is specified, the configurations are for IP+VPN hybrid FRR. Based on the backup next hop, a matched VPNv4 route from another PE is found. Then a hybrid FRR entry is formed according to the fields of Token, BackupToken, and Label in the route.
- It is invalid to only specify the backup outgoing interface.

Precautions

Only one policy can be used at one time. New configuration will replace the previous one if another policy is configured. Configuration in the system view and that in the VPN instance view will not interfere each other.

Example

# Specify a backup outbound interface and a backup next hop in route-policy **ip_frr_rp** and enable IP FRR for private routes in the VPN instance view.

```
<HUAWEI> system-view
[HUAWEI] route-policy ip_frr_rp permit node 10
[HUAWEI-route-policy] apply backup-interface vlanif 100
[HUAWEI-route-policy] apply backup-nexthop 192.168.20.2
[HUAWEI-route-policy] quit
[HUAWEI] ip vpn-instance vpn1
[HUAWEI-vpn-instance-vpn1] ip frr route-policy ip_frr_rp
```

10.4.36 ipv6 frr (VPN instance IPv6 address family view)

Function

The **ipv6 frr** command enables IPv6 FRR of the private network in the VPN instance IPv6 address family view.

The **undo ipv6 frr** command disables IPv6 FRR of the private network.

By default, IPv6 FRR of the private network is disabled.

NOTE

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

Format

ipv6 frr route-policy *route-policy-name*

undo ipv6 frr

Parameters

Parameter	Description	Value
route-policy *route-policy-name*	Specifies the name of the Route-Policy used by IPv6 FRR.	The name must be unique. The value is a string of 1 to 40 case-sensitive characters.

Views

VPN instance IPv6 address family view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

With the development of the network, services such as audio, online video, and finance have more requirements for real time. Generally, active/standby links are deployed on the network to ensure service stability.

However, under traditional forwarding modes, when multiple routes to the same destination exist, the system selects the optimal route, which is delivered to FIB table to direct data forwarding. When the optimal link is faulty, the system waits for the completion of route convergence, then selects another optimal route, and then deliver the route to the FIB table. Then the service is recovered. This process leads to a long-time service interruption and cannot meet service requirements.

Using the **ipv6 frr** command enables IPv6 FRR of the private network. IPv6 FRR can specify a backup next hop and a backup interface and set backup forwarding information for IPv6 routes. When the active link is faulty, the system can switch the traffic immediately to the backup link. This process is irrelevant to route convergence and therefore services are interrupted for short time.

Pre-configuration Tasks

The **ipv6 frr** command should be used with the **apply ipv6 backup-interface** command and the **apply ipv6 backup-nexthop** command. You are advised to use the **route-policy** command to create Route-Policy at first, in which the **apply ipv6 backup-interface** command and the **apply ipv6 backup-nexthop** command are used to set a backup outbound interface and a backup next hop for IPv6 route of the private network.

Precautions

Only one policy can be used at one time. New configuration will replace the previous one if another policy is configured. Configuration in the system view and that in the VPN instance IPv6 address family view will not interfere each other.

Example

# Specify a backup next hop in the Route-Policy named ipv6_frr_rp. Enable IPv6 FRR of the private network in the VPN instance IPv6 address family view.

```
<HUAWEI> system-view
[HUAWEI] route-policy ipv6_frr_rp permit node 10
[HUAWEI-route-policy] apply ipv6 backup-interface GigabitEthernet1/0/0
[HUAWEI-route-policy] apply ipv6 backup-nexthop 2001:db8:1::1
[HUAWEI-route-policy] quit
[HUAWEI] ip vpn-instance vpn1
[HUAWEI-vpn-instance-vpn1] ipv6-family
[HUAWEI-vpn-instance-vpn1-af-ipv6] route-distinguisher 100:100
[HUAWEI-vpn-instance-vpn1-af-ipv6] ipv6 frr route-policy ip_frr_rp
```

10.4.37 ip vpn-instance

Function

The **ip vpn-instance** command creates a VPN instance and displays the VPN instance view.

The **undo ip vpn-instance** command deletes a specified VPN instance.

By default, no VPN instance is configured.

Format

ip vpn-instance *vpn-instance-name*

undo ip vpn-instance *vpn-instance-name*

Parameters

Parameter	Description	Value
vpn-instance-name	Specifies the name of a VPN instance.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When private network data needs to travel across a public network, you need to configure a VPN instance on the PE of the public network. The public network mentioned here is an MPLS backbone network.

A multi-VPN-instance CE (MCE) device can connect to multiple VPNs. The MCE solution isolates services of different VPNs while reducing cost of network devices. Before configuring an MCE device, configure a VPN instance on the MCE device.

VPN instances are required for all L3VPN configurations.

Precautions

After the ip vpn-instance command is run, a virtual routing table is created on the PE or MCE and consumes resources on the PE or MCE.

After the **undo ip vpn-instance** command is used to delete a VPN instance, all configurations of this VPN instance are deleted.

A VPN instance with a BFD session bound can be deleted using the **undo ip vpn-instance** command only after the bound BFD session is deleted.

When you run the **undo ip vpn-instance** command to delete the VPN instance, if this instance is specified by the **source ip** (NETCONF view) command, you need to delete the bound VPN instance using the **undo source ip** (NETCONF view) command, and then delete the VPN instance.

Follow-up Procedure

After creating a VPN instance, perform the following configurations in the VPN instance view:

- Enable the IPv4 or IPv6 address family for the VPN instance. A VPN instance supports both the IPv4 and IPv6 address families. You need to run the **ipv4-family (VPN instance view)** or **ipv6-family (VPN instance view)** command to enable the IPv4 or IPv6 address family based on the type of the protocol stack used to advertise VPN routes in the VPN instance.

- Configure an RD for the IPv4 address family of the VPN instance. You are allowed to perform VPN configurations in the address family view only after using the **route-distinguisher** command to configure an RD for the address family.
- Configure a VPN target for the VPN instance using the **vpn-target** command. The VPN target controls route learning between VPN instances.
- Bind the VPN instance to the PE or MCE interface connected to the VPN using the **ip binding vpn-instance** command. After an interface is bound to a VPN instance, the interface becomes a part of the VPN. Packets entering the interface will be forwarded based on the VRF table of the VPN.

Example

# Create a VPN instance named **vrf1**.

```
<HUAWEI> system-view
[HUAWEI] ip vpn-instance vrf1
[HUAWEI-vpn-instance-vrf1]
```

10.4.38 ipv4-family (VPN instance view)

Function

The **ipv4-family** command enables the IPv4 address family for a VPN instance and displays the VPN instance IPv4 address family view.

The **undo ipv4-family** command disables the IPv4 address family for a VPN instance.

By default, VPN instances are disabled with the IPv4 address family.

Format

ipv4-family

undo ipv4-family

Parameters

None.

Views

VPN instance view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In BGP/MPLS IP VPN networking, after running the **ip vpn-instance** command to create a VPN instance, you can run the **ipv4-family** command to enable the IPv4 address family for the VPN instance. You can then perform VPN configurations in the address family view to advertise IPv4 VPN routes and allow IPv4 VPN data to be forwarded.

Follow-up Procedure

Run the **route-distinguisher** command to configure an RD for the IPv4 address family of the VPN instance. Before performing VPN configurations in the IPv4 address family view, configure an RD for the IPv4 address family of the VPN instance.

Precautions

Configurations of the commands run in the VPN instance view, except the **description** and **service id** command, are automatically synchronized to the VPN instance IPv4 address family view.

The IPv4 address family for a VPN instance with a BFD session bound can be disabled using the **undo ipv4-family** command only after the bound BFD session is deleted.

Example

# Enable the IPv4 address family for a VPN instance.

```
<HUAWEI> system-view
[HUAWEI] ip vpn-instance vrf1
[HUAWEI-vpn-instance-vrf1] ipv4-family
[HUAWEI-vpn-instance-vrf1-af-ipv4]
```

10.4.39 ipv6-family (VPN instance view)

Function

The **ipv6-family** command enables the IPv6 address family for a VPN instance and displays the VPN instance IPv6 address family view.

The **undo ipv6-family** command disables the IPv6 address family for a VPN instance.

By default, the IPv6 address family is disabled for a VPN instance.

Format

ipv6-family

undo ipv6-family

Parameters

None

Views

VPN instance view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In BGP/MPLS IPv6 VPN networking, after running the **ip vpn-instance** command to create a VPN instance, you can run the **ipv6-family** command to enable the IPv6 address family for the VPN instance and perform VPN configurations in the address family view if you want to have IPv6 VPN routes advertised and IPv6 VPN data forwarded.

Follow-up Procedure

Run the **route-distinguisher** command to configure an RD for the IPv6 address family of the VPN instance. VPN configurations can be performed in the IPv6 address family view only after an RD is configured for the IPv6 address family of the VPN instance.

Precautions

The IPv6 address family for a VPN instance with a BFD session bound can be disabled using the **undo ipv6-family** command only after the bound BFD session is deleted.

Example

# Enable the IPv6 address family for the VPN instance named vrf1.

```
<HUAWEI> system-view
[HUAWEI] ip vpn-instance vrf1
[HUAWEI-vpn-instance-vrf1] ipv6-family
[HUAWEI-vpn-instance-vrf1-af-ipv6]
```

10.4.40 limit-log-interval

Function

The **limit-log-interval** command configures the interval for displaying logs when the number of routes exceeds the threshold.

The **undo limit-log-interval** command restores the default setting.

By default, the interval for displaying logs when the number of routes exceeds the threshold is 5 seconds.

Format

limit-log-interval *interval*

undo limit-log-interval

Parameters

Parameter	Description	Value
interval	Specifies the interval for displaying logs when the number of routes exceeds the threshold.	An integer ranging from 1 to 60, in seconds.

Views

VPN instance view, VPN instance IPv4 address family view or VPN instance IPv6 address family view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If the routes or prefixes in the IPv4 or IPv6 address family of a VPN instance reach the maximum, the system will generate logs at intervals (defaulting to 5 seconds). To prevent logs from being displayed frequently, run the **limit-log-interval** command to prolong the interval of log generation.

The maximum number of routes or prefixes that the IPv4 or IPv6 address family of a VPN instance supports can be configured using the **routing-table limit** or **prefix limit** command.

Prerequisites

1. The **ip vpn-instance** command has been executed to create a VPN instance and enter the VPN instance view.
2. The **ipv4-family** or **ipv6-family** command has been executed to create a VPN instance and enter the VPN instance IPv4 or IPv6 address family view.
3. The **route distinguisher** command has been executed to set the RD of the VPN instance.

Precautions

If a log is generated to record the event that routes or prefixes in the IPv4 or IPv6 address family of a VPN instance reach the maximum, no more routes can be added to the routing table of the IPv4 or IPv6 address family of the VPN instance. Instead, the routes will be discarded.

Example

# Set the interval for displaying logs to 8 seconds when the number of routes in the IPv4 address family of the VPN instance named vpn1 exceeds the threshold.

```
<HUAWEI> system-view
[HUAWEI] ip vpn-instance vpn1
[HUAWEI-vpn-instance-vpn1] ipv4-family
[HUAWEI-vpn-instance-vpn1-af-ipv4] route-distinguisher 100:1
[HUAWEI-vpn-instance-vpn1-af-ipv4] limit-log-interval 8
```

10.4.41 mpls te reserved-for-binding

Function

The **mpls te reserved-for-binding** command reserves an MPLS TE tunnel for VPN binding.

The **undo mpls te reserved-for-binding** command removes the configuration.

By default, an MPLS TE tunnel can be selected based on any type of tunnel policy.

Format

mpls te reserved-for-binding

undo mpls te reserved-for-binding

Parameters

None

Views

Tunnel interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If a VPN has high requirements for bandwidth, you can apply a tunnel binding policy to the VPN to have the routes of the VPN recursing to MPLS TE tunnels. Before applying that tunnel binding policy to the VPN, you need to run the **mpls te reserved-for-binding** command to reserve MPLS TE tunnels for VPN binding.

Prerequisites

MPLS TE tunnels are available in the system.

Configuration Impact

After the **mpls te reserved-for-binding** command is configured on an MPLS TE tunnel, the tunnel can be selected based on a tunnel binding policy only. Even if no tunnel binding policy is configured, a tunnel type prioritizing policy created using the **tunnel select-seq** command will not select the MPLS TE tunnel for which the **mpls te reserved-for-binding** command has been configured.

Follow-up Procedure

Run the **tunnel-policy** command to create a tunnel policy and the **tunnel binding** command to bind the policy to the MPLS TE tunnel.

Example

# Reserve Tunnel1 for VPN binding.

```
<HUAWEI> system-view
[HUAWEI] interface tunnel 1
[HUAWEI-Tunnel1] tunnel-protocol mpls te
[HUAWEI-Tunnel1] mpls te reserved-for-binding
```

# Delete the configuration of a tunnel that is reserved for VPN binding.

```
<HUAWEI> system-view
[HUAWEI] interface tunnel 1
[HUAWEI-Tunnel1] undo mpls te reserved-for-binding
```

10.4.42 nd vpn-cross enable

Function

The **nd vpn-cross enable** command enables direct ND entry delivery for mutual access between IPv6 VPNs.

The **undo nd vpn-cross enable** command disables direct ND entry delivery for mutual access between IPv6 VPNs.

By default, direct ND entry delivery for mutual access between IPv6 VPNs is disabled.

NOTE

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

Format

nd vpn-cross enable

undo nd vpn-cross enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In a scenario of mutual access between IPv6 VPNs, traffic initiated during mutual access for the first time will trigger ND Miss messages and ND entry learning. If a PE device fails to process the ND Miss messages in time (for example, when a new card is installed), mutual access traffic between the VPNs cannot be transmitted.

After direct ND entry delivery for mutual access between IPv6 VPNs is enabled on the PE device, the device delivers ND entries in advance when a new card is installed without the need to trigger mutual access traffic. This ensures proper transmission of mutual access traffic between local VPNs.

Precautions

After direct ND entry delivery for mutual access between IPv6 VPNs is enabled, the ND entries delivered by the device in advance will consume some ND entry resources. Therefore, configure this function only when required.

Example

# Enable direct ND entry delivery for mutual access between IPv6 VPNs.

```
<HUAWEI> system-view
[HUAWEI] nd vpn-cross enable
Warning: After this function is enabled, a large number of ND entries will be occupied.
```

10.4.43 peer default-originate vpn-instance

Function

The **peer default-originate vpn-instance** command configures BGP to advertise all default routes related to the specified VPN instance to the specified VPNv4 peer or peer group.

The **undo peer default-originate vpn-instance** command removes the configuration.

By default, BGP does not advertise its default route to the VPNv4 peer or peer group.

Format

peer { *ipv4-address* | *group-name* } **default-originate vpn-instance** *vpn-instance-name*

undo peer { *ipv4-address* | *group-name* } **default-originate vpn-instance** *vpn-instance-name*

Parameters

Parameter	Description	Value
ipv4-address	Specifies the IPv4 address of a peer.	It is in dotted decimal notation.
group-name	Specifies the name of the peer group.	The name is a string of 1 to 47 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

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

Views

BGP-VPNv4 address family view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

HoVPN refers to a hierarchical VPN, with multiple PEs functioning as different roles to form a hierarchical architecture and provide functions of a single PE. In this manner, the performance requirement on PEs is lowered. If the **peer default-originate vpn-instance** command is used, SPE sends the default route with the address of the next hop as the local address, regardless of whether there is a default route in the local routing table. The UPE then only needs to maintain the local VPN routes, whereas all remote routes are replaced by the default route. The workload of the UPE is reduced.

Precautions

If an SPE does not have an active default route, either of the following methods can be used to generate a default route on the SPE and allow the SPE to advertise the route to the UPE:

- Method 1: Run the **peer default-originate vpn-instance** command to enable the SPE to automatically generate a default route and advertise it to the UPE.
- Method 2: Run the **ip route-static vpn-instance** command to configure a default route on the SPE, run the **default-route imported** command to enable the SPE to import the default route to the BGP routing table, and then run the **import-route static** or **network** command in the BGP-VPN instance IPv4 address family view to import the default route to the BGP IPv4 VPN instance routing table.

Either of the preceding methods can be used to advertise a default route to the UPE. The priority of the default route generated through method 1 is higher than that generated through method 2. If method 1 is used, the default route generated through method 2 will be suppressed, and no Update messages will be sent for a route change or withdrawal. If the SPE has an active default route, the SPE can advertise the route to the UPE without the need for either of the preceding methods.

Example

# Advertise default routes of vpn1 to VPNv4 peer 1.1.1.1.

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

```
[HUAWEI] bgp 100
[HUAWEI-bgp] peer 1.1.1.1 as-number 100
[HUAWEI-bgp] ipv4-family vpnv4
[HUAWEI-bgp-af-vpnv4] peer 1.1.1.1 enable
[HUAWEI-bgp-af-vpnv4] peer 1.1.1.1 upe
[HUAWEI-bgp-af-vpnv4] peer 1.1.1.1 default-originate vpn-instance vpn1
```

10.4.44 peer mpls-local-ifnet disable

Function

The **peer mpls-local-ifnet disable** command disables EBGP peers from establishing an MPLS local ifnet tunnel between them.

The **undo peer mpls-local-ifnet disable** command enables EBGP peers to establish an MPLS local ifnet tunnel between them.

By default, EBGP peers can automatically establish MPLS local ifnet tunnels between them if one of the following conditions is met:

- EBGP peers are enabled to exchange labeled routes.
- EBGP peers are configured in the BGP-VPLS address families.
- EBGP peers are configured in the BGP-VPNv4 or BGP-VPNv6 address family.

Format

peer { *group-name* | *ipv4-address* } **mpls-local-ifnet disable**

undo peer { *group-name* | *ipv4-address* } **mpls-local-ifnet disable**

Parameters

Parameter	Description	Value
group-name	Specifies the name of a BGP peer group.	The name is a string of 1 to 47 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
ipv4-address	Specifies the IPv4 address of a BGP peer.	The value is in dotted decimal notation.

Views

BGP view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

MPLS local ifnet tunnel: In inter-AS VPN Option B or Option C scenarios, the VPN routes with L2VPN label block information that ASBRs advertise to BGP peers must contain public-network tunnel information. However, no tunnels are configured between ASBRs. To allow EBGP routes to be advertised to IBGP peers, an MPLS local ifnet tunnel is generated between MPLS interfaces of ASBRs.

In the L3VPN over inter-as seamless MPLS or VPLS scenario, EBGP peer relationships are established between BGP peers. The BGP peers can be endpoint PEs in the VPLS scenario or the CSG and MASG in the inter-AS seamless MPLS scenario. These EBGP peers automatically establish MPLS local ifnet tunnels between them. The E2E MPLS local ifnet tunnel fails to transmit traffic if the two peers are indirectly connected.

If a fault occurs on a tunnel between the two EBGP peers, the route recurses to the MPLS local ifnet tunnel, not an FRR bypass tunnel. As the MPLS local ifnet tunnel cannot forward traffic, traffic is interrupted. To prevent the traffic interruption, run this command to disable the establishment of an MPLS local ifnet tunnel between the EBGP peers.

Prerequisites

The EBGP peer relationship must be in the Established between PEs.

Example

# Disable EBGP peers from establishing an MPLS local ifnet tunnel.

```
<HUAWEI> system-view
[HUAWEI] bgp 100
[HUAWEI-bgp] peer 10.1.1.1 as-number 200
[HUAWEI-bgp] peer 10.1.1.1 mpls-local-ifnet disable
```

10.4.45 peer upe

Function

The **peer upe** command specifies a BGP peer or peer group as UPE of HoVPN.

The **undo peer upe** command cancels the configuration.

Format

peer { *group-name* | *ipv4-address* } **upe**

undo peer { *group-name* | *ipv4-address* } **upe**

Parameters

Parameter	Description	Value
group-name	Specifies the name of the peer group.	The name is a string of 1 to 47 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Parameter	Description	Value
ipv4-address	Specifies the IPv4 address of a peer.	-

Views

BGP-VPNv4 address family view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After a UPE is specified on the SPE through the **peer upe** command, the SPE does not send a specific route to the UPE. If the **peer route-policy export** command is run on the SPE to configure routing policies for the UPE and certain specific routes can pass the filtration of routing policies, these specific routes can be sent to the UPE.

Prerequisites

Before you run the peer upe command, the **peer as-number** command should be used to create a peer or peer group.

Precautions

The BGP peer relationship is interrupted after you run the **peer upe** command. So, confirm the action before you use the command.

If an SPE does not have an active default route, either of the following methods can be used to generate a default route on the SPE and allow the SPE to advertise the route to the UPE:

- Method 1: Run the **peer default-originate vpn-instance** command to enable the SPE to automatically generate a default route and advertise it to the UPE.
- Method 2: Run the **ip route-static vpn-instance** command to configure a default route on the SPE, run the **default-route imported** command to enable the SPE to import the default route to the BGP routing table, and then run the **import-route static** or **network** command in the BGP-VPN instance IPv4 address family view to import the default route to the BGP IPv4 VPN instance routing table.

Either of the preceding methods can be used to advertise a default route to the UPE. The priority of the default route generated through method 1 is higher than that generated through method 2. If method 1 is used, the default route generated through method 2 will be suppressed, and no Update messages will be sent for a route change or withdrawal. If the SPE has an active default route, the SPE can advertise the route to the UPE without the need for either of the preceding methods.

Follow-up Procedure

After the **peer upe** command is configured, to send the default route 0.0.0.0 to the UPE, you need to run the **peer default-originate vpn-instance** command on the SPE.

Example

# Specify the peer 1.1.1.2 as UPE.

```
<HUAWEI> system-view
[HUAWEI] bgp 100
[HUAWEI-bgp] peer 1.1.1.2 as-number 100
[HUAWEI-bgp] ipv4-family vpnv4
[HUAWEI-bgp-af-vpnv4] peer 1.1.1.2 enable
[HUAWEI-bgp-af-vpnv4] peer 1.1.1.2 upe
```

10.4.46 peer soo

Function

The **peer soo** command configures the Site of Origin (SoO) attribute for an EBGP peer in a BGP VPN instance.

The **undo peer soo** command deletes the SoO.

By default, no SoO attribute is configured for an EBGP peer in a BGP VPN instance.

Format

peer { *group-name* | *ipv4-address* | *ipv6-address* } **soo** *site-of-origin*

undo peer { *group-name* | *ipv4-address* | *ipv6-address* } **soo**

Parameters

Parameter	Description	Value
group-name	Specifies the name of a BGP peer group.	The name is a string of 1 to 47 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
ipv4-address	Specifies the IPv4 address of a BGP peer.	It is in dotted decimal notation.
ipv6-address	Specifies the IPv6 address of a BGP peer.	The address is in the format of X:X:X:X:X:X:X:X.

Parameter	Description	Value
Site-of-origin	Specifies the SoO attribute, which is a BGP extended community attribute and can be expressed in any of the following formats: ● 2-byte AS number: 4-byte user-defined number, for example, 1:3. The AS number ranges from 0 to 65535. The user-defined number ranges from 0 to 4294967295. The AS number and the user-defined number cannot both be 0. That is, a SoO cannot be 0:0. ● IPv4-address: 2-byte user-defined number, for example, 192.168.122.15:1. The IP address ranges from 0.0.0.0 to 255.255.255.255. The user-defined number ranges from 0 to 65535. ● Integral 4-byte AS number:2-byte user-defined number, for example, 65537:3. An AS number ranges from 65536 to 4294967295. A user-defined number ranges from 0 to 65535. The AS number and user-defined number cannot be both 0s. That is, a SoO cannot be 0:0. ● 4-byte AS number in dotted notation:2-byte user-defined number, for example, 0.0:3 or 0.1:0. A 4-byte AS number in dotted notation is in the format of *x.y*, where *x* and *y* are integers that range from 0 to 65535 and from 0 to 65535, respectively. A user-defined number ranges from 0 to 65535. The AS number and user-defined number cannot be both 0s. That is, a SoO cannot be 0.0:0.	-

Views

BGP-VPN instance IPv4 address family view, BGP-VPN instance IPv6 address family view, BGP view, BGP-IPv4 unicast address family view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In a BGP/MPLS IP VPN scenario, if the ASs to which two VPN sites belong use private AS numbers, the AS numbers of the two VPN sites may be the same. As a result, different sites of the same VPN cannot communicate. The **peer substitute-**

as command can be used to enable AS number substitution on PEs to address this problem.

Enabling AS number substitution will cause another problem. Several CEs at a VPN site may establish EBGP connections with different PEs of a BGP/MPLS IP VPN backbone network, and a routing protocol has been configured on the CEs. If AS number substitution is enabled on PEs, the AS numbers carried by VPN routes of this site will be replaced on the PEs. As a result, routes advertised from a CE to a PE may be re-advertised to this VPN site after the routes traverse the backbone network, causing a routing loop. The **peer soo** command can be run on the PEs to address this problem.

After the **peer soo** command is run on a PE to configure the SoO attribute for a specified CE, the PE adds the attribute to a route sent from the CE and advertises the route to the remote PE. The remote PE checks the SoO attribute of the route before sending it to its attached CE. If the SoO attribute is the same as the local SoO attribute on the remote PE, the remote PE does not send the route to its attached CE, preventing a routing loop in a VPN site.

Precautions

The **peer soo** command is used only in the scenarios where PEs and CEs establish EBGP peer relationships.

Example

# Configure the SoO attribute for EBGP peers in a BGP VPN instance.

```
<HUAWEI> system-view
[HUAWEI] bgp 100
[HUAWEI-bgp] ipv4-family vpn-instance vpna
[HUAWEI-bgp-vpna] peer 192.168.15.2 soo 10.2.2.2:45
```

10.4.47 peer substitute-as

Function

The **peer substitute-as** command enables AS number substitution. This command enables a device to replace the AS number of the peer specified in the AS_Path attribute with the local AS number.

The **undo peer substitute-as** command disables AS number substitution.

By default, AS number substitution is disabled.

Format

peer { *group-name* | *ipv4-address* | *ipv6-address* } **substitute-as**

undo peer { *group-name* | *ipv4-address* | *ipv6-address* } **substitute-as**

Parameters

Parameter	Description	Value
group-name	Specifies the name of a peer group.	The name is a string of 1 to 47 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
ipv4-address	Specifies the IPv4 address of a peer.	It is in dotted decimal notation.
ipv6-address	Specifies the IPv6 address of a peer.	The address is in the format of X:X:X:X:X:X:X:X.

Views

BGP view, BGP-IPv4 unicast address family view, BGP-VPN instance IPv4 address family view, BGP-VPN instance IPv6 address family view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In a BGP/MPLS IP VPN scenario, if the ASs to which two VPN sites belong use private AS numbers, the AS numbers of the two VPN sites may be the same. If a CE in a VPN site sends a VPN route to the connected PE using EBGP and the PE then sends the route to the remote PE, the remote CE will discard the route because the AS number carried by the route is the same as the local AS number. As a result, different sites of the same VPN cannot communicate. The **peer substitute-as** command can be used on the PE to enable AS number substitution to address this problem. After that, the PE replaces the AS number carried in the VPN route with the local AS number. As a result, the remote CE will not discard the route due to identical AS numbers.

Pre-configuration Tasks

Run the **peer as-number** command to create a peer or configure an AS number for a specified peer group.

Example

# Configure a device to replace the AS number of a specified peer in the AS_Path of a route with the local AS number.

```
<HUAWEI> system-view
[HUAWEI] bgp 100
[HUAWEI-bgp] ipv4-family vpn-instance vpn1
```

```
[HUAWEI-bgp-vpn1] peer 10.1.1.2 as-number 200
[HUAWEI-bgp-vpn1] peer 10.1.1.2 substitute-as
```

10.4.48 policy vpn-target

Function

The **policy vpn-target** command configures a device to implement VPN target-based filtering for received routes.

The **undo policy vpn-target** command cancels VPN target-based filtering.

By default, the VPN-Target filtering is enabled.

Format

policy vpn-target

undo policy vpn-target

Parameters

None

Views

BGP-VPNv4 address family view, BGP-VPNv6 address family view, BGP-MDT address family view, BGP-MVPN address family view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In the networking of BGP/MPLS IP VPN, Kompella VLL, and Kompella VPLS, VPN target attributes are used to filter received VPN routes or label blocks. If VPN target attributes are not configured, received VPN routes or label blocks are discarded.

VPNs and VPN target attributes are not configured on the following devices in certain networking scenarios:

- RRs in BGP/MPLS IP VPN, Kompella VPLS, or Kompella VLL
- ASBRs (not functioning as PEs) in inter-AS BGP/MPLS IP VPN OptionB

In this case, VPN routes or label blocks are not saved on the RRs or ASBRs.

The RRs or ASBRs, however, need to save all VPN routes or label blocks sent from PEs. Therefore, the **undo policy vpn-target** command can be configured on the RRs or ASBRs to disable the filtering of VPN routes or label blocks.

Precautions

Running the **undo policy vpn-target** makes all VPN routes or label blocks from PEs received. Therefore, this command is configured only on devices of particular roles (RRs or ASBRs)

Example

# Configure a device to implement VPN target-based filtering for received VPNv4 routes.

```
<HUAWEI> system-view
[HUAWEI] bgp 100
[HUAWEI-bgp] ipv4-family vpnv4
[HUAWEI-bgp-af-vpnv4] policy vpn-target
```

10.4.49 prefix limit

Function

The **prefix limit** command sets a limit on the maximum number of prefixes supported in the existing VPN instance address family, preventing the PE from importing excessive VPN route prefixes.

The **undo prefix limit** command restores the default setting.

By default, the maximum number of VPN route prefixes is not limited.

Format

prefix limit *number* { *alert-percent* [**route-unchanged**] | **simply-alert** }

undo prefix limit

Parameters

Parameter	Description	Value
number	Specifies the maximum number of prefixes supported in the VPN instance address family.	The value is an integer, and the minimum value is 1. The maximum number is determined by the license file.

Parameter	Description	Value
alert-percent	Specifies the proportion of the alarm threshold to the maximum number of prefixes. When the number of prefixes in the VPN instance address family exceeds *number* x *alert-percent*/100, alarms are displayed. The VPN route prefixes, however, can still join the VPN routing table. When the number of the prefixes exceeds the *number*, the subsequent prefixes are discarded.	The value is an integer ranging from 1 to 100.
route-unchanged	Indicates that the routing table remains unchanged. By default, **route-unchanged** is not configured. When the number of prefixes in the routing table is greater than the value of the parameter number, routes are processed as follows: ● If **route-unchanged** is configured, routes in the routing table remain unchanged. ● If **route-unchanged** is not configured, all routes in the routing table are deleted and then re-added.	-
simply-alert	Indicates that when the number of VPN route prefixes exceeds *number*, prefixes can still join the VPN routing table and alarms are displayed. On the device, however, the subsequent VPN route prefixes are discarded after the total number of the unicast prefixes of the private network and the public network reaches the upper limit.	-

Views

VPN instance view, VPN instance IPv4 address family view or VPN instance IPv6 address family view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If many useless route prefixes imported into a VPN instance constitute a large proportion of the route prefixes on a device, run the **prefix limit** command to set a limit on the maximum number of prefixes supported by the VPN instance. After the **prefix limit** command is run in the current VPN instance address family, if the number of route prefixes reaches the set limit, the system will generate an alarm to instruct the user to check the validity of route prefixes of the VPN instance.

The **prefix limit** command enables the system to display a message when the number of route prefixes added to the routing table of the VPN instance IPv6 address family exceeds the limit. If you run the **prefix limit** command to increase the maximum number of route prefixes in the VPN instance IPv6 address family or run the **undo prefix limit** command to cancel the limit, the system adds the excess route prefixes to the VPN IP routing table.

When the number of route prefixes exceeds the limit, direct routes and static routes can still be added to the routing table of the VPN instance IPv6 address family.

Prerequisites

The **route-distinguisher** command has been executed to set the RD of the VPN instance.

Precautions

The **prefix limit** command can prevent the routing table of the current VPN instance address family on a PE from importing too many route prefixes, but cannot prevent the PE from importing excessive route prefixes from other PEs. Therefore, configuring both the **prefix limit** and **peer route-limit** commands is recommended.

Do not run both the **routing-table limit** (the command restricts the number of routes) and **prefix limit** (the command restricts the number of route prefixes) commands in the current VPN instance address family. Configure either one of them based on your need.

Example

# Configure the system to only generate alarms when the number of prefixes exceeds the maximum number 1000 in the VPN instance named vpn1.

```
<HUAWEI> system-view
[HUAWEI] ip vpn-instance vpn1
[HUAWEI-vpn-instance-vpn1] ipv4-family
[HUAWEI-vpn-instance-vpn1-af-ipv4] route-distinguisher 100:1
[HUAWEI-vpn-instance-vpn1-af-ipv4] prefix limit 1000 simply-alert
```

10.4.50 route-distinguisher

Function

The **route-distinguisher** command configures a route distinguisher (RD) for a VPN instance address family.

By default, no RD is configured for the VPN instance address family.

Format

route-distinguisher *route-distinguisher*

Parameters

Parameter	Description	Value
route-distinguisher	Specifies the value of an RD. The forms of RD are as follows: ● 2-byte AS number:4-byte user-defined number, for example, 101:3. An AS number ranges from 0 to 65535. A user-defined number ranges from 0 to 4294967295. The AS number and the user-defined number cannot be 0s at the same time. That is, an RD cannot be 0:0. ● Integral 4-byte AS number:2-byte user-defined number, for example, 65537:3. An AS number ranges from 65536 to 4294967295. A user-defined number ranges from 0 to 65535. The AS number and user-defined number cannot be both 0s. That is, an RD cannot be 0:0. ● 4-byte AS number in dotted notation:2-byte user-defined number, for example, 0.0:3 or 0.1:0. A 4-byte AS number in dotted notation is in the format of *x.y*, where *x* and *y* are integers that range from 0 to 65535 and from 0 to 65535, respectively. A user-defined number ranges from 0 to 65535. The AS number and user-defined number cannot be both 0s. That is, an RD cannot be 0.0:0. ● IPv4-address:2-byte user-defined number, for example, 192.168.122.15:1. An IP address ranges from 0.0.0.0 to 255.255.255.255. A user-defined number ranges from 0 to 65535.	-

Views

VPN instance view, VPN instance IPv4 address family view, VPN instance IPv6 address family view, EVPN instance view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After creating a VPN instance and enabling the IPv4 or IPv6 address family for the VPN instance, you need to run the **route-distinguisher** command to configure an RD for the address family.

Different VPN instances may have the same route prefix. To allow a PE to determine to which VPN instance a route belongs, run the **route-distinguisher** command to configure an RD for an address family of a VPN instance on the PE. After the configuration, the PE will add an RD to the route received from the VPN instance, and then the route prefix becomes a globally unique VPNv4 or VPNv6 route.

Configuration Impact

An RD configured for the IPv4 or IPv6 address family of a VPN instance cannot be directly modified or deleted. Before modifying an RD, you need to disable the IPv4 or IPv6 address family of the VPN instance or delete the VPN instance and then reconfigure the address family or the VPN instance.

Precautions

Configuring a unique RD for the IPv4 or IPv6 address family of a VPN instance is recommended; otherwise, route overlap may occur.

When the **route-distinguisher** command is run in the VPN instance view, an **ipv4-family** command is created at the same time by default. The command results are equivalent to running the **ipv4-family** command in the VPN instance view and then running the **route-distinguisher** command in the VPN instance IPv4 address family view. For example:

```
[HUAWEI-vpn-instance-vpn1] route-distinguisher 200:1
[HUAWEI-vpn-instance-vpn1-af-ipv4] display this
#
 ipv4-family
  route-distinguisher 200:1
#
return
```

Example

# Configure an RD for the VPN instance named **vpn1**.

```
<HUAWEI> system-view
[HUAWEI] ip vpn-instance vpn1
[HUAWEI-vpn-instance-vpn1] ipv4-family
[HUAWEI-vpn-instance-vpn1-af-ipv4] route-distinguisher 22:1
```

10.4.51 routing-table limit

Function

The **routing-table limit** command sets the maximum number of routes that the current VPN instance address family supports.

The **undo routing-table limit** command restores the maximum number of routes that the current VPN instance address family can support to the default setting.

By default, there is no limit on the maximum number of routes that the current VPN instance address family can support, but the total number of private network and public network routes on a device cannot exceed the allowed maximum number of unicast routes.

Format

routing-table limit *number* { *alert-percent* | **simply-alert** }

undo routing-table limit

Parameters

Parameter	Description	Value
number	Specifies the maximum number of routes supported by a VPN instance.	The value is an integer, and the minimum value is 1. The maximum number is determined by the license file.
alert-percent	Specifies the percentage of the maximum number of routes. When the maximum number of routes that join the VPN instance is up to the value (*number***alert-percent*)/100, the system prompts alarms. The VPN routes can be still added to the routing table, but after the number of routes reaches *number*, the subsequent routes are dropped.	An integer ranging from 1 to 100.
simply-alert	Indicates that when VPN routes exceed *number*, routes can still be added into the routing table, but the system prompts alarms. However, after the total number of VPN routes and network public routes reaches the unicast route limit specified in the License, the subsequent VPN routes are dropped.	-

Views

VPN instance view, VPN instance IPv4 address family view or VPN instance IPv6 address family view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If many useless routes imported into a VPN instance constitute a large proportion of the routes on a device, run the **routing-table limit** command to set a limit on the maximum number of routes supported by the VPN instance. After the **routing-table limit** command is run in the current VPN instance address family, if the number of routes of the VPN instance reaches the set limit, the system will generate an alarm to instruct the user to check the validity of routes of the VPN instance.

The **routing-table limit** command enables the system to display a message when the number of routes added to the routing table of the VPN instance IPv6 address family exceeds the limit. If you run the **routing-table limit** command to increase the maximum number of routes in the VPN instance IPv6 address family or run the **undo routing-table limit** command to cancel the limit, the system adds the excess routes to the VPN IP routing table.

Prerequisites

1. The **ip vpn-instance** command has been executed to create a VPN instance and enter the VPN instance view.
2. The **ipv4-family** or **ipv6-family** command has been executed to enter the IPv4 or IPv6 VPN instance address family view.
3. The **route distinguisher** command has been executed to set the RD of the VPN instance.

Precautions

Using the **routing-table limit** command prevents the routing table of the current VPN instance address family on a PE from importing too many routes, but cannot prevent the PE from importing excessive routes from other PEs. Therefore, configuring both the **routing-table limit** and **peer route-limit** commands is recommended.

Do not run both the **routing-table limit** (the command restricts the number of routes) and **prefix limit** (the command restricts the number of route prefixes) commands in the current VPN instance address family. Configure either one of them based on your need.

If the remote cross routes learned using MP-IBGP and the BGP routes learned from CEs failed to be added to the routing table, the system automatically refreshes the routing table to add these routes.

Example

# Configure the maximum number of routes for the IPv4 address family of the VPN instance named vpn1 to 1000, and when VPN routes exceed 1000, routes can still be added into the routing table, but the system prompts alarms.

```
<HUAWEI> system-view
[HUAWEI] ip vpn-instance vpn1
[HUAWEI-vpn-instance-vpn1] ipv4-family
[HUAWEI-vpn-instance-vpn1-af-ipv4] route-distinguisher 100:1
[HUAWEI-vpn-instance-vpn1-af-ipv4] routing-table limit 1000 simply-alert
```

10.4.52 rr-filter

Function

The **rr-filter** command creates a reflection policy for the route reflectors.

The **undo rr-filter** command removes the configuration.

By default, no reflection policy for a route reflector is created.

Format

rr-filter { *extcomm-filter-number* | *extcomm-filter-name* }

undo rr-filter

Parameters

Parameter	Description	Value
extcomm-filter-number	specifies the number of the extended community filter supported by the route-reflector group. You can specify only one extended community filter each time.	It is an integer that ranges from 1 to 399.
extcomm-filter-name	specifies the name of the extended community filter supported by the route-reflector group. You can specify only one extended community filter each time.	The name is a string of 1 to 51 characters without any space. It is case-sensitive. When double quotation marks are used around the string, spaces are allowed in the string.

Views

BGP-VPNv4 address family view, BGP-VPNv6 address family view, BGP-MDT address family view, BGP-MVPN address family view

Default Level

2: Configuration level

Usage Guidelines

Full-mesh connections need to be established between IBGP peers in an AS to ensure the connectivity between the IBGP peers. When there are many IBGP peers, it is costly to establish a fully-meshed network. An RR or a confederation can be used to solve the problem. Only the IBGP route of which route-target extended community attribute meets the matching rules can be reflected. This allows load balancing among RRs.

Example

# Create a route-reflector group, and enable the automatic filtering for VPNv4 route updates on the outbound interface. The group should be created on the basis of the permitted route target extended community attributes.

```
<HUAWEI> system-view
[HUAWEI] bgp 100
[HUAWEI-bgp] ipv4-family vpnv4
[HUAWEI-bgp-af-vpnv4] rr-filter 10
```

10.4.53 service-id (VPN instance view)

Function

The **service-id** command sets a service ID for a VPN instance.

The **undo service-id** command deletes the service ID of a VPN instance.

By default, no service ID is set for a VPN instance.

Format

service-id *service-id*

undo service-id

Parameters

Parameter	Description	Value
service-id	Specifies the service ID of a VPN instance.	An integer ranging from 1 to 4294967295.

Views

VPN instance view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A service ID set in the view of a VPN instance identifies the service of the VPN instance, which facilitates later service query using the NMS.

A service ID is unique on a device. It distinguishes a VPN service from other VPN services on the network. A service ID used by a VPN instance cannot be allocated to other VPN instances.

Configuration Impact

If the **service-id** command is run repeatedly, the last configuration overrides the previous ones.

Example

# Set a service ID for a VPN instance.

```
<HUAWEI> system-view
[HUAWEI] ip vpn-instance vrf1
[HUAWEI-vpn-instance-vrf1] service-id 123
```

10.4.54 source

Function

The **source** command configures the source address or source interface of the tunnel.

The **undo source** command deletes the configured source address or source interface.

The source address and source interface of a tunnel are not specified by default.

Format

source { *source-ip-address* | *interface-type interface-number* }

undo source

Parameters

Parameter	Description	Value
source-ip-address	Specifies the source address of a tunnel interface. If a tunnel interface works in IPv4-IPv6 mode, specify an IPv6 address as the source address of the tunnel interface.	The IPv4 address is in dotted decimal notation. The IPv6 address is a 32-digit hexadecimal number, in the format X:X:X:X:X:X:X:X.
interface-type interface-number	Specifies the type and the number of the source interface of the tunnel. The following types of interfaces are often used: VLANIF and loopback.	-

Views

Tunnel interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When configuring a GRE, MPLS TE, IPv4 over IPv6 tunnel or manual IPv6 over IPv4 tunnel, create a tunnel interface. After a tunnel interface is created, run the **source** command to specify the source IP address for the tunnel interface.

Prerequisites

A tunnel interface has been created using the **interface tunnel** command, and the encapsulation mode is set to GRE, MPLS TE, IPv4 over IPv6 or IPv6 over IPv4 of manual mode using the **tunnel-protocol** command.

Precautions

Two tunnel interfaces with the same encapsulation mode, source address, and destination address cannot be configured simultaneously.

You can configure a main interface working in Layer 3 mode as the source tunnel interface.

On the GRE, MPLS TE, IPv4 over IPv6 tunnel or manual IPv6 over IPv4 tunnel, the source address of the local tunnel interface is the destination address of the remote tunnel interface, and the destination address of the local tunnel interface is the source address of the remote tunnel interface.

Example

# Set the tunnel type of Tunnel1 to IPv6 over IPv4 of manual mode and configure the source IP address of Tunnel1 as 10.1.1.1.

```
<HUAWEI> system-view
[HUAWEI] interface tunnel 1
[HUAWEI-Tunnel1] tunnel-protocol ipv6-ipv4
[HUAWEI-Tunnel1] source 10.1.1.1
```

# Configure Tunnel1 of GRE and use Loopback1 address as the interface address.

```
<HUAWEI> system-view
[HUAWEI] interface Loopback 1
[HUAWEI-LoopBack1] ip address 10.2.1.1 32
[HUAWEI-LoopBack1] quit
[HUAWEI] interface tunnel 1
[HUAWEI-Tunnel1] tunnel-protocol gre
[HUAWEI-Tunnel1] source loopback 1
```

10.4.55 supernet label-route advertise

Function

The **supernet label-route advertise disable** command disables a BGP device from advertising BGP supernet labeled routes.

The **undo supernet label-route advertise disable** or **supernet label-route advertise enable** command restores the default configuration.

By default, BGP supernet labeled routes can be preferentially selected and advertised.

Format

supernet label-route advertise disable

supernet label-route advertise enable

undo supernet label-route advertise disable

Parameters

None

Views

BGP view, BGP-IPv4 unicast address family view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A BGP supernet route has the same destination address and next hop address or has a more detailed destination address than the next hop address. Any route that meets one of the following conditions is a BGP supernet route.

- If you perform bitwise AND operations on the destination address mask with the destination address and next hop address, respectively, the calculated network addresses are the same, and the destination address mask is greater than or equal to the next hop address mask.
- If you perform bitwise AND operations on the destination address mask with the destination address and next hop address, respectively, the calculated network addresses are different. However, if you perform bitwise AND operations on the next hop address mask with the destination address and next hop address, respectively, the calculated network addresses are the same.

For example, the route destined for 10.6.6.6 in the following command output is a BGP supernet route.

```
<HUAWEI> display bgp routing-table
 BGP Local router ID is 10.1.1.2
 Status codes: * - valid, > - best, d - damped,
               h - history,  i - internal, s - suppressed, S - Stale
               Origin : i - IGP, e - EGP, ? - incomplete

 Total Number of Routes: 1
       Network            NextHop        MED        LocPrf    PrefVal Path/Ogn
   *>i  10.6.6.6/32        10.6.6.6       0          100       0      ?
```

Example

# Disable a BGP device from advertising BGP supernet labeled routes.

```
<HUAWEI> system-view
[HUAWEI] bgp 100
[HUAWEI-bgp] ipv4-family unicast
[HUAWEI-bgp-af-ipv4] supernet label-route advertise disable
```

10.4.56 tunnel binding

Function

The **tunnel binding** command binds a specified tunnel to the destination IP address. Therefore, the tunnel can be used by a specified VPN.

The **undo tunnel binding** command cancels the binding.

By default, a tunnel is not bound to any IP address.

Format

tunnel binding destination *dest-ip-address* **te** { **tunnel** *interface-number* } &<1-6> [**ignore-destination-check**] [**down-switch**]

undo tunnel binding destination *dest-ip-address*

Parameters

Parameter	Description	Value
dest-ip-address	Specifies the destination address of the tunnel.	-
interface-number	Specifies the interface number of the bound tunnel interface.	-
ignore-destination-check	Specifies whether to ignore destination consistency check. If this parameter is enabled, a tunnel policy selects a TE tunnel for route recursion even if the destination address of that TE tunnel is different from the destination address specified in the tunnel policy.	-
down-switch	Indicates that the tunnel switchover is enabled. After this parameter is configured, an available tunnel, with the priority as LSP, CR-LSP, is adopted when the bound TE tunnel fails.	-

Views

Tunnel policy view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A tunnel policy determines the selection of proper tunnels for VPN services. There are two types of tunnel policies. Only one policy type can be configured in the tunnel policy view.

- Tunnel type prioritizing policy: Such a policy specifies the sequence in which different types of tunnels are selected. The **tunnel select-seq** command is used to configure a tunnel type prioritizing policy.
- Tunnel binding policy: Such a policy binds a tunnel to a VPN for service transmission. The **tunnel binding** command is used to configure a tunnel binding policy.

Only MPLS TE tunnels can be bound to VPNs. The **tunnel binding** command can specify the MPLS TE tunnels that are used for VPN binding, facilitating QoS deployment. If some VPN services have high requirements for QoS, run the **tunnel binding** command to use specific MPLS TE tunnels to transmit these VPN services.

Prerequisites

The **tunnel-policy** command is run to create a tunnel policy.

The **mpls te reserved-for-binding** command is run in the view of the tunnel interface to be bound to an MPLS TE tunnel.

Precautions

The **tunnel binding** command can be run repeatedly in the tunnel policy view so long as the value of *dest-ip-address* varies.

Apply the tunnel binding policy to the VPN instance so that the VPN instance can have its routes recursing to the bound MPLS TE tunnel.

Example

# Bind the IP address of the remote PE, 10.2.2.9, to the local tunnel interface Tunnel1 in the tunnel policy view.

```
<HUAWEI> system-view
[HUAWEI] tunnel-policy tnlpolicyname
[HUAWEI-tunnel-policy-tnlpolicyname] tunnel binding destination 10.2.2.9 te tunnel 1
```

10.4.57 tunnel-selector (system view)

Function

The **tunnel-selector** command creates a tunnel selector and displays the tunnel selector view.

The **undo tunnel-selector** command cancels the setting.

By default, no tunnel selector is created.

Format

tunnel-selector *tunnel-selector-name* { **permit** | **deny** } **node** *node*

undo tunnel-selector *tunnel-selector-name* [**node** *node*]

Parameters

Parameter	Description	Value
tunnel-selector-name	Specifies the name of a tunnel selector.	The value is a string of 1 to 40 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Parameter	Description	Value
permit	Specifies the matching mode of the tunnel selector to **permit**. If a route matches all the **if-match** clauses of a node, the route matches the node and all the actions defined by the **apply** clause are performed on the route. If a route does not match one **if-match** clause of a node, the route continues to match the next node.	-
deny	Specifies the matching mode of the tunnel selector to **deny**. If a route matches all the **if-match** clauses of a node, the route is denied and does not match the next node.	-
node *node*	Specifies the index of the node of the tunnel selector. The route first matches the node with a smaller index value.	The value is an integer ranging from 0 to 65535.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **tunnel-selector** command is often used in BGP/MPLS IP VPN networking. A tunnel selector needs to be created in the following scenarios:

- The SPE in the HVPN networking needs to apply a tunnel policy to VPNv4 routes that are received from UPEs.

Follow-up Procedure

Configure the following clauses after creating a tunnel selector (each node of the tunnel selector consists of two parts):

- **if-match** clause: sets filtering conditions on a node. To filter routes by RD, run the **if-match rd-filter** command. To filter routes by next hop, run the **if-match ip next-hop** command.
- **apply** clause: applies a tunnel policy to the routes filtered by the **if-match** clause using the **apply tunnel-policy** command.

In addition, the system will have routes recursing to expected tunnels only after applying a tunnel selector. The **tunnel-selector** command can be run in the BGP view for the application of a tunnel selector.

Precautions

A change in the tunnel selector may cause VPN services to be interrupted because BGP-VPNv4 or BGP labeled routes may fail to recurse to tunnels.

Example

# Create a tunnel selector named tps, and set the node number to 10 and the matching mode to **permit**.

```
<HUAWEI> system-view
[HUAWEI] tunnel-selector tps permit node 10
[HUAWEI-tunnel-selector]
```

10.4.58 tunnel-selector (BGP-VPNv4 address family view)

Function

The **tunnel-selector** command applies a tunnel selector to BGP-VPNv4 or BGP labeled routes.

The **undo tunnel-selector** command cancels the configuration.

By default, no tunnel selector is applied to BGP-VPNv4 or BGP labeled routes. BGP-VPNv4 or BGP labeled route recurse only to LSPs.

Format

tunnel-selector *tunnel-selector-name*

undo tunnel-selector

Parameters

Parameter	Description	Value
tunnel-selector-name	Specifies the name of a tunnel policy selector.	The value is a string of 1 to 40 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Views

BGP-VPNv4 address family view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **tunnel-selector** command is often used in BGP/MPLS IP VPN networking. It can be used in the following scenarios to apply a tunnel selector to BGP-VPNv4 or BGP labeled routes:

- The SPE in the HVPN networking needs to apply a tunnel policy to VPNv4 routes that are received from UPEs.

Prerequisites

The **tunnel-selector** command is run to create a tunnel selector.

Precautions

Deleting the tunnel selector applied to BGP-VPNv4 or BGP labeled routes may cause VPN service interruption because the BGP-VPNv4 or BGP labeled routes may fail to recurse to tunnels.

Example

# Apply a tunnel selector to BGP labeled routes.

```
<HUAWEI> system-view
[HUAWEI] bgp 100
[HUAWEI-bgp] ipv4-family vpnv4
[HUAWEI-bgp-af-vpnv4] tunnel-selector tps
```

10.4.59 tunnel select-seq

Function

The **tunnel select-seq** command specifies the priority sequence of the tunnels taking part in load balancing.

The **undo tunnel select-seq load-balance-number** command restores the default setting.

By default, only LDP LSPs, BGP LSP or static LSPs are selected and no load balancing is performed.

Format

tunnel select-seq { **gre** | **lsp** | **cr-lsp** } * **load-balance-number** *load-balance-number*

undo tunnel select-seq

Parameters

Parameter	Description	Value
gre	Specifies a GRE tunnel. **NOTE** This parameter is not supported in this version.	-

Parameter	Description	Value
lsp	Specifies the LDP LSPs, BGP LSP or static LSPs. **NOTE** This parameter is not supported by the S5731S-S, S6730S-S, and S6735-S.	-
cr-lsp	Specifies the CR-LSP tunnel. **NOTE** This parameter is not supported by the S5731S-S, S6730S-S, and S6735-S.	-
load-balance-number	Specifies the number of tunnels taking part in load balancing.	The value is an integer that ranges from 1 to 6.

Views

Tunnel policy view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

By default, a VPN instance uses LSPs for service transmission on the backbone network. To use other types of tunnels or configure load balancing for service transmission of the VPN instance, you need to apply a tunnel policy to the VPN instance.

Precautions

A tunnel policy determines the selection of proper tunnels for VPN services. There are two types of tunnel policies.

- Tunnel type prioritizing policy: Such a policy specifies the sequence in which different types of tunnels are selected. The **tunnel select-seq** command is used to configure a tunnel type prioritizing policy.
- Tunnel binding policy: Such a policy binds a tunnel to a VPN for service transmission. The **tunnel binding** command is used to configure a tunnel binding policy.

If the **tunnel select-seq** command is run, the VPN instance preferably selects the tunnel type with the highest priority according to the specified sequence. For example, after the **tunnel select-seq cr-lsp lsp load-balance-number 2** command is run in the tunnel policy view, the VPN instance will select CR-LSPs to transmit services on the backbone network.

- If two or more CR-LSPs are available on the network, the VPN instance randomly selects two of them for service transmission.
- If no CR-LSP or only one CR-LSP is available on the network, the VPN instance selects LSPs as substitutes with the existing CR-LSP for service transmission.
- If the number of tunnels used by the VPN instance is reduced to 1, the VPN instance uses the tunnel policy to re-select tunnels.

If **lsp** is specified in the command, three types of LSPs can serve as candidate tunnels: LDP LSP, BGP LSP, and static LSP. The priority sequence of these LSPs taking part in load balancing is LDP LSP > BGP LSP > static LSP. For example, if the **tunnel select-seq lsp cr-lsp load-balance-number 3** command is configured for the tunnel policy:

- If three or more LDP LSPs are available on the network, the VPN instance randomly selects three of them for service transmission.
- If less than three LDP LSPs are available on the network, the VPN instance selects BGP LSPs as substitutes to ensure that three LSPs work in load balancing mode to transmit services.
- If the total number of LDP and BGP LSPs available on the network is less than 3, the VPN instance selects static LSPs as substitutes to ensure that three LSPs work in load balancing mode to transmit services.

After the **tunnel select-seq** command is executed, apply the configured tunnel policy to the VPN instance so that the VPN instance can select tunnels based on the tunnel policy and have its services load-balanced across tunnels.

The load balancing mode configured using the **tunnel select-seq** command in a tunnel policy takes effect only for L3VPN.

Example

# Configure a tunnel policy that only LDP LSPs, BGP LSP or static LSPs can be used and no load balancing is performed.

```
<HUAWEI> system-view
[HUAWEI] tunnel-policy l2
[HUAWEI-tunnel-policy-l2] tunnel select-seq lsp load-balance-number 1
```

10.4.60 tunnel-policy nonexistent-config-check

Function

The **tunnel-policy nonexistent-config-check** command configures whether a nonexistent tunnel policy can be specified in a command.

The **undo tunnel-policy nonexistent-config-check disable** command configures only an existing tunnel policy can be specified in a command.

By default, only an existing tunnel policy can be specified in a command.

Format

tunnel-policy nonexistent-config-check { **disable** | **enable** }

undo tunnel-policy nonexistent-config-check disable

Parameters

Parameter	Description	Value
disable	Indicates that a nonexistent tunnel policy can be specified in a command.	-
enable	Indicates that only an existing tunnel policy can be specified in a command.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

By default, if you specify a nonexistent tunnel policy in a command, the command does not take effect.

If you need the nonexistent tunnel policy can be specified in a command, run the **tunnel-policy nonexistent-config-check disable** command.

Example

# Indicates that a nonexistent tunnel policy can be specified in a command.

```
<HUAWEI> system-view
[HUAWEI] tunnel-policy nonexistent-config-check disable
```

10.4.61 tunnel-policy (system view)

Function

The **tunnel-policy** command creates a tunnel policy and displays the tunnel policy view.

The **undo tunnel-policy** command deletes the specified tunnel policy.

By default, no tunnel policy is created in the system.

Format

tunnel-policy *policy-name*

undo tunnel-policy *policy-name*

Parameters

Parameter	Description	Value
policy-name	Displays the name of a tunnel policy.	The value is a string of 1 to 39 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

By default, a VPN instance selects LSPs without performing load balancing based on the default tunnel policy. If you want to make a change, run the **tunnel-policy** command to create a tunnel policy.

There are two types of tunnel policies:

- Tunnel type prioritizing policy: It specifies the sequence in which different types of tunnels are selected and the number of tunnels taking part in load balancing.
- Tunnel binding policy: It binds a tunnel to a destination address. In this manner, the VPN traffic bound for the destination address enters the bound tunnel only, and as a result, QoS is guaranteed for the VPN traffic.

Precautions

If you change the tunnel policy in a VPN instance, VPN services may be interrupted due to a possibility of recursion failures.

Run one of the following commands to perform further configuration on the created tunnel policy:

- To configure the tunnel policy as a tunnel type prioritizing policy, run the **tunnel select-seq** command.
- To configure the tunnel policy as a tunnel binding policy, run the **tunnel binding** command.

The system can select tunnels for a VPN instance based on a tunnel policy only after the tunnel policy is applied to the VPN instance. The mode in which a tunnel policy is applied to a VPN instance varies according to the VPN type.

Example

# Create a tunnel policy named policy1 and enter the tunnel policy view.

```
<HUAWEI> system-view
[HUAWEI] tunnel-policy policy1
[HUAWEI-tunnel-policy-policy1]
```

10.4.62 tunnel-protocol

Function

The **tunnel-protocol** command configures the tunnel protocol on a tunnel interface.

The **undo tunnel-protocol** command restores the tunnel protocol to the default configuration.

By default, no tunnel protocol is used on a tunnel interface.

Format

tunnel-protocol { **gre** | **ipv6-ipv4** [**6to4** | **isatap**] | **ipv4-ipv6** | **mpls te** | **none** }

undo tunnel-protocol

Parameters

Parameter	Description	Value
gre	Indicate that the GRE tunnel protocol is configured on a tunnel 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 the parameters.	-
ipv4-ipv6	Indicate that the IPv4 to IPv6 tunnel protocol is configured on a tunnel interface. **NOTE** Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S support the parameter.	-
ipv6-ipv4 [**6to4** | **isatap**]	Configure the tunnel protocol of the tunnel interface as ipv6-ipv4: ● **ipv6-ipv4**: use a manual IPv6 over IPv4 tunnel ● **ipv6-ipv4 6to4** : using 6to4 tunnel ● **ipv6-ipv4 isatap** : using isatap tunnel **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 these parameter.	-

Parameter	Description	Value
mpls te	Indicate that the MPLS TE tunnel protocol is configured on a tunnel interface. **NOTE** Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6720-EI, S6720S-EI, S6730-H, S6730-S, S6730S-S, and S6730S-H support the parameter.	-
none	Indicate that no tunnel protocol is configured on a tunnel interface.	-

Views

Tunnel interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After creating a tunnel interface using the **interface tunnel** command, run the **tunnel-protocol** command to configure the tunnel encapsulation mode for the tunnel interface.

The following tunnel encapsulation modes are available:

- GRE: encapsulates packets of some network layer protocols such as IP or IPX to enable these encapsulated packets to be transmitted on networks running other protocols such as IP.
- IPv4-IPv6: creates tunnels on the IPv6 networks to connect IPv4 isolated sites so that IPv4 isolated sites can access other IPv4 networks through the IPv6 public network.
- IPv6-IPv4: creates tunnels on the IPv4 networks to connect IPv6 isolated sites so that IPv6 packets can be transmitted on IPv4 networks.
- MPLS TE: integrates the MPLS technology with traffic engineering. It can reserve resources by setting up LSP tunnels for a specified path in an attempt to avoid network congestion and balance network traffic.

Precautions

- The **none** mode indicates the initial configuration, that is, no tunnel encapsulation mode is configured. In practice, you must select another tunnel encapsulation mode.
- You must configure the tunnel encapsulation mode before setting the source IP address or other parameters for a tunnel interface. Changing the encapsulation mode of a tunnel interface deletes other parameters of the tunnel interface.

Example

# Set the tunnel encapsulation mode of Tunnel2 to GRE.

```
<HUAWEI> system-view
[HUAWEI] interface tunnel 2
[HUAWEI-Tunnel2] tunnel-protocol gre
```

10.4.63 tnl-policy

Function

The **tnl-policy** command associates a tunnel policy with the current VPN instance address family.

The **undo tnl-policy** command dissociates the current VPN instance address family from a tunnel policy.

By default, no tunnel policy is associated with the VPN instance address family. By default, a tunnel is selected for a VPN in the sequence of the LSP, CR-LSP, and Local_IfNet, and no load balancing is performed.

Format

tnl-policy *policy-name*

undo tnl-policy

Parameters

Parameter	Description	Value
policy-name	Specifies the name of the tunnel policy to be associated with the VPN instance address family.	The value is a string of 1 to 39 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Views

VPN instance view, VPN instance IPv4 address family view, VPN instance IPv6 address family view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

By default, a device only uses an LSP tunnel to forward data on the backbone network and cannot implement multi-path load balancing at the same time. To ensure transmission quality of services and specify a TE tunnel to transmit VPN services, or to improve transmission efficiency and implement load balancing, run the **tunnel-policy** command to configure a tunnel policy and run the **tnl-policy** command to reference the tunnel policy in the VPN address family view.

Prerequisites

1. The **ip vpn-instance** command has been executed to create a VPN instance and enter the VPN instance view.
2. The **ipv4-family** command has been executed to create a VPN instance and enter the VPN instance IPv4 address family view.
3. The **route distinguisher** command has been executed to set the RD of the VPN instance.

Precautions

If the tunnel policy associated with a VPN instance enabled with the address family cannot match an existing tunnel on the network, the routes in the VPN instance enabled with the address family will have routes recursing to tunnels based on the default tunnel policy. If the recursion fails, services will be interrupted.

If the address family of a VPN instance changes or the associated tunnel policy is deleted, VPN services will be interrupted for a short time even if tunnels matching the tunnel policy are available on the network. Therefore, use the **tnl-policy** command with caution.

Follow-up Procedure

If the associated tunnel policy does not exist, run the **tunnel-policy** command to create the tunnel policy.

Example

# Associate a tunnel policy named **po1** with the VPN instance named *vpn2*.

```
<HUAWEI> system-view
[HUAWEI] tunnel-policy po1
[HUAWEI-tunnel-policy-po1] tunnel select-seq lsp load-balance-number 2
[HUAWEI-tunnel-policy-po1] quit
[HUAWEI] ip vpn-instance vpn2
[HUAWEI-vpn-instance-vpn2] ipv4-family
[HUAWEI-vpn-instance-vpn2-af-ipv4] route-distinguisher 100:1
[HUAWEI-vpn-instance-vpn2-af-ipv4] tnl-policy po1
```

10.4.64 transit-vpn

Function

The **transit-vpn** command ensures that the status of a VRF (VPN Routing and Forwarding table) obtained from MIB is always Up, no matter whether this VRF is bound to interfaces.

The **undo transit-vpn** command restores the default setting.

By default, the status of a VRF obtained from MIB is Up only if it is bound to at least one interface in the Up state.

NOTE

Only the following switch models support this command:

S5731-S, S5731S-S, S5731-H, S5731S-H, S5732-H, S6730-S, S6730S-S, S6735-S, S6720-EI, S6720S-EI, S6730S-H, and S6730-H

Format

transit-vpn

undo transit-vpn

Parameters

None.

Views

VPN instance view or VPN instance IPv4 address family view

Level

2: Configuration level

Usage Guidelines

Usage Scenario

According to RFC, the status of a VRF obtained from MIB is Up only if it is bound to at least one interface in the Up state. In the HoVPN or H-VPN networking, however, a VRF does not need to be bound to any interface. If the VRF is not bound to an interface in this networking, the status of the VRF obtained from MIB is Down by default.

In this case, you can run the **transit-vpn** command to ensure that the status of a VRF obtained from MIB is always Up.

Prerequisites

The **route-distinguisher** command has been executed to set the RD of the VPN instance.

Example

# Configure the status of the VRF vpna obtained from MIB to be always Up, no matter whether the VRF is bound to interfaces.

```
<HUAWEI> system-view
[HUAWEI] ip vpn-instance vpna
[HUAWEI-vpn-instance-vpna] ipv4-family
[HUAWEI-vpn-instance-vpna-af-ipv4] route-distinguisher 100:1
[HUAWEI-vpn-instance-vpna-af-ipv4] transit-vpn
```

10.4.65 undo vpn frr all

Function

Using the **undo vpn frr all** command, you can disable VPN FRR in all the VPN instances.

Format

undo vpn frr all

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The VPN FRR function may be configured in multiple VPN instances on a device. The **undo vpn frr** command takes a long time to cancel the VPN FRR function of all VPN instances one by one.

In the system view, run the **undo vpn frr all** command to simultaneously cancel the VPN FRR function of IPv4 and IPv6 address families in all VPN instances.

Precautions

To cancel the VPN FRR function of a VPN instance, run the **undo vpn frr** command.

Example

# Disable VPN FRR of all the VPN instances in the system view.

```
<HUAWEI> system-view
[HUAWEI] undo vpn frr all
```

10.4.66 vpn-route cross multipath

Function

The **vpn-route cross multipath** command adds multiple VPNv4 or VPNv6 routes to a VPN instance with a different RD from these routes' RDs.

The **undo vpn-route cross multipath** command restores the default configuration.

By default, if the RDs of multiple VPNv4 or VPNv6 routes are different from the RD of a VPN instance, only the optimal route is added to the VPN instance.

Format

vpn-route cross multipath

undo vpn-route cross multipath

Parameters

None

Views

BGP-VPN instance IPv4 address family view or BGP-VPN instance IPv6 address family view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

By default, if the RD of the VPN instance on the local PE is different from the RDs of the VPN instances on multiple remote PEs, and the RDs of the VPN instances on remote PEs are the same, the local PE adds only the optimal route to the VPN instance after receiving VPNv4 or VPNv6 routes with the same destination address from the remote PEs. As a result, load balancing or VPN FRR does not take effect. To resolve this problem, run the **vpn-route cross multipath** command on the local PE.

Configuration Impact

After you run the **vpn-route cross multipath** command, the local PE adds multiple VPNv4 or VPNv6 routes to a VPN instance with a different RD from these routes' RDs. The number of VPNv4 or VPNv6 routes that can be added to the VPN instance depends on whether load balancing or VPN FRR is configured.

- If no load balancing is configured, a maximum of two VPNv4 or VPNv6 routes can be added to the VPN instance.
- If you set the maximum number of equal-cost routes for load balancing to *n* using the **maximum load-balancing** command, *n* VPNv4 or VPNv6 routes can be added to the VPN instance.
- If you configure VPN FRR and set the maximum number of equal-cost routes for load balancing to *n* using the **maximum load-balancing** and **auto-frr** command, *n* + 1 VPNv4 or VPNv6 routes can be added to the VPN instance.

Example

# Add multiple VPNv4 routes to a VPN instance with a different RD from these routes' RDs.

```
<HUAWEI> system-view
[HUAWEI] bgp 100
[HUAWEI-bgp] ipv4-family vpn-instance vrf1
[HUAWEI-bgp-vrf1] vpn-route cross multipath
```

# Add multiple VPNv6 routes to a VPN instance with a different RD from these routes' RDs.

```
<HUAWEI> system-view
[HUAWEI] bgp 100
[HUAWEI-bgp] ipv6-family vpn-instance vrf1
[HUAWEI-bgp6-vrf1] vpn-route cross multipath
```

10.4.67 vpn-target

Function

The **vpn-target** command configures the export or import VPN target extended community attribute for the VPN instance address family.

The **undo vpn-target** command deletes the setting.

By default, no export or import VPN target extended community list is configured for the VPN instance address family.

Format

vpn-target *vpn-target* &<1-8> [**both** | **export-extcommunity** | **import-extcommunity**]

undo vpn-target { **all** | *vpn-target* &<1-8> [**both** | **export-extcommunity** | **import-extcommunity**] }

NOTE

Only the following switch models support this command:

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

The S5720I-SI, S5735-S, S5735S-S, S5735-S-I, S5735S-H, S5736-S, and S6720S-S only support the VPN instance view and VPN instance IPv4 address family view.

Parameters

Parameter	Description	Value
vpn-target	Specifies the VPN target extended community attribute to be added to the VPN target extended community list of the VPN instance address family. The forms of VPN targets are as follows: ● 2-byte AS number: 4-byte user-defined number, for example, 1:3. The AS number ranges from 0 to 65535. The user-defined number ranges from 0 to 4294967295. The AS number and the user-defined number cannot both be 0. That is, a VPN target cannot be 0:0. ● IPv4-address: 2-byte user-defined number, for example, 192.168.122.15:1. The IP address ranges from 0.0.0.0 to 255.255.255.255. The user-defined number ranges from 0 to 65535. ● Integral 4-byte AS number:2-byte user-defined number, for example, 65537:3. An AS number ranges from 65536 to 4294967295. A user-defined number ranges from 0 to 65535. The AS number and user-defined number cannot be both 0s. That is, a VPN target cannot be 0:0. ● 4-byte AS number in dotted notation:2-byte user-defined number, for example, 0.0:3 or 0.1:0. A 4-byte AS number in dotted notation is in the format of *x.y*, where *x* and *y* are integers that range from 0 to 65535 and from 0 to 65535, respectively. A user-defined number ranges from 0 to 65535. The AS number and user-defined number cannot be both 0s. That is, a VPN target cannot be 0.0:0.	-
both	Adds the VPN target extended community attribute to the export and import VPN target extended community lists of the VPN instance address family. If none of **both**, **export-extcommunity**, or **import-extcommunity** is specified, **both** is adopted by default.	-
export-extcommunity	Adds the VPN target extended community attribute to the export VPN target extended community lists of the VPN instance address family.	-
import-extcommunity	Adds the VPN target extended community attribute to the import VPN target extended community lists of the VPN instance address family.	-

Parameter	Description	Value
all	Delete all the VPN targets of the VPN instance IPv4 address family.	-

Views

VPN instance view, VPN instance IPv4 address family view, VPN instance IPv6 address family view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If a VPN instance is configured on a PE, the **vpn-target** command must be used to configure a VPN target for the IPv4 or IPv6 address family of the VPN instance.

The VPN target controls route learning between VPN sites. A VPN target may be either an import VPN target or an export VPN target. An export VPN target is contained in a VPNv4 or IPv6 route to be advertised to a remote MP-BGP peer. After receiving a VPNv4 or IPv6 route, an MP-BGP peer compares the received export VPN target with the local import VPN target to determine whether the VPNv4 or IPv6 route can be added to the routing table of the local VPN instance enabled with the IPv4 or IPv6 address family.

Prerequisites

The **route-distinguisher** command has been executed to set the RD of the VPN instance.

Precautions

A VPN target configured using the **vpn-target** command will not overwrite any previously configured VPN target. If the number of configured VPN targets has reached the maximum limit, no VPN target can be added by using the **vpn-target** command.

After a VPN target is configured for the IPv4 or IPv6 address family of a VPN instance, only the routes that match the VPN target will be accepted by the IPv4 or IPv6 address family of the VPN instance.

If all the VPN targets of the IPv4 or IPv6 address family of a VPN instance are deleted using the **undo vpn-target** command, all routes learned by the IPv4 or IPv6 address family of the VPN instance from other VPN instances will be deleted.

Multiple VPN targets can be configured for the IPv4 or IPv6 address family of a VPN instance. One **vpn-target** command can configure a maximum of eight VPN targets at a time. If you want to configure more VPN targets in the VPN instance IPv4 or IPv6 address family view, run the **vpn-target** command multiple times. When VPN routes are advertised between VPN instances, if one of the VPN targets carried in the VPNv4 or IPv6 routes matches the import VPN target of the IPv4 or

IPv6 address family of a local VPN instance, the routes will be added to the routing table of the local VPN instance.

Example

# Add 3:3 to the export VPN target extended community list and 4:4 to the import VPN target extended community list of the VPN instance named *vrf1*.

```
<HUAWEI> system-view
[HUAWEI] ip vpn-instance vrf1
[HUAWEI-vpn-instance-vrf1] ipv4-family
[HUAWEI-vpn-instance-vrf1-af-ipv4] route-distinguisher 100:1
[HUAWEI-vpn-instance-vrf1-af-ipv4] vpn-target 3:3 export-extcommunity
[HUAWEI-vpn-instance-vrf1-af-ipv4] vpn-target 4:4 import-extcommunity
```

10.4.68 vpn frr

Function

Using the **vpn frr** command, you can enable VPN FRR.

Using the **undo vpn frr** command, you can disable VPN FRR.

By default, VPN FRR is disabled.

Format

vpn frr route-policy *route-policy-name*

undo vpn frr

Parameters

Parameter	Description	Value
route-policy *route-policy-name*	Specifies the name of the route-policy.	The name is a string of 1 to 40 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Views

VPN instance view, VPN instance IPv4 address family view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

VPN FRR is applied on a VPN where a CE is dual-homed to two PEs. VPN FRR uses a secondary tunnel to back up the primary tunnel and detects the connectivity of the primary tunnel in combination with rapid detection technologies such as BFD. When a fault occurs on the primary tunnel, a PE configured with VPN FRR can switch VPN traffic to the secondary tunnel before the VPN routes are converged. This improves reliability of data forwarding on the public network.

VPN FRR has two modes: VPN static FRR and VPN auto FRR. The **vpn frr** command configures manual VPN FRR and the **auto-frr** command configures VPN Auto FRR.

Compared with VPN Auto FRR, manual VPN FRR specifies backup next hop more precisely. If manual VPN FRR and VPN Auto FRR are configured simultaneously, manual VPN FRR takes preference over VPN Auto FRR. If manual VPN FRR fails, VPN Auto FRR takes effect.

Prerequisites

Manual VPN FRR function takes effect after the backup next hop is manually specified. It is recommended that you run the **route-policy** command to specify the backup next hop for VPN routes before configuring Manual VPN FRR function.

Follow-up Procedure

After configuring Manual VPN FRR function, run the **display ip routing-table vpn-instance** *vpn-instance-name ip-address* **verbose** command to check whether the route has a secondary tunnel and a backup label.

Precautions

NOTE

The **undo vpn frr** command cancels the VPN FRR function of only the specified VPN instance. In the system view, run the **undo vpn frr all** command to simultaneously cancel the VPN FRR function of IPv4 and IPv6 address families in all VPN instances.

Example

# Specify the IP address of the backup next hop in the route-policy named **vpn_frr_rp**, and enable VPN FRR in the VPN instance view.

```
<HUAWEI> system-view
[HUAWEI] route-policy vpn_frr_rp permit node 10
[HUAWEI-route-policy] apply backup-nexthop 10.2.2.9
[HUAWEI-route-policy] quit
[HUAWEI] ip vpn-instance vpn1
[HUAWEI-vpn-instance-vpn1] ipv4-family
[HUAWEI-vpn-instance-vpn1-af-ipv4] route-distinguisher 100:1
[HUAWEI-vpn-instance-vpn1-af-ipv4] vpn frr route-policy vpn_frr_rp
[HUAWEI-vpn-instance-vpn1-af-ipv4] quit
```

10.5 VLL Configuration Commands

10.5.1 Command Support

Only the following switch models support VLL:

S5731-S, S5731-H, S5731S-H, S5732-H, S6720-EI, S6720S-EI, S6730-S, S6730S-H, and S6730-H

Command support and parameter support on your switches may differ from those described in this section. For details, see the specific commands.

10.5.2 bfd bind pw

Function

The **bfd bind pw** command configures a BFD session to detect a PW.

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

By default, no BFD session is configured to detect a PW.

Format

bfd *cfg-name* **bind pw interface** *interface-type interface-number* [**secondary**]

undo bfd *cfg-name*

Parameters

Parameter	Description	Value
cfg-name	Specifies the name of the BFD session.	The value is a string of 1 to 15 case-insensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
interface *interface-type interface-number*	Specifies the type and number of the interface where the PW to be detected resides, namely, the AC interface. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number.	-
secondary	Indicates that the BFD session detects the secondary PW.	-

Views

System 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 detection mechanism on an interface. On networks demanding fast fault detection, run the **bfd bind pw** command to configure a BFD session to detect a PW.

Prerequisites

- A PW has been configured on an AC interface by running the **mpls l2vc** command.
- BFD has been enabled globally by running the **bfd** command.
- A single-segment or multi-segment PW has been configured.

Precautions

- When detecting a PW, BFD sessions must be bound to the source and destination ends of a PW.
- You need to create a BFD session to detect primary and secondary PWs separately.

NOTE

When running the **bfd bind pw** command to detect a multi-segment PW, ensure that the first-segment PW is a VLL PW configured on a non-SPE node.

When running the **bfd bind pw** command to detect a single-segment PW, ensure that the single-segment PW is configured on a non-SPE node.

Example

# Create a BFD session to detect a PW.

```
<HUAWEI> system-view
[HUAWEI] bfd pe2 bind pw interface vlanif 10
```

10.5.3 ccc interface in-label out-label

Function

The **ccc interface in-label out-label** command creates a remote CCC connection between CEs connected to different PEs. This command must be configured on two PEs.

The **undo ccc** command deletes the CCC connection.

By default, no remote CCC connection is created.

Format

ccc *ccc-connection-name* **interface** *interface-type1 interface-number1* [**raw** | **tagged**] **in-label** *in-label-value* **out-label** *out-label-value* **nexthop** *nexthop-address* [**control-word** | **no-control-word**]

undo ccc *ccc-connection-name*

Parameters

Parameter	Description	Value
ccc-connection-name	Specifies the CCC connection name, which uniquely identifies a CCC connection on a PE.	The value is a string of 1 to 20 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
interface *interface-type1 interface-number1*	Specifies the type and number of the incoming interface of data traffic. In the preceding information: ● *interface-type1* specifies the interface type. ● *interface-number1* specifies the interface number.	-
raw	Sets the inbound interface to raw mode. When packets arrive at the inbound interface in raw mode, the system deletes the Provider tags (P-Tags) of packets.	By default, the tagged mode is used.
tagged	Sets the inbound interface to tagged mode. When packets arrive at the inbound interface in tagged mode, the system retains the Provider tags (P-Tags) of packets.	By default, the tagged mode is used.
in-label *in-label-value*	Specifies the inbound label.	The value is a decimal integer that ranges from 16 to 1023.
out-label *out-label-value*	Specifies the outbound label.	The value is a decimal integer that ranges from 0 to 1048575.
nexthop *nexthop-address*	Specifies the IP address of the next hop.	The value is in dotted decimal notation.
control-word | **no-control-word**	Enables or disable the control word (CW).	By default, the control word is disabled.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When two CEs connected to different PEs, use the **ccc interface in-label out-label** command to create a remote CCC connection between the CEs. This command must be executed on both PEs.

Precautions

An interface cannot serve as an L2VPN AC (Attachment Circuit) interface and L3VPN AC interface at the same time. After an interface is bound to an L2VPN, the Layer 3 features such as the IP address and routing protocol configured on this interface become invalid.

NOTE

The device supports only VLANIF interfaces as AC interfaces of CCC connections.

A PE uses connection names to identify different CCC connections. On different PEs, the same CCC connection can use different names. When a P is connected to a PE, the static LSP must be configured between the P and PE. Do not configure the name of a CCC connection as **type**. Otherwise, you cannot view information about the CCC connection using the **display vll ccc** *ccc-name* command. Note that the outgoing label of the previous device is the inner label of the next device.

By default, link type negotiation is enabled globally on the device. If a VLANIF interface is used as an AC-side interface for L2VPN, the configuration conflicts with link type negotiation. In this case, run the **lnp disable** command in the system view to disable link type negotiation.

Example

# Create a remote CCC connection between CEs connected to different PE devices.

```
<HUAWEI> system-view
[HUAWEI] ccc ccc-connection interface vlanif 10 in-label 100 out-label 200 nexthop 10.1.1.2
```

10.5.4 ccc interface out-interface

Function

The **ccc interface out-interface** command creates a local CCC connection between two CEs connected to the same PE.

The **undo ccc** command deletes the CCC connection.

By default, no local CCC connection is created.

Format

ccc *ccc-connection-name* **interface** *interface-type1 interface-number1* [**raw** | **tagged**] **out-interface** *interface-type2 interface-number2* [**raw** | **tagged**]

undo ccc *ccc-connection-name*

Parameters

Parameter	Description	Value
ccc-connection-name	Specifies a CCC connection name, which uniquely identifies a CCC connection on a PE.	The value is a string of 1 to 20 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
interface *interface-type1 interface-number1*	Specifies the type and number of the interface connected to the first CE. ● *interface-type1* specifies the interface type. ● *interface-number1* specifies the interface number.	-
out-interface *interface-type2 interface-number2*	Specifies the type and number of the interface connected to the second CE. ● *interface-type2* specifies the interface type. ● *interface-number2* specifies the interface number.	-
raw	Sets the inbound interface to raw mode. When packets arrive at the inbound interface in raw mode, the system deletes the provider tags (P-tags) of packets.	By default, the tagged mode is used.
tagged	Sets the inbound interface to tagged mode. When packets arrive at the inbound interface in tagged mode, the system retains the provider tags (P-tags) of packets.	By default, the tagged mode is used.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When two CEs connect to the same PE, use the **ccc interface out-interface** command to create a local CCC connection between the CEs.

Precautions

An interface cannot serve as an L2VPN AC interface and L3VPN AC interface at the same time. After an interface is bound to an L2VPN, the Layer 3 features such as the IP address and routing protocol configured on this interface become invalid. After the interface is bound to a CCC connection, its sub-interfaces no longer transmit Layer 3 traffic.

NOTE

- The device supports only VLANIF interfaces as AC interfaces of CCC connections.

A CCC connection is bidirectional; therefore, only one connection is needed. Do not configure the name of a CCC connection as **type**; otherwise, you cannot view information about the CCC connection by running the **display vll ccc** command.

By default, link type negotiation is enabled globally on the device. If a VLANIF interface is used as an AC-side interface for L2VPN, the configuration conflicts with link type negotiation. In this case, run the **lnp disable** command in the system view to disable link type negotiation.

Example

# Create a local CCC connection between two CEs connected to the same PE device.

```
<HUAWEI> system-view
[HUAWEI] mpls lsr-id 1.1.1.1
[HUAWEI] mpls
[HUAWEI-mpls] quit
[HUAWEI] mpls l2vpn
[HUAWEI-l2vpn] quit
[HUAWEI] ccc ccc-connect-1 interface vlanif 10 out-interface vlanif 11
```

10.5.5 ce

Function

The **ce** command creates a CE and displays the MPLS-L2VPN-CE view.

The **undo ce** command deletes a CE.

By default, no CE is created in a L2VPN instances.

Format

ce *ce-name* [**id** *ce-id* [**range** *ce-range*] [**default-offset** *ce-offset*]]

undo ce *ce-name*

Parameters

Parameter	Description	Value
ce-name	Specifies the name of a CE.	The value is a string of 1 to 20 case-sensitive characters, spaces not supported.
id *ce-id*	Specifies the ID of the CE.	The value is a decimal integer that ranges from 0 to 249. A CE ID uniquely identifies a CE in a L2VPN instances. For convenience, you are advised to set the CE IDs in the sequence of natural number that starts from 1.
range *ce-range*	Specifies the number of CEs in an L2VPN instance.	The value is a decimal integer that ranges from 1 to 250 and the default is 10.
default-offset *ce-offset*	Indicates the default CE offset. The CE offset refers to the ID of the other local CE or the remote CE that establishes the connection with the local CE.	It can be either 0 or 1. The default is 0.

Views

MPLS-L2VPN instance view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In a Kompella VLL networking, you can use the **ce** command to create a CE in a L2VPN instance and enter the MPLS-L2VPN-CE view.

Prerequisites

An RD has been configured for the L2VPN instance.

Precautions

ce-range can be increased but cannot be decreased. If multiple label blocks exist, the *ce-range* equals the total size of all label blocks. A device allocates labels to the ranges of Kompella L2VPN instances and VPLS VSIs from the same label block. Therefore, the ranges of Kompella L2VPN instances and VPLS VSIs cannot be larger than the size of the label block. Otherwise, the system displays a message indicating that the number of required labels exceeds the permitted maximum labels. As a result, the system fails to create a CE or fails to allocate a site ID to a VSI.

The constraints between **default-offset** and *ce-range* in this command and *ce-offset* in **connection** are as follows:

- If **default-offset** in this command is 0, *ce-offset* in the **connection** command must be less than *ce-range* in this command.
- If **default-offset** in this command is 1, *ce-offset* in the **connection** command must be not more than *ce-range* in this command and cannot be 0.

Example

# Create a CE named ce1 inside the vpn1.

```
<HUAWEI> system-view
[HUAWEI] mpls l2vpn vpn1 encapsulation ethernet
[HUAWEI-mpls-l2vpn-vpn1] route-distinguisher 100:1
[HUAWEI-mpls-l2vpn-vpn1] ce ce1 id 1 range 10
[HUAWEI-mpls-l2vpn-ce-vpn1-ce1]
```

10.5.6 connection

Function

The **connection** command creates a connection in Kompella mode between CEs.

The **undo connection ce-offset** command deletes a connection in Kompella mode between CEs.

By default, no connection in Kompella mode is created between CEs.

Format

connection [**ce-offset** *id*] **interface** *interface-type interface-number* [**tunnel-policy** *policy-name*] [**raw** | **tagged**] [**secondary**]

undo connection ce-offset *id*

Parameters

Parameter	Description	Value
ce-offset *id*	Specifies the ID of the peer CE connected to the L2VPN.	The value is a decimal integer that ranges from 0 to 249. *id* must be not more than *ce-range*. For the configuration about *ce-range*, see **ce**. For a remote connection, **ce-offset** and the ID of the remote CE must be the same; for a local connection between two CEs, **ce-offset** of a CE is the ID of the other CE.
interface *interface-type interface-number*	Specifies the type and number of the interface connected to the CE. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number.	-
tunnel-policy *policy-name*	Specifies the name of a tunnel policy applied to a VLL connection.	The value is a string of 1 to 39 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
raw	Sets the encapsulation mode to raw mode. In raw mode, the device deletes the Provider tag (P-Tag) in the packets. The P-Tag is inserted by an SP device to distinguish traffic from different users.	-
tagged	Sets the encapsulation mode to tagged mode. In tagged mode, the device retains the P-Tag in the packets.	-

Parameter	Description	Value
secondary	Specifies the secondary connection of the CE. If this parameter is not specified, the new connection becomes the primary connection. Specify this parameter only when a primary connection exists locally.	-

Views

MPLS-L2VPN-CE view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In a Kompella VLL networking, you can use the **connection** command to create a connection.

Precautions

An interface cannot serve as an L2VPN AC interface and L3VPN AC interface at the same time. After an interface is bound to an L2VPN, the Layer 3 features such as the IP address and routing protocol configured on this interface become invalid.

NOTE

- When the sub-interface is bound to a VLL, the encapsulation protocol type of the main interface cannot be changed.
- If a sub-interface is bound to a VLL, the sub-interface can be deleted only after the sub-interface is unbound from the VLL.
- VLANIF interfaces, XGE interfaces, MultiGE interface, 25GE interface, 40GE interfaces, 100GE interfaces, GE interfaces, Eth-Trunk interfaces, XGE sub-interfaces, 25GE sub-interface, MultiGE sub-interfaces, 40GE sub-interfaces, 100GE sub-interfaces, GE sub-interfaces, or Eth-Trunk sub-interfaces can be used as AC interfaces connected to CEs.

  To use an XGE interface, a GE interface, a 25GE interface, a MultiGE interface, a 40GE interface, a 100GE interface, or an Eth-Trunk interface of the device as the AC interface of the PE, run the **undo portswitch** command to change a Layer 2 interface to a Layer 3 interface.
- The management interface cannot be configured as the AC interface connected to a CE.

When creating a connection in Kompella mode, you need to specify the peer CE ID and the local CE interface.

If you do not specify **ce-offset** *id*:

- For the first connection of the CE, by default, **ce-offset** *id* is the same as the **default-offset**. For the description about **default-offset**, see **ce**. If **ce-offset** equals the current CE ID, **ce-offset** increases by 1.

- For other connections, **ce-offset** *id* is the last CE ID plus 1. If the CE offset ID of the last connection plus 1 equals the current CE ID, the **ce-offset** *id* is the value obtained by CE offset of the last connection plus 2.

It is recommended that you number CE IDs from 1 in ascending order, and to configure connections in the order of CE IDs. To simplify configuration, you can use the default **ce-offset** directly in most connections.

After the command is configured, the default policy is adopted in the following situations:

- If you do not specify a policy name
- If the specified policy is not configured

In the default policy:

- Only LSP tunnels are selected.
- No load balancing is performed.

By default, link type negotiation is enabled globally on the device. If a VLANIF interface is used as an AC-side interface for L2VPN, the configuration conflicts with link type negotiation. In this case, run the **lnp disable** command in the system view to disable link type negotiation.

Example

# Create a connection in Kompella mode.

```
<HUAWEI1> system-view
[HUAWEI1] mpls l2vpn vpn1 encapsulation vlan
[HUAWEI1-mpls-l2vpn-vpn1] route-distinguisher 100:1
[HUAWEI1-mpls-l2vpn-vpn1] vpn-target 1:1
[HUAWEI1-mpls-l2vpn-vpn1] ce ce1 id 1 range 10
[HUAWEI1-mpls-l2vpn-ce-vpn1-ce1] connection ce-offset 2 interface vlanif 10
<HUAWEI2> system-view
[HUAWEI2] mpls l2vpn vpn1 encapsulation vlan
[HUAWEI2-mpls-l2vpn-vpn1] route-distinguisher 100:1
[HUAWEI2-mpls-l2vpn-vpn1] vpn-target 1:1
[HUAWEI2-mpls-l2vpn-vpn1] ce ce2 id 2 range 10
[HUAWEI2-mpls-l2vpn-ce-vpn1-ce2] connection ce-offset 1 interface vlanif 20
```

10.5.7 display bgp l2vpn

Function

The **display bgp l2vpn** command displays information about the Kompella L2VPN label block stored in BGP.

Format

display bgp l2vpn { **all** | **group** [*group-name*] | **peer** [[*peer-ip-address*] **verbose**] | **route-distinguisher** *route-distinguisher* [**ce-id** *ce-id* [**label-offset** *label-offset*]] }

Parameters

Parameter	Description	Value
all	Displays all information about the local label block of Kompella L2VPN stored in BGP.	-
group *group-name*	Displays information about the label block of Kompella L2VPN stored in a specified BGP peer group.	The value is an existing BGP peer group.
peer-ip-address	Displays information about the Kompella L2VPN label block of the specified peer stored in BGP.	The value is in dotted decimal notation.
verbose	Displays detailed information about the Kompella L2VPN label block stored in BGP.	-
route-distinguisher *route-distinguisher*	Specifies the specific route identification value. The RD format can be any of the following: ● 2-byte AS number:4-byte user-defined number, for example, 101:3. An AS number ranges from 0 to 65535. A user-defined number ranges from 0 to 4294967295. The AS number and the user-defined number cannot be 0s at the same time. That is, an RD cannot be 0:0. ● Integral 4-byte AS number:2-byte user-defined number, for example, 65537:3. An AS number ranges from 65536 to 4294967295. A user-defined number ranges from 0 to 65535. The AS number and user-defined number cannot be both 0s. That is, an RD cannot be 0:0. ● 4-byte AS number in dotted notation:2-byte user-defined number, for example, 0.0:3 or 0.1:0. A 4-byte AS number in dotted notation is in the format of *x.y*, where *x* and *y* are integers that range from 0 to 65535 and from 0 to 65535, respectively. A user-defined number ranges from 0 to 65535. The AS number and user-defined number cannot be both 0s. That is, an RD cannot be 0.0:0. ● IPv4-address:2-byte user-defined number, for example, 192.168.122.15:1. An IP address ranges from 0.0.0.0 to 255.255.255.255. A user-defined number ranges from 0 to 65535.	-
ce-id *ce-id*	Specifies the number of CE of the L2VPN instance.	The value ranges from 0 to 65535.

Parameter	Description	Value
label-offset *label-offset*	Specifies the offset value of the label.	It is a decimal integer ranging from 0 to 65535.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

In a Kompella VLL networking, you can use the **display bgp l2vpn** command to check information about a label block, including the RD value, CE ID, label offset, start label in the label block, and BGP routing attributes of the label block.

Precautions

If **route-distinguisher**, **ce-id**, and **label-offset** all are specified, you can view the BGP extended community attribute, the value of each label in the label block, the status of the L2VPN connection status using this label as well as the BGP peers to which this label block is advertised.

Example

# View the BGP L2VPN label block with the specified RD, CE ID, and label offset.

```
<HUAWEI> display bgp l2vpn route-distinguisher 1:1 ce-id 1 label-offset 0
 BGP Local router ID : 10.1.1.2, local AS number : 100
 Origin codes:i - IGP, e - EGP, ? - incomplete
 nexthop:6.6.6.6,  pref :100,     as-path :(null)
 label base: 35840, label range: 10, layer-2 mtu: 1500, encap type:Ethernet VLAN
 label          state
  35840           down
  35841           down
  35842           up
  35843           down
  35844           down
  35845           down
  35846           down
  35847           down
  35848           down
  35849           down
```

Table 10-47 Description of the **display bgp l2vpn** command output

Item	Description
BGP Local router ID	Local router ID of local BGP. Its format is the same as the IPv4 address.

Item	Description
Origin codes	The origin attributes of BGP route: ● i - IGP: Interior Gateway Protocol (IGP), It is of the highest priority. ● e - EGP: Exterior Gateway Protocol (EGP): It is of the second highest priority. ● ? - incomplete: It is of the lowest priority.
local AS number	Local autonomous system (AS) number.
nexthop	Next-hop address of MP-BGP.
pref	Local preference, which is one type of BGP routing attribute.
as-path	AS path attribute, which is one type of BGP routing attribute. It records the numbers of all ASs sequentially that a packet passes through from the local address to the destination address.
label base	Starting value of the label.
label range	Range of the labels.
layer-2 mtu	MTU value of the link layer.
encap type	Encapsulation mode of the link layer.
label	Allocated label.
state	Status of the allocated label.

10.5.8 display l2vpn ccc-interface vc-type

Function

The **display l2vpn ccc-interface vc-type** command displays information about the interface used by an L2VPN connection.

Format

display l2vpn ccc-interface vc-type { **all** | *vc-type* } [**down** | **up**]

Parameters

Parameter	Description	Value
all	Displays information about all interfaces of L2VPN connections.	-
vc-type	Specifies the type of the L2VPN connection.	The following types of the L2VPN connection are available: ● ccc: Cross Circuit Connection ● ldp-vc: L2VPN connection in the Martini mode ● static-vc: L2VPN connection in the SVC mode ● bgp-vc: L2VPN connection in the Kompella mode ● vpls-vc: VPLS connection
down	Displays information about interfaces of L2VPN connection in the Down state.	-
up	Displays information about interfaces of L2VPN connection in the Up state.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

When locating L2VPN faults, you can use the **display l2vpn ccc-interface vc-type** command to view information about the AC interface of the current L2VPN connection, the total number of AC interfaces of various L2VPN connections, interface status, interface encapsulation type, and L2VPN connection types.

Example

# Display information about all the interfaces of L2VPN.

```
<HUAWEI> display l2vpn ccc-interface vc-type all
Total ccc-interface of LDP VC: 1
up (1), down (0)
Interface               Encap Type            State     VC Type
Vlanif12                vlan               up       ldp-vc
```

Table 10-48 Description of the **display l2vpn ccc-interface vc-type** command output

Item	Description
Total ccc-interface of CCC : 2 up (2), down (0)	Total number of L2VPN connections is 2. Two connections is Up. No connection is Down.
Interface	Interface connected to the L2VPN connection on the switch.
Encap Type	Encapsulation type of the L2VPN connection. The encapsulation type can be VLAN encapsulation or Ethernet encapsulation.
State	Current status of the L2VPN connection. The status can be Up or Down.
VC Type	Type of the L2VPN connection: ● ccc: Cross Circuit Connection ● ldp-vc: L2VPN connection in the Martini mode ● static-vc: L2VPN connection in the SVC mode ● bgp-vc: L2VPN connection in the Kompella mode ● vpls-vc: VPLS connection

10.5.9 display mpls l2vc

Function

The **display mpls l2vc** command displays information about virtual circuits (VCs) in LDP mode.

Format

display mpls l2vc [*vc-id* | **interface** *interface-type interface-number* | **remote-info** [*vc-id* | **verbose**] | **state** { **down** | **up** }]

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Specifies the type and number of the AC interface connected to the CE. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number.	-

Parameter	Description	Value
remote-info	Displays information about the VC on the remote end.	-
vc-id	Displays static PW information with a specified VC ID.	The value is an integer that ranges from 1 to 4294967295.
verbose	Displays the detailed information about the VC on the remote end.	-
state { **down** | **up** }	Displays VC information based on the VC status. ● **down**: Displays information about the VC in Down state. ● **up**: Displays information about the VC in Up state.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The **display mpls l2vc** command displays information about the VCs in LDP signaling mode, including the Martini VC and PWE3 VC.

- If the interface is specified, information about VCs on the specified AC interface is displayed.
- If **remote-info** is specified but *vc-id* is not specified, information about all VCs set up by the remote and local peers is displayed.

Example

# Display information about all the LDP VCs configured on the switch.

```
<HUAWEI> display mpls l2vc
 Total LDP VC : 1     1 up       0 down

 *client interface       : Vlanif1111 is up
  Administrator PW       : no
  session state          : up
  AC status              : up
  Ignore AC state        : disable
  VC state               : up
  Label state            : 0
  Token state            : 0
  VC ID                  : 101
  VC type                : VLAN
  destination            : 10.3.3.9
  local VC label         : 1026         remote VC label      : 1026
```

```
control word            : disable
remote control word     : disable
forwarding entry        : exist
local group ID          : 0
remote group ID         : 0
local AC OAM State      : up
local PSN OAM State     : up
local forwarding state : forwarding
local status code       : 0x0
remote AC OAM state     : up
remote PSN OAM state    : up
remote forwarding state: forwarding
remote status code      : 0x0
ignore standby state    : no
BFD for PW              : unavailable
VCCV State              : up
manual fault            : not set
active state            : active
link state              : up
local VC MTU            : 1500          remote VC MTU          : 1500
local VCCV              : alert ttl lsp-ping bfd
remote VCCV             : alert ttl lsp-ping bfd
tunnel policy name      : --
PW template name        : --
primary or secondary    : primary
load balance type       : flow
Access-port             : false
Switchover Flag         : false
VC tunnel/token info    : 1 tunnels/tokens
  NO.0  TNL type        : lsp   , TNL ID : 0x48000020
  Backup TNL type       : lsp   , TNL ID : 0x0
create time             : 0 days, 0 hours, 6 minutes, 50 seconds
up time                 : 0 days, 0 hours, 6 minutes, 34 seconds
last change time        : 0 days, 0 hours, 6 minutes, 34 seconds
VC last up time         : 2013/09/24 18:23:35
VC total up time        : 0 days, 0 hours, 6 minutes, 34 seconds
CKey                    : 16
NKey                    : 15
PW redundancy mode      : frr
AdminPw interface       : --
AdminPw link state      : --
Diffserv Mode           : uniform
Service Class           : be
Color                   : --
DomainId                : --
Domain Name             : --
```

Table 10-49 Description of the **display mpls l2vc** command output

Item	Description
Total LDP VC	Total number of established LDP VCs, including the number of LDP VCs in Up and Down state.
client interface	AC interface and its status.
Administrator PW	Whether the PW is an mPW. The PW can be an mPW only when the AC interface is a loopback interface. This field can be displayed as **yes** or **no**.
session state	Status of the LDP session established between both ends of the VC: ● up: The LDP session has been established. ● down: The LDP session is not established.

Item	Description
AC status	Status of the AC: ● up: An AC has been established. ● down: An AC is not established.
Ignore AC state	Whether the AC status change affects the status of services on the active or standby PWE3. ● enable: The impact of the AC status change on the status of services on the active or standby PWE3 is ignored. ● disable: The AC status change affects the status of services on the active or standby PWE3.
VC state	Status of the VC: ● up: A VC has been established. ● down: A VC is not established.
Label state	Label status: ● 0: The label can be used. ● 1: Wait for the SMB to confirm the label status. ● 2: The label is released. ● 3: SMB confirmation failed.
Token state	Token status: ● 0: The token can be used. ● 1: Wait for the SMB to confirm the token status. ● 2: The token is released. ● 3: SMB confirmation failed.
VC ID	ID of the VC, which uniquely identifies a VC. **NOTE** If the VC IDs on both ends are different, run the **mpls l2vc** command in the interface view to change the VC ID on one end to be the same as that on the other end.
VC type	Encapsulation type of the VC: ● VLAN ● Ethernet The PW can go Up only when the local and remote encapsulation types are the same.
destination	LSR ID of the VC peer device.
local VC label	Local VC label.
remote VC label	Remote VC label.

Item	Description
control word	Whether the control word is enabled: ● enable: The control word is enabled. ● disable: The control word is disabled.
forwarding entry	Whether forwarding entries exist.
local group ID	Local group ID.
remote group ID	Remote group ID.
manual fault	Whether a PW fault is simulated.
active state	Whether the PW is in active state. A PW in active state can forward packets.
link state	Integrative PW status: ● up ● down If any of the following status is Down, the PW link state is Down: ● Service PW status ● Status of the mPW associated with service PWs ● Status of the BFD session associated with service PWs ● PW state code ● PW status detected by VCCV ● OAM status
local VC MTU	MTU of the local VC.
remote VC MTU	MTU of the remote VC.
tunnel policy name	Name of the tunnel policy.
PW template name	Name of the PW template.
primary or secondary	Whether the VC is a primary VC or a secondary VC.
load balance type	Load balancing mode of Martini VLL: ● flow: indicates flow-based load balancing. ● packet: indicates packet-based load balancing.
Access-port	Whether the interface supports the access-port attribute: ● true: indicates that the interface supports the access-port attribute. ● false: indicates that the interface does not support the access-port attribute.

Item	Description
Switchover Flag	Whether a switchover has occurred.
create time	How long the VC has been created.
up time	How long the VC keeps the Up state. If the current PW status is Down, the value is 0.
last change time	How long the VC status remains unchanged.
VC last up time	Last time when the VC became Up.
VC total up time	Total duration of the VC in Up state.
CKey	Index of the public tunnel for VPN QoS.
NKey	Index of the public tunnel.
AdminPw interface	AC interface on which the mPW is bound to the PW. The AC interface must be a loopback interface. This field is displayed only when the PW is not an mPW: ● Name of the loopback interface. ● --: indicates that the PW is not bound to an mPW.
AdminPw link state	Status of the mPW bound to the PW. This field is displayed only when the PW is not an mPW. This field can be displayed as: ● Up ● Down ● --: indicates that the PW is not bound to an mPW.
Diffserv Mode	QoS DiffServ mode.
Service Class	QoS service class.
Color	QoS color.
DomainId	ID of a domain.
Domain Name	Name of a domain.

# Display LDP VC information about the AC interface VLANIF 100.

```
<HUAWEI> display mpls l2vc interface vlanif 100
 *client interface       : Vlanif100  is up
  Administrator PW       : no
  session state          : up
  AC status              : up
  Ignore AC state        : disable
  VC state               : up
  Label state            : 0
  Token state            : 0
  VC ID                  : 1
  VC type                : VLAN
  destination            : 10.2.2.2
  local group ID         : 0            remote group ID      : 0
  local VC label         : 16400        remote VC label      : 16400
  local AC OAM State     : up
  local PSN OAM State    : up
  local forwarding state : forwarding
  local status code      : 0x0
  remote AC OAM state    : up
  remote PSN OAM state   : up
  remote forwarding state: forwarding
  remote status code     : 0x20
  ignore standby state   : no
  BFD for PW             : unavailable
  VCCV State             : up
  manual fault           : not set
  active state           : active
  forwarding entry       : exist
  link state             : up
  local VC MTU           : 1500         remote VC MTU        : 1500
  local VCCV             : cw alert ttl lsp-ping bfd
  remote VCCV            : cw alert ttl lsp-ping bfd
  local control word     : enable       remote control word  : enable
  tunnel policy name     : --
  PW template name       : --
  primary or secondary   : primary
  load balance type      : flow
  Access-port            : false
  Switchover Flag        : false
  VC tunnel/token info   : 1 tunnels/tokens
    NO.0  TNL type       : lsp   , TNL ID : 0x800802
    Backup TNL type      : lsp   , TNL ID : 0x0
  create time            : 0 days, 0 hours, 0 minutes, 29 seconds
  up time                : 0 days, 0 hours, 0 minutes, 6 seconds
  last change time       : 0 days, 0 hours, 0 minutes, 6 seconds
  VC last up time        : 2011/07/04 20:25:50
  VC total up time       : 0 days, 0 hours, 0 minutes, 6 seconds
  CKey                   : 2
  NKey                   : 1
  PW redundancy mode     : frr
  AdminPw interface      : --
  AdminPw link state     : --
  Diffserv Mode          : uniform
  Service Class          : --
  Color                  : --
  DomainId               : --
  Domain Name            : --
```

Table 10-50 Description of the **display mpls l2vc interface** command output

Item	Description
local AC OAM State	OAM status of the local AC. ● up ● down
local PSN OAM State	Status of the local device on the Packet Switch Network (PSN) side. ● up ● down

Item	Description
local forwarding state	Status of the local forwarding table. ● forwarding ● down
local status code	Status code of the local PW: ● 0x0: indicates that the local PW functions as the master PW and is in Up state. ● 0x20: indicates that the local PW functions as the backup PW and is in Up state. ● 0x1: indicates that the local PW functions as the master PW and is in Down state. ● 0x21: indicates that the local PW functions as the backup PW and is in Down state.
remote AC OAM state	OAM status of the remote AC. ● up ● down
remote PSN OAM state	Status of the remote device on the PSN side. ● up ● down
remote forwarding state	Status of the remote forwarding table. ● forwarding ● down
remote status code	Status code of the remote PW: ● 0x0: indicates that the remote PW functions as the master PW and is in Up state. ● 0x20: indicates that the remote PW functions as the backup PW and is in Up state. ● 0x1: indicates that the remote PW function as the master PW and is in Down state. ● 0x21: indicates that the remote PW function as the backup PW and is in Down state.
BFD for PW	Whether BFD for PW is enabled: ● available ● unavailable
VCCV State	Whether Virtual Circuit Connectivity Verification (VCCV) is enabled.

Item	Description
local VCCV	Type of VCCV supported on the local device. ● By default, the VCCV type is **alert ttl lsp-ping bfd**, indicating that the control word function is disabled and LSP ping and BFD are supported for the alert channel. ● If the control word function is enabled, the VCCV type is **cw alert ttl lsp-ping bfd**, indicating that LSP ping and BFD are supported for both the control word channel and the alert channel.
remote VCCV	Type of VCCV supported on the remote device. ● By default, the VCCV type is **alert ttl lsp-ping bfd**, indicating that the control word function is disabled and LSP ping and BFD are supported for the alert channel. ● If the control word function is enabled, the VCCV type is **cw alert ttl lsp-ping bfd**, indicating that LSP ping and BFD are supported for both the control word channel and the alert channel.
local control word	Whether the control word is enabled on the local device: ● Disable ● Enable
remote control word	Whether the control word is enabled on the remote device: ● Disable ● Enable
ignore standby state	Whether the status of the secondary PW is ignored.
VC Tunnel/token info: 1 tunnels/tokens	Information about the tunnel or token used by the VC. The value **1 tunnels/tokens** indicates that the PW uses one tunnel or token.
TNL type	Type of the tunnel used by the PW.
TNL ID	ID of the tunnel used by the PW.
Backup TNL Type	Type of the backup tunnel when PW over LDP FRR is used.

Item	Description
PW redundancy mode	PW redundancy mode. By default, the mode is FRR. ● Independent: indicates that the PW is in negotiation mode. ● frr: indicates that the PW is in FRR mode. ● --: indicates that the PW is in master/slave mode.

# Display the LDP VC information received from the remote peer.

```
<HUAWEI> display mpls l2vc remote-info
Total remote ldp vc : 1

Transport  Group      Peer           Remote        Remote     C   MTU/  N   S
VC ID      ID         Addr           Encap         VC Label   Bit CELLS Bit Bit

101        0          10.3.3.9       ethernet      1024       0   1500  0   0
```

# Display the detailed LDP VC information received from the remote peer.

```
<HUAWEI> display mpls l2vc remote-info verbose
Total remote LDP VC : 1

VC ID              : 1
VC Type            : vlan
VC Label           : 1025
Peer Address       : 10.5.5.5
Group ID           : 0
MTU                : 1500
Control Word       : 0
Notification       : 1
Status Code        : 0
Match Local VC     : MATCH
Max ATM CELLS      : --
TDM RTP Header     : --
TDM Encap Num      : --
TDM Bit Rate       : --
```

Table 10-51 Description of the **display mpls l2vc remote-info** command output

Item	Description
Total remote ldp vc	Total number of created remote LDP VCs.
Transport VC ID	VC ID, which uniquely identifies a VC.
Group ID	ID of the group to which the L2VPN belongs. The default value is 0.
Peer Addr and Peer Address	IP address of the remote peer.
Remote Encap	Encapsulation type of the remote VC. ● vlan ● ethernet

Item	Description
Remote VC Label	Remote VC label.
C Bit	Whether the control word is enabled: - 1: indicates that the control word is enabled. - 0: indicates that the control word is disabled.
MTU/CELLS	MTU of the L2VPN.
N Bit and Notification	Whether the Notification message is supported: - 1: indicates the message is supported. - 0: indicates the message is not supported.
S Bit and Status Code	Status code: - 0: indicates the forwarding state. - 1: indicates the non-forwarding state. - 32: indicates the backup state.
Match Local VC	Whether the local VC ID matches the remote VC ID: - MATCH - NOT-MATCH
Max ATM CELLS	Maximum number of ATM cells that can be transmitted. If ATM encapsulation is used, the value ranges from 1 to 28, and the default value is 28. If non-ATM encapsulation is used, double hyphens (--) are displayed.
TDM RTP Header	Whether the RTP-header option is enabled: - enable: The RTP header is added to TDM packets to be transparently transmitted. - disable: The RTP header is not added to TDM packets to be transparently transmitted. This is the default value. - --: Non-TDM encapsulation is used.
TDM Encap Num	Number of frames in a TDM packet. If TDM encapsulation is used, the value is 8, 16, 24, 32 or 40, and the default value is 32. If non-TDM encapsulation is used, double hyphens (--) are displayed.
TDM Bit Rate	Number of timeslots in a TDM packet. Number of timeslots in a TDM packet = Number of bytes in a TDM packet/Number of frames in a TDM packet

Display information about the VCs in Up state.

```
<HUAWEI> display mpls l2vc state up
 Total LDP VC : 1     1 up       0 down

 *client interface       : Vlanif1111 is up
  Administrator PW       : no
  session state          : up
  AC status              : up
  Ignore AC state        : disable
  VC state               : up
  Label state            : 0
  Token state            : 0
  VC ID                  : 100
  VC type                : VLAN
  destination            : 10.2.2.9
  local VC label         : 1024         remote VC label      : 1024
  control word           : disable
  remote control word    : disable
  forwarding entry       : exist
  local group ID         : 0
  remote group ID        : 0
  local AC OAM State     : up
  local PSN OAM State    : up
  local forwarding state : forwarding
  local status code      : 0x0
  remote AC OAM state    : up
  remote PSN OAM state   : up
  remote forwarding state: forwarding
  remote status code     : 0x0
  ignore standby state   : no
  BFD for PW             : unavailable
  VCCV State             : up
  manual fault           : not set
  active state           : active
  link state             : up
  local VC MTU           : 1500         remote VC MTU        : 1500
  local VCCV             : alert ttl lsp-ping bfd
  remote VCCV            : alert ttl lsp-ping bfd
  tunnel policy name     : --
  PW template name       : --
  primary or secondary   : primary
  load balance type      : flow
  Access-port            : false
  Switchover Flag        : false
  VC tunnel/token info   : 1 tunnels/tokens
    NO.0  TNL type       : lsp   , TNL ID : 0x12
    Backup TNL type      : lsp   , TNL ID : 0x0
  create time            : 0 days, 1 hours, 0 minutes, 17 seconds
  up time                : 0 days, 0 hours, 24 minutes, 56 seconds
  last change time       : 0 days, 0 hours, 24 minutes, 56 seconds
  VC last up time        : 2013/10/10 14:29:39
  VC total up time       : 0 days, 0 hours, 24 minutes, 56 seconds
  CKey                   : 10
  NKey                   : 9
  PW redundancy mode     : frr
  AdminPw interface      : --
  AdminPw link state     : --
  Diffserv Mode          : uniform
  Service Class          : --
  Color                  : --
  DomainId               : --
  Domain Name            : --
```

10.5.10 display mpls l2vc brief

Function

The **display mpls l2vc brief** command displays brief information about LDP Layer 2 virtual circuits (L2VCs) on the device.

Format

display mpls l2vc brief

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The **display mpls l2vc brief** command is recommended when many L2VCs are configured on a device. The command output is more concise than that of the **display mpls l2vc** command.

Example

# Display brief information about all LDP L2VCs on the device.

```
<HUAWEI> display mpls l2vc brief
 Total LDP VC : 1     1 up       0 down

 *Client Interface     : Vlanif1111
  Administrator PW     : no
  AC status            : up
  Ignore AC state      : disable
  VC state             : up
  Label state          : 0
  Token state          : 0
  VC ID                : 116119
  VC Type              : VLAN
  session state        : up
  Destination          : 10.6.6.6
  link state           : up
```

Table 10-52 Description of the **display mpls l2vc brief** command output

Item	Description
Total LDP VC	Total number of LDP VCs, including the number of LDP VCs in Up and Down state.

Item	Description
Client Interface	AC interface and its status.
Administrator PW	Whether the PW is an mPW. The PW can be an mPW only when the AC interface is a loopback interface.
AC status	Status of the AC: ● up ● down
Ignore AC state	Whether the AC status change affects the status of services on the active or standby PWE3. ● enable: The impact of the AC status change on the status of services on the active or standby PWE3 is ignored. ● disable: The AC status change affects the status of services on the active or standby PWE3.
VC state	Status of the VC: ● up ● down
Label state	Label status: ● 0: The label can be used. ● 1: Wait for the SMB to confirm the label status. ● 2: The label is released. ● 3: SMB confirming failed.
Token state	Token status: ● 0: The label can be used. ● 1: Wait for the SMB to confirm the label status. ● 2: The label is released. ● 3: SMB confirming failed.
VC ID	ID of the VC, which uniquely identifies a VC.
VC Type	Encapsulation type of the VC.
session state	Status of the session between peers: ● up ● down
Destination	Peer address.
link state	Status of the VC: ● up ● down

10.5.11 display mpls l2vpn

Function

The **display mpls l2vpn** command displays information about an L2VPN on a PE.

Format

display mpls l2vpn [*l2vpn-name* [**local-ce** | **remote-ce**]]

Parameters

Parameter	Description	Value
l2vpn-name	Specifies the VPN to be displayed.	The value is an existing VPN name.
local-ce	Displays information about all the local CEs of a specified L2VPN.	-
remote-ce	Displays information about remote CEs learned from other PEs of a specified L2VPN.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

If you specify parameters, the **display mpls l2vpn** command displays information related to the parameters. If not, information about all the L2VPNs is displayed.

Example

# Display information about all the VPNs configured on the PE.

```
<HUAWEI> display mpls l2vpn
VPN number: 1
vpn-name        encap-type   route-distinguisher     mtu   ce(L)  ce(R)
vpn1            ethernet     100:1                   1500   1      1
```

Table 10-53 Description of the display mpls l2vpn command output

Item	Description
vpn-name	Name of the created VPN instance.
encap-type	Encapsulation type of L2VPN.
route-distinguisher	RD of L2VPN.

Item	Description
mtu	MTU of L2VPN.
ce (L)	The number of local CE connections. "L" indicates "local".
ce (R)	Number of remote CE connections. "R" indicates "remote".

# Display information about the L2VPN named vpn1.

```
<HUAWEI> display mpls l2vpn vpn1
VPN name: vpn1, encap type: vlan, local ce number(s): 1, remote ce number(s): 1
route distinguisher: 100:1, MTU: 128
import vpn target: 1:1
export vpn target: 1:1

remote vpn site(s) :
no.  remote-pe-id    route-distinguisher
1    3.3.3.9         100:1
```

Table 10-54 Description of the display mpls l2vpn vpn1 command output

Item	Description
VPN name	Name of the created VPN instance.
encap type	Encapsulation type of the L2VPN.
local ce number (s)	Number of local CE connections.
remote ce number (s)	Number of remote CE connections.
route distinguisher	RD of the local L2VPN.
MTU	MTU of the interface associated with the L2VPN.
import vpn target	Route attribute of the received VPN route.
export vpn target	Attributes configured for the target VPN route.
remote vpn site (s)	The following display is about the remote site.
no.	Remote peer number.
remote-pe-id	ID of remote PE peer. Usually, it is MPLS LSR-ID or the session address of the BGP peer.
route-distinguisher	RD of the remote L2VPN. For the related command, see **route-distinguisher (MPLS-L2VPN instance view)**.

# Display information about the local CE on L2VPN named vpn1.

```
<HUAWEI> display mpls l2vpn vpn1 local-ce
ce-name             ce-id   range   conn-num  CEBase/LBBase/Offset/Range
ce1               1       10      1          0/21504/0/10
ce2               2       10      1          0/21514/0/10
```

Table 10-55 Description of the display mpls l2vpn vpn1 local-ce command output

Item	Description
ce-name	CE name.
ce-id	CE ID that uniquely identifies a CE.
range	Local CE range. Indicates how many CEs are connected to the local CEs.
conn-num	Number of local connections set for local CEs.
CEBase/LBBase/Offset/Range	Label block assigned by the CE with which the local port sets up a connection. 0/21504/0/10 indicates the offset base address of the label block/the initial value of the label block/initial CE offset/the number of remote labels.

# Display information about the remote CE on the L2VPN named vpn1.

```
<HUAWEI> display mpls l2vpn vpn1 remote-ce
no.  ce-id peer-id         route-distinguisher       LB
1    2     3.3.3.9         100:1                     19456/0/10
```

Table 10-56 Description of the display mpls l2vpn vpn1 remote-ce command output

Item	Description
no.	Sequence number of the connection.
ce-id	ID of the remote CE.
peer-id	IP address of the remote peer.
route-distinguisher	RD of the remote peer.
LB	Remote Label block. 19456/0/10 indicates the initial value of the label block/remote initial CE offset/the number of remote labels.

10.5.12 display mpls l2vpn (route-target-list)

Function

The **display mpls l2vpn** command displays the VPN target list for Kompella VLL.

Format

display mpls l2vpn { **export-route-target-list** | **import-route-target-list** }

Parameters

Parameter	Description	Value
export-route-target-list	Displays the VPN target list for Kompella VLL in the outbound direction.	-
import-route-target-list	Displays the VPN target list for Kompella VLL in the inbound direction.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

When an L2VPN connection in Kompella mode is Up but packet forwarding between CE devices fails, you can run this command to view the VPN target list of a specified VPN instance and check whether the VPN targets of the two PE devices match each other.

- The VPN target in the outbound direction of the local PE device must be the same as the VPN target in the inbound direction of the remote PE device.
- The VPN target in the inbound direction of the local PE device must be the same as the VPN target in the outbound direction of the remote PE device.

Example

# Display the VPN target list for Kompella VLL in the inbound direction.

```
<HUAWEI> display mpls l2vpn import-route-target-list
import vpn target list:
 744:7  745:7  746:7  888:8
```

# Display the VPN target list for Kompella VLL in the outbound direction.

```
<HUAWEI> display mpls l2vpn export-route-target-list
export vpn target list:
 755:7  888:8
```

Table 10-57 Description of the **display mpls l2vpn** command output

Item	Description
import vpn target list	VPN target list in the inbound direction.
export vpn target list	VPN target list in the outbound direction.

10.5.13 display mpls l2vpn connection

Function

The **display mpls l2vpn connection** command displays information about L2VPN connections of the Kompella mode.

Format

display mpls l2vpn connection *vpn-name* [**remote-ce** *ce-id* | **down** | **up** | **verbose**]

display mpls l2vpn connection [**summary** | **interface** *interface-type interface-number*]

Parameters

Parameter	Description	Value
vpn-name	Displays information about the specified L2VPN.	The value is an existing VPN name. If you do not specify a VPN name, information about all the L2VPNs is displayed.
remote-ce *ce-id*	Displays information about the remote connections of the specified CE.	The value is a decimal integer ranging from 0 to 249.
down	Displays the information of the connections that are Down. If you do not specify this parameter, the detailed information about connections in both Up and Down state is displayed.	-
up	Displays the information of the connections that are Up. If you do not specify this parameter, the detailed information about connections in both Up and Down state is displayed.	-

Parameter	Description	Value
verbose	Shows detailed information of connections. It is valid only when information about all the connections is displayed.	-
summary	Displays the summary information of connections.	-
interface *interface-type interface-number*	Displays information about the connections on the interface of the specified type and number. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After configuring an L2VPN connection of the Kompella mode, you can use the **display mpls l2vpn connection** *vpn-name* command to check the status of the connection.

The **display mpls l2vpn connection** command displays information about all the L2VPN connections of the Kompella mode on the local device.

Example

# Display information about all the L2VPN Kompella connections.

```
<HUAWEI> display mpls l2vpn connection
1 total connections,
connections: 1 up, 0 down, 0 local, 1 remote, 0 unknown

VPN name: komcon1,
1 total connections,
connections: 1 up, 0 down, 0 local, 1 remote, 0 unknown

  CE name: 116-119, id: 2,
  Rid type status peer-id          route-distinguisher interface
  primary or not
--------------------------------------------------------------------------------
  1    rmt  up     6.6.6.6         1:1                 Vlanif222
  primary
```

Table 10-58 Description of the display mpls l2vpn connection command output

Item	Description
1 total connections,connections: 1 up, 0 down, 0 local, 1 remote, 0 unknown	The first two lines indicate information about all the Kompella connections on the local device, including: ● Total number of connections ● Number of connections in the Up state ● Number of connections in the Down state ● Number of local connections ● Number of remote connections ● Number of unknown connections
VPN name	Name of the created VPN instance.
1 total connections,connections: 1 up, 0 down, 0 local, 1 remote, 0 unknown	Information about the VPN connections, including: ● Total number of connections ● Number of connections in the Up state ● Number of connections in the Down state ● Number of local connections ● Number of remote connections ● Number of unknown connections
CE name:	Name of the CE.
id:	CE ID of the CE connection, which uniquely identifies a CE in a VPN.
Rid	ID of the remote CE that establishes the connection with the local CE.
type	Type of the CE connection: ● rmt: indicates a remote connection. ● loc: indicates a local connection. ● ---: indicates the destination CE does not exist or the signaling connection setup fails when you set up a remote connection.
status	Status of the CE connection: ● Up: indicates the connection is set up successfully. ● Down: indicates the connection setup fails because the configuration is incorrect or the associated interface is Down.

Item	Description
peer-id	IP address of the peer that sets up the session with the local end.
route-distinguisher	RD of the VPN to which the CE belongs.
interface	Interface (an AC interface) connected to the CE.
primary or not	Whether the VC is a primary VC or a secondary VC.

# Display the Kompella L2VPN remote connection on GE0/0/1

```
<HUAWEI> display mpls l2vpn connection interface gigabitethernet 0/0/1
conn-type: remote
    local vc state:              up
    remote vc state:             up
    local ce-id:                 1
    local ce name:               ce1
    remote ce-id:                2
    intf (state,encap):          GigabitEthernet0/0/1(up,ethernet)
    peer id:                     2.2.2.2
    route-distinguisher:         100:2
    local vc label:              31745
    remote vc label:             35842
    tunnel policy:               default
    CKey:                        2
    NKey:                        1
    primary or secondary:        primary
    forward entry exist or not: true
    forward entry active or not:true
    manual fault set or not:     not set
    AC OAM state:                up
    BFD for PW session index:    --
    BFD for PW state:            invalid
    BFD for LSP state:           true
    Local C bit is not set
    Remote C bit is not set
    tunnel type:                 lsp
    tunnel id:                   0x1000c
    Slave tunnel type:           lsp
    Slave tunnel id:             0x0
```

Table 10-59 Description of the remote connection in the display mpls l2vpn connection interface command output

Item	Description
conn-type	Type of the L2VPN connection: ● local: indicates the local L2VPN connection. ● remote: indicates the remote L2VPN connection. ● unknown: indicates the unknown L2VPN connection. The reason that the unknown connection appears may be that the destination CE does not exist, or the signaling connection fails to be set up during the configuration of a remote connection.
local vc state	Status of the local VC: ● Up: indicates that the connection is successfully set up. ● Down: indicates the setup of the connection fails because the configuration is incorrect or the status of related interfaces is Down.
remote vc state	Status of the destination VC: ● Up: indicates that the connection is successfully set up. ● Down: indicates the setup of the connection fails because the configuration is incorrect or the status of related interfaces is Down.
local ce-id	ID of the local CE.
local ce name	Name of the local CE.
remote ce-id	ID of the destination CE that sets up the connection with the local CE.
intf (state,encap)	Status and encapsulation type of the local interface.
peer id	IP address of the peer setting up a session with the CE.
route-distinguisher	RD of the VPN to which the CE interface belongs.
local vc label	Label generated by the local system.
remote vc label	Remote label that is assigned to the local end by the remote LDP.

Item	Description
tunnel policy	Tunnel policy applied to the CE connection.
CKey	Index of the public tunnel (for VPN QoS).
NKey	Index of the public tunnel.
primary or secondary	Whether the VC is a primary VC or a secondary VC.
forward entry exist or not	Whether forwarding entries exist.
forward entry active or not	Whether forwarding entries are in the active state. (If so, user packets can be forwarded.)
manual fault set or not	Whether the PW fault is configured manually.
AC OAM state	OAM status of the local AC.
BFD for PW session index	Index of the BFD for PW.
BFD for PW state	Status of BFD for PW.
BFD for LSP state	Status of BFD for LSP.
Local C bit is not set	L2VPN disabled with the control word. If the control word is enabled, the information is not displayed.
Remote C bit is not set	The remote site disabled with the control word. If the control word is enabled, the information is not displayed.
tunnel type	Tunnel type. The tunnel transmits data of the CE in the public network.
tunnel id	ID of the tunnel. The tunnel transmits data of the CE in the public network.
Slave tunnel type	Type of the backup tunnel when PW over LDP FRR is applied.
Slave tunnel id	ID of the backup tunnel when PW over LDP FRR is applied.

# Display the summary of the Kompella L2VPN connections.

```
<HUAWEI> display mpls l2vpn connection summary
1 total connections,
connections: 1 up,  0 down , 0 local, 1 remote, 0 unknown
No.   vpn-name    local-num remote-num unknown-num up-num total-num
1     vpn1              0         1          0         1      1
```

Table 10-60 Description of the display mpls l2vpn connection summary command output

Item	Description
total connections	Number of all L2VPN connections on the device.
connections:	Number of L2VPN connections of the following status: ● Up ● Down ● remote ● local ● unknown
No.	Sequence number of the connection.
vpn-name	VPN instance name. Various types of connections are displayed in the order of L2VPN instances.
local-num	Number of local connections of the L2VPN instance.
remote-num	Number of all remote connections of the L2VPN instance.
unknown-num	Number of all unknown connections of the L2VPN instance.
up-num	Total number of successful connections of the L2VPN instance.
total-num	Total number of connections of the L2VPN instance.

10.5.14 display mpls l2vpn forwarding-info

Function

The **display mpls l2vpn forwarding-info** command displays MPLS L2VPN forwarding information.

Format

display mpls l2vpn forwarding-info [*vc-label*] **interface** *interface-type interface-number*

Parameters

Parameter	Description	Value
vc-label	Specifies L2VPN VC label.	The value is a decimal integer that ranges from 16 to 1048575.
interface *interface-type interface-number*	Specifies the type and number of the interface. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The **display mpls l2vpn forwarding-info** command displays:

- Private network data carrying the specified label is forwarded from which tunnel.
- Whether the data supports the connectivity verification.
- Whether the data carries the control word.

Example

# Display MPLS L2VPN forwarding information.

```
<HUAWEI> display mpls l2vpn forwarding-info interface vlanif 10
 The Main PW Forward Information :
VCLABEL TNLTYPE        ENTRYTYPE PWSTATE  BFDSTATE ADMIN CTLWORD CC CV TNLID
------------------------------------------------------------------------------
35841   LSP            SEND      ACTIVE   UP       UP    FALSE   2  a  0x1
   1   Record(s) Found.

 The Second PW Forward Information :
VCLABEL TNLTYPE        ENTRYTYPE PWSTATE  BFDSTATE ADMIN CTLWORD CC CV TNLID
------------------------------------------------------------------------------
   0   Record(s) Found.
```

Table 10-61 Description of the display mpls l2vpn forwarding-info interface command output

Item	Description
The Main PW Forward Information :	Forwarding information about the primary PW.
VCLABEL	Label of the VC bound to the interface.
TNLTYPE	Types of public network tunnels used by the VC such as LSP and CR-LSP.
ENTRYTYPE	Type of forwarding entries: ● SEND: forwarding entries of L2VPN except CCC ● CCC_SEND: forwarding entries of the CCC remote connection ● LOCAL: forwarding entries of the local connection ● INVALID: invalid forwarding entries
PWSTATE	PW state used for guiding packet forwarding: active or inactive. The primary PW and the secondary PW are mutually exclusive and both cannot be in the active state simultaneously.
BFDSTATE	BFD state used for guiding packet forwarding. If BFD is not configured, this flag bit is Up by default. If BFD is configured and the BFD session is Down (not Admin Down), this flag bit is Down and packets cannot be forwarded.
ADMIN	Whether the primary or secondary PW fault is configured manually: ● Up: indicates that the primary or secondary PW fault is not configured manually. ● Down: indicates that the primary or secondary PW fault is configured manually.
CTLWORD	Whether the control word is enabled on the local end: ● FALSE: indicates that the control word is disabled. ● TRUE: indicates that the control word is enabled.
CC	Connection channel of the VCCV: Control word Label alert.
CV	Connectivity verification.

Item	Description
TNLID	ID of the public tunnel used by the VC, which is a hexadecimal integer.
Record (s) Found	Number of VC forwarding entries on the local interface.
The Second PW Forward Information :	Forwarding information about the secondary PW.

# Display MPLS L2VPN forwarding information with VC label as 35842.

```
<HUAWEI> display mpls l2vpn forwarding-info 35842 interface vlanif 10
 The Main PW Forward Information :
VCLABEL TNLTYPE      ENTRYTYPE PWSTATE  BFDSTATE ADMIN CTLWORD CC CV TNLID
------------------------------------------------------------------------------
35842   LSP          SEND      ACTIVE   UP       UP    FALSE   0  0  0x1
   1   Record(s) Found.

 The Second PW Forward Information :
VCLABEL TNLTYPE      ENTRYTYPE PWSTATE  BFDSTATE ADMIN CTLWORD CC CV TNLID
------------------------------------------------------------------------------
   0   Record(s) Found.
```

10.5.15 display mpls l2vpn label-space

Function

The **display mpls l2vpn label-space** command displays information about label space distribution and different types of labels in the label cache.

Format

display mpls l2vpn label-space

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After L2VPN is enabled, run the **display mpls l2vpn label-space** command and you can view information about label space distribution and different types of labels in the label cache.

Example

# Display information about label space distribution when L2VPN is enabled and the cache contains labels.

```
<HUAWEI> display mpls l2vpn label-space
 there are 0 labels or label blocks in label-space.
 -------------------------------------------------------------
 label(s) released in SVC connection:             0
 label(s) released in LDP connection:             1
 label block(s) released in BGP connection:        0
 label(s) released in VPLS LDP connection:         0
 label block(s) released in VPLS BGP connection:   0
 -------------------------------------------------------------
```

Table 10-62 Description of the **display mpls l2vpn label-space** command output

Item	Description
Label	Indicates the value of the label in the label cache.
Label (s) released in SVC connection	Indicates the total number of labels in the label cache for the VLL SVC connections.
Label (s) released in LDP connection	Indicates the total number of labels in the label cache for the VLL LDP connections.
Label block (s) released in BGP connection	Indicates the total number of label blocks in the label cache for the VLL BGP connections.
Label (s) released in VPLS LDP connection	Indicates the total number of labels in the label cache for the VPLS LDP connections.
Label (s) released in VPLS BGP connection	Indicates the total number of labels in the label cache for the VPLS BGP connections.

10.5.16 display mpls l2vpn vpws

Function

The **display mpls l2vpn vpws** command displays information about the VPWS service.

Format

display mpls l2vpn vpws [**interface** *interface-type interface-number* [**verbose**]]

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.	-
verbose	Displays detailed VPWS service information.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

When configuring or commissioning VPWS, you can run the **display mpls l2vpn vpws** command to check whether VPWS service configurations are correct.

Note the following points when using the **display mpls l2vpn vpws** command:

- If **interface** *interface-type interface-number* is specified, only VPWS service information on a specified AC interface is displayed.
- If **verbose** is also specified, detailed information about the VPWS service on a specified AC interface is displayed.

Prerequisites

VPWS configurations are complete on the local end.

Example

# Display VPWS service information.

```
<HUAWEI> display mpls l2vpn vpws

Pri : Primary          Sec : Secondary          Byp : Bypass
PWb : PW-bypass          ACb : AC-bypass

Access Circuit              Virtual Circuit              States Active   Role
GE0/0/2                    10.3.3.9:200                 Up     Active   Pri
                           10.2.2.9:201               Up     Inactive Sec
```

Table 10-63 Description of the display mpls l2vpn vpws command output

Item	Description
Access Circuit	Access circuit.

Item	Description
Virtual Circuit	Virtual circuit.
States	VC status, which can be: ● Up ● Down
Active	Activation status of a VC, which can be: ● Active ● Inactive
Role	Role of a PW, which can be: ● Pri: Primary PW ● Sec: Secondary PW ● PWb: PW-bypass ● ACb: AC-bypass ● Byp: Bypass

# Display the detailed information about the VPWS service on a specified AC interface.

```
<HUAWEI> display mpls l2vpn vpws interface gigabitethernet 0/0/2 verbose

Access circuit      : GigabitEthernet0/0/2
Interface state     : Up
Protect mode        : FRR

Members:
Virtual Circuit               States Active   Role
10.3.3.9:200                   Up     Active   Primary
10.2.2.9:201                   Up     Inactive Secondary

Primary:
 VC type                : LDP VC
 VC state               : up
 Peer IP                : 10.3.3.9
 VC ID                  : 200
 Encapsulation type     : Ethernet
 LDP session state      : up
 VC information (Local / Remote)
  Label                 : 1025 / 1024
  MTU                   : 1500 / 1500
  Control word          : enable / enable
  Status code           : 0x0 / 0x0
  Group ID              : 0 / 0
  VCCV status           : cw alert ttl lsp-ping bfd / cw alert ttl lsp-ping bfd
 VC last up time        : 2013/12/21 16:42:51
 VC total up time       : 0 days, 6 hours, 20 minutes, 0 seconds

Secondary:
 VC type                : LDP VC
 VC state               : up
 Peer IP                : 10.2.2.9
 VC ID                  : 201
 Encapsulation type     : Ethernet
 LDP session state      : up
 VC information (Local / Remote)
  Label                 : 1026 / 1025
  MTU                  : 1500 / 1500
  Control word           : enable / enable
  Status code           : 0x0 / 0x0
  Group ID             : 0 / 0
  VCCV status           : cw alert ttl lsp-ping bfd / cw alert ttl lsp-ping bfd
 VC last up time        : 2013/12/21 14:57:13
 VC total up time       : 0 days, 20 hours, 44 minutes, 40 seconds
```

Table 10-64 Description of the display mpls l2vpn vpws command output

Item	Description
Access Circuit	Access circuit.
Protect mode	Protection mode, which can be FRR, independent, or master.
Members	PW member.
Virtual Circuit	Virtual circuit.
States	VC status
Active	Activation status of a VC, which can be:
Role	Role of a PW, which can be: ● Pri: Primary PW ● Sec: Secondary PW ● PWb: PW-bypass ● ACb: AC-bypass ● Byp: Bypass
Primary	Information about the primary PW.
VC type	The type of a VC.
VC state	VC status.
Peer IP	IP address of a peer.
VC ID	ID of a VC. The value is an integer in decimal notation. The default value is 0.
Encapsulation type	Encapsulation type of a VC.
LDP session state	Status of an LDP session.
VC information (Local / Remote)	VC information (local/remote).
Label	VC label.
MTU	Maximum transmission unit of a VC interface.
Control word	Whether the control word is enabled.

Item	Description
Status code	Status code, which can be: ● 0x0: indicates the forwarding state. ● 0x1: indicates the non-forwarding state. ● 0x06: indicates the ACOAM fault. ● 0x18: indicates the public network fault. ● 0x20: indicates the standby state.
Group ID	Group ID.
VCCV status	VCCV status.
VC last up time	Time when the VC last goes Up.
VC total up time	Total Up time of a VC.
Secondary	Information about the secondary PW.

10.5.17 display mpls label-stack vll interface

Function

The **display mpls label-stack vll interface** command displays information about label stacks in VLL networking.

Format

display mpls label-stack vll interface *interface-type interface-number*

Parameters

Parameter	Description	Value
interface-type interface-number	Specifies the type and number of an interface.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

To view information about label stacks in VLL networking, run the **display mpls label-stack vll interface** command.

Example

# Display information about the label stack on VLANIF100 in VLL networking.

```
<HUAWEI> display mpls label-stack vll interface vlanif 100
Label-stack  : 1
Level        : 1
Type         : VLL primary
Label        : 1027
Level        : 2
Type         : LDP
Label        : --
OutInterface : Vlanif1024
```

Table 10-65 Description of the **display mpls label-stack vll interface** command output

Item	Description
Label-stack	Number of label stacks
Level	Number of labels
Type	Tunnel type
Label	Value of the outgoing label
OutInterface	Outbound interface

10.5.18 display mpls static-l2vc

Function

The **display mpls static-l2vc** command displays information about static VCs on the device.

Format

display mpls static-l2vc [*vc-id* | **interface** *interface-type interface-number* | **state** { **down** | **up** }]

Parameters

Parameter	Description	Value
vc-id	Displays information about a static VC with a specified VC ID.	The value is an integer that ranges from 1 to 4294967295.

Parameter	Description	Value
interface *interface-type interface-number*	Displays information about all static PWs on a specified interface. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number.	-
state { **down** | **up** }	Displays VC information based on the VC status. ● **down**: Displays information about the VC in Down state. ● **up**: Displays information about the VC in Up state.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

If you run the **display mpls static-l2vc** command with the interface name specified, information about static VCs on the interface connected to a CE is displayed. If no interface is specified, information about static VCs on all interfaces is displayed.

Example

# Display information about static VCs on the device.

```
<HUAWEI> display mpls static-l2vc
 Total svc connections:  1,  1 up,  0 down

 *Client Interface     : Vlanif10 is up
  AC Status            : down
  VC State             : up
  VC ID                : 1
  VC Type              : VLAN
  Destination          : 2.2.2.2
  Transmit VC Label    : 400
  Receive VC Label     : 600
  Label Status         : 0
  Token Status         : 0
  Control Word         : Enable
  VCCV Capability      : cw alert ttl lsp-ping bfd
  active state         : active
  Link State           : down
  Tunnel Policy Name   : tun
  PW Template Name     : --
  Main or Secondary    : Main
```

```
load balance type    : flow
Access-port          : false
VC tunnel/token info : 1 tunnels/tokens
NO.0  TNL type       : lsp   , TNL ID : 0x800802
Backup TNL type      : lsp   , TNL ID : 0x0
Create time          : 0 days, 0 hours, 0 minutes, 34 seconds
UP time              : 0 days, 0 hours, 0 minutes, 31 seconds
Last change time     : 0 days, 0 hours, 0 minutes, 31 seconds
VC last up time      : 2011/07/04 20:29:18
VC total up time     : 0 days, 0 hours, 0 minutes, 33 seconds
CKey                 : 2
NKey                 : 1
BFD for PW           : unavailable
```

Table 10-66 Description of the **display mpls static-l2vc** command output

Item	Description
Total svc connections	Number of established SVCs, including the number of SVCs in Up and Down states.
Client Interface	AC interface and its status.
AC Status	Status of the AC: ● up ● down
VC State	Status of the VC: ● up ● down
VC ID	ID of the VC, which uniquely identifies a VC. If you run the **mpls static-l2vc** command without the VC ID specified, the value of this field is displayed as 0.
VC Type	Encapsulation type of the VC: ● VLAN ● Ethernet
Destination	LSR ID of the remote end on the VC.
Transmit VC Label	Local VC label.
Receive VC Label	Remote VC label.
Label Status	Whether the label can be used: ● 0: The label can be used. ● 1: Wait for the SMB to confirm the label status. ● 2: The label is released. ● 3: SMB confirmation failed.

Item	Description
Token Status	Whether the token can be used: ● 0: The token can be used. ● 1: Wait for the SMB to confirm the token status. ● 2: The token is released. ● 3: SMB confirmation failed.
Control Word	Whether the control word function is enabled: ● enable ● disable
VCCV Capability	Whether VCCV is enabled.
active state	Whether the PW is in active state. A PW in active state can forward packets. ● active ● inactive
Link State	Integrative PW status: ● up ● down If any of the following status is Down, the PW link state is Down: ● Service PW status ● OAM status
Tunnel Policy Name	Name of the tunnel policy.
PW Template Name	Name of the PW template.
Main or Secondary	Whether the VC is a primary VC or a secondary VC.
load balance type	Load balancing mode of Martini VLL: ● flow: indicates flow-based load balancing. ● packet: indicates packet-based load balancing.
Access-port	Whether the interface supports the access-port attribute: ● true: indicates that the interface supports the access-port attribute. ● false: indicates that the interface does not support the access-port attribute.
VC Tunnel/token info	Information about the VC tunnel or token used by the VC. The value **1 tunnels/tokens** indicates that the PW uses one tunnel or token.
NO.0 TNL Type	Type of the tunnel used by the PW

Item	Description
Backup TNL Type	Type of the backup tunnel when PW over LDP FRR is used.
Create time	How long the VC has been created.
UP time	How long the VC keeps the Up state.
Last change time	How long the VC status remains unchanged.
VC last up time	Last time when the VC became Up.
VC total up time	Total duration of the VC in Up state.
CKey	Index of the public tunnel for VPN QoS.
NKey	Index of the public tunnel.
BFD for PW	Whether BFD is configured. ● unavailable: indicates that BFD is not configured. ● available: indicates that BFD is configured. ● timeout: timeout period after which a BFD session fails to be established

# Display information about static VCs on VLANIF 10.

```
<HUAWEI> display mpls static-l2vc interface vlanif 10
 *Client Interface     : Vlanif10 is up
  AC Status            : down
  VC State             : up
  VC ID                : 1
  VC Type              : VLAN
  Destination          : 2.2.2.2
  Transmit VC Label    : 400
  Receive VC Label     : 600
  Label Status         : 0
  Token Status         : 0
  Control Word         : Enable
  VCCV Capability      : cw alert ttl lsp-ping bfd
  active state         : active
  Link State           : down
  Tunnel Policy        : tun
  PW Template Name     : --
  Main or Secondary    : Main
  load balance type    : flow
  Access-port          : false
  VC tunnel/token info : 1 tunnels/tokens
  NO.0  TNL Type       : lsp   , TNL ID : 0x56
  Backup TNL Type      : lsp   , TNL ID : 0x0
  Create time          : 0 days, 0 hours, 0 minutes, 34 seconds
  UP time              : 0 days, 0 hours, 0 minutes, 31 seconds
  Last change time     : 0 days, 0 hours, 0 minutes, 31 seconds
  VC last up time      : 2011/07/04 20:29:18
  VC total up time     : 0 days, 0 hours, 0 minutes, 33 seconds
  CKey                 : 2
  NKey                 : 1
  Diffserv Mode        : uniform
  Service Class        : be
  Color                : --
  DomainId             : --
```

```
Domain Name          : --
BFD for PW           : unavailable
```

Table 10-67 Description of the **display mpls static-l2vc interface** command output

Item	Description
Client Interface	AC interface and its status.
AC Status	Status of the link between the PE and its directly connected CE.
VC State	Status of the VC.
VC ID	ID of the VC, which uniquely identifies a VC.
VC Type	Encapsulation type of the VC.
Destination	LSR ID of the remote end on the VC.
Transmit VC Label	VC label sent by the local device.
Receive VC Label	VC label received by the local device.
Control Word	Whether the control word function is enabled.
VCCV Capability	Whether VCCV is enabled.
Tunnel Policy	Name of the tunnel policy. The value -- indicates that no tunnel policy is configured.
PW Template Name	Name of the PW template. The value -- indicates that no PW template is configured.
Main or Secondary	Whether the VC is a primary VC or a secondary VC.
VC tunnel/token info	Information about the tunnel or token used by the VC. The value **1 tunnels/tokens** indicates that the PW uses one tunnel or token.
Create time	How long the VC has been created.
UP time	How long the VC keeps the Up state.
Last change time	How long the VC status remains unchanged.
VC last up time	Last time when the VC became Up.
VC total up time	Total duration of the VC in Up state.
CKey	Index of the public tunnel for VPN QoS.
NKey	Index of the public tunnel.
Diffserv Mode	QoS DiffServ mode for VLL services.
Service Class	QoS service class for VLL services.
Color	QoS color for VLL services.

Item	Description
DomainId	ID of a domain.
Domain Name	Name of a domain.
BFD for PW	Whether BFD is configured. ● unavailable: indicates that BFD is not configured. ● available: indicates that BFD is configured. ● timeout: timeout period after which a BFD session fails to be established

# Display information about SVCs in Up state between peers.

```
<HUAWEI> display mpls static-l2vc state up
 Total svc connections:  1,  1 up,  0 down
 *Client Interface     : Vlanif10 is up
  AC Status            : up
  VC State             : up
  VC ID                : 0
  VC Type              : Ethernet
  Destination          : 2.2.2.2
  Transmit VC Label    : 100
  Receive VC Label     : 200
  Label Status         : 0
  Token Status         : 0
  Control Word         : Disable
  VCCV Capability      : alert ttl lsp-ping bfd
  active state         : active
  Link State           : up
  Tunnel Policy Name   : --
  PW Template Name     : --
  Main or Secondary    : Main
  load balance type    : flow
  Access-port          : false
  VC tunnel/token info : 1 tunnels/tokens
  NO.0  TNL Type       : lsp   , TNL ID : 0x56
  Backup TNL Type      : lsp   , TNL ID : 0x0
  Create time          : 0 days, 4 hours, 55 minutes, 41 seconds
  UP time              : 0 days, 4 hours, 55 minutes, 40 seconds
  Last change time     : 0 days, 4 hours, 55 minutes, 40 seconds
  VC last up time      : 2011/09/09 10:25:22
  VC total up time     : 0 days, 4 hours, 55 minutes, 40 seconds
  CKey                 : 19
  NKey                 : 1
  BFD for PW           : unavailable
```

Table 10-68 Description of the **display mpls static-l2vc state** command output

Item	Description
Total svc connections	Number of established SVCs, including the number of SVCs in Up and Down states.
Client Interface	AC interface and its status.
AC Status	Status of the AC.
VC State	Status of the VC.

Item	Description
VC ID	ID of the VC, which uniquely identifies a VC.
VC Type	Encapsulation type of the VC.
Destination	LSR ID of the remote end on the VC.
Transmit VC Label	Local VC label.
Receive VC Label	Remote VC label.
Control Word	Whether the control word function is enabled.
VCCV Capability	Whether VCCV is enabled.
Tunnel Policy Name	Name of the tunnel policy.
PW Template Name	Name of the PW template.
Main or Secondary	Whether the VC is a primary VC or a secondary VC.
Create time	How long the VC has been created.
UP time	How long the VC keeps the Up state.
Last change time	How long the VC status remains unchanged.
VC last up time	Last time when the VC became Up.
VC total up time	Total duration of the VC in Up state.
CKey	Index of the public tunnel for VPN QoS.
NKey	Index of the public tunnel.
BFD for PW	Whether BFD is configured. ● unavailable: indicates that BFD is not configured. ● available: indicates that BFD is configured. ● timeout: timeout period after which a BFD session fails to be established

10.5.19 display mpls static-l2vc brief

Function

The **display mpls static-l2vc brief** command displays brief information about static VCs on the device.

Format

display mpls static-l2vc brief

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The **display mpls static-l2vc brief** command is recommended when a large number of static VCs are configured on the device.

Example

# Display brief information about static VCs on the device.

```
<HUAWEI> display mpls static-l2vc brief
Total svc connections:  2,  1 up,  1 down

 *Client Interface          : Eth-Trunk2  is up
  AC Status                 : up
  VC State                  : up
  VC ID                     : 0
  VC Type                   : VLAN
  Destination               : 10.1.1.1

 *Client Interface          : Eth-Trunk3  is down
  AC Status                 : down
  VC State                  : down
  VC ID                     : 100
  VC Type                   : Ethernet
  Destination               : 10.1.1.2
```

Table 10-69 Description of the **display mpls static-l2vc brief** command output

Item	Description
Total SVC Connections	Number of established SVCs, including the number of SVCs in Up and Down states.
Client Interface	AC interface and its status.
AC Status	Status of the AC: ● up: An AC has been established. ● down: An AC is not established.
VC State	Status of the VC: ● up: A VC has been established. ● down: A VC is not established.

Item	Description
VC ID	ID of the static VC. If you run the **mpls static-l2vc** command without the VC ID specified, the value of this field is displayed as 0.
VC Type	Encapsulation type of the VC: ● VLAN ● Ethernet
Destination	IPv4 address of the peer. Generally, the value is the loopback address of the peer.

10.5.20 display traffic-statistics l2vpn interface

Function

The **display traffic-statistics l2vpn interface** command displays VLL traffic statistics on a specified interface.

Format

display traffic-statistics l2vpn interface *interface-type interface-number*

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Displays VLL traffic statistics 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

After enabling the function of collecting L2VPN traffic statistics by running the **mpls l2vpn traffic-statistics enable** command, you can run the **display traffic-statistics l2vpn interface** command to view traffic statistics on the created VLL. The VLL traffic sent and received through the interface are collected from the time when the VLL becomes Up to the time you run the **display traffic-statistics l2vpn interface** command.

Example

# Display VLL traffic statistics on VLANIF10.

```
<HUAWEI> display traffic-statistics l2vpn interface vlanif 10
 Input: 1000 bytes, 10 packets
 Output: 2000 bytes, 20 packets
```

10.5.21 display vll ccc

Function

The **display vll ccc** command displays information about a CCC connection.

Format

display vll ccc [*ccc-name* | **type** { **local** | **remote** }]

Parameters

Parameter	Description	Value
ccc-name	Specifies the connection name.	The value is an existing connection name.
type	Specifies the CCC connection type.	-
local	Displays local CCC connections.	-
remote	Displays remote CCC connections.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After a CCC connection is configured, you can use the **display vll ccc** command to see whether the configuration is successful.

If you do not specify a connection name or type, information about all the existing CCC connections is displayed.

Example

# Display a specified CCC connection.

```
<HUAWEI> display vll ccc CE1-CE2
name: CE1-CE2, type: remote, state: up
intf: Vlanif11 (up ethernet), in-label: 116 ,
out-label: 119 , nexthop: 10.1.1.1
no control word
VC last up time : 2009/10/08 13:38:01
VC total up time: 0 days, 0 hours, 11 minutes, 2 seconds
```

# Display information about all the CCC connections.

```
<HUAWEI> display vll ccc
total  ccc vc : 1
local  ccc vc : 0,  0 up
remote ccc vc : 1,  1 up

name: CE1-CE2, type: remote, state: up,
intf: Vlanif11 (up), in-label: 116 , out-label: 119 , nexthop: 10.1.1.1
VC last up time : 2009/10/08 13:38:01
VC total up time: 0 days, 0 hours, 10 minutes, 50 seconds
```

Table 10-70 Description of the display vll ccc command output

Item	Description
total ccc vc	Total number of CCC local connections and remote connections at the local end.
local ccc vc	The number of CCC local connections at the local end.
remote ccc vc	The number of CCC remote connections at the local end.
name	Name of CCC connection in a character string.
type	Types of CCC connections. ● local: connection between two CEs that are connected to the same PE. ● remote: connection between CEs that are connected to two different PEs.

Item	Description
state	Status of a CCC connection: ● down: indicates that the CCC connection fails because the configuration is incorrect or the associated interface is Down. ● up: indicates that the CCC connection is set up successfully.
intf	Interface connected to the CCC connection. The S300, S500, S2700, S5700, and S6700 supports only VLANIF interfaces to be connected to CCC connections. By default, the Ethernet encapsulation type is adopted.
in-label	Incoming label of the CCC connection that is specified manually. It is consistent with the outgoing label of the peer end.
out-label	Outgoing label of the CCC connection which is specified manually. It is consistent with the incoming label of the peer end.
nexthop	Next-hop address of the CCC connection.
VC last up time	Indicates the last time the VC was Up.
VC total up time	Indicates the total duration the VC is Up.

# Display information about all the local CCC connections.

```
<HUAWEI> display vll ccc type local
total local  ccc vc : 1,  1 up
name: c2, type: local, state: up,
intf1: Vlanif10 (up),  access-port: false

intf2: Vlanif11 (up),  access-port: false
VC last up time : 2009/03/23 11:16:07
VC total up time: 0 days, 0 hours, 14 minutes, 14 seconds
```

Table 10-71 Description of the display vll ccc type local command output

Item	Description
total local ccc vc	Total number of local CCC connections and the number of local CCC connections whose status is Up.
name	Name of the CCC connection in a character string.
type: local	Information about the local CCC connection. Local indicates the connection between two CEs that are connected to a PE.

Item	Description
state	Status of a CCC connection: ● down: indicates that the CCC connection fails to be set up. The cause may be that the configuration is incorrect or the associated interface is Down. ● up: indicates that the CCC connection is successfully set up.
intf1: Vlanif10 (up), intf2: Vlanif11 (up)	Interfaces of the local connection on two CEs. One is Vlanif10(the status is Up), and the other is Vlanif11(the status is Up).
access-port	Whether the interface supports the access-port attribute. ● true: indicates that the interface supports the access-port attribute. ● false: indicates that the interface does not support the access-port attribute.

# Display information about all the remote CCC connections.

```
<HUAWEI> display vll ccc type remote
total remote ccc vc : 1,  1 up
name: CE1-CE2, type: remote, state: up,
intf: Vlanif11 (up), in-label: 116 , out-label: 119 , nexthop: 10.1.1.1
VC last up time : 2007/10/08 13:38:01
VC total up time: 0 days, 0 hours, 18 minutes, 10 seconds
```

Table 10-72 Description of the display vll ccc type remote command output

Item	Description
total remote ccc vc	Total number of remote CCC connections and the number of remote CCC connections whose status is Up.
name	Name of CCC connection in a character string.
type: remote	Type of the displayed CCC connection. The word **remote** indicates that the connection is of the remote type.
state	Status of a CCC connection: ● down: indicates that the CCC connection fails to be set up. The cause may be that the configuration is incorrect or the associated interface is Down. ● up: indicates that the CCC connection is successfully set up.

Item	Description
intf: Vlanif11 (up)	Access interface on the CE for setting up CCC connection at the local end. The interface is Vlanif11, and its status is Up.
in-label	Incoming label of the CCC connection. The label is manually specified, and is consistent with the outgoing label of the peer.
out-label	Outgoing label of the CCC connection. The label is manually specified, and is consistent with the incoming label of the peer.
nexthop	Next-hop address of the CCC connection.

10.5.22 interface-parameter-type vccv (interface view)

Function

The **interface-parameter-type vccv** command configures Mapping packets to carry the VCCV byte.

The **undo interface-parameter-type vccv** command deletes the VCCV byte (an interface parameter) in the Mapping packet.

By default, a Mapping packet carries the VCCV byte.

Format

interface-parameter-type vccv [**secondary**]

undo interface-parameter-type vccv [**secondary**]

Parameters

Parameter	Description	Value
secondary	Indicates that the configuration applies to the secondary VC. If this keyword is not specified, the command applies to the primary VC. The command can be configured only when a local VC exists.	-

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

The command can be configured only when a local VC exists.

Example

# When configuring the VLL in LDP mode on an interface, delete the VCCV byte in the Mapping packet.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 10
[HUAWEI-Vlanif10] mpls l2vc 2.2.2.2 100
[HUAWEI-Vlanif10] undo interface-parameter-type vccv
```

10.5.23 ignore-mtu-match (MPLS-L2VPN instance view)

Function

The **ignore-mtu-match** command disables the MTU matching check of the L2VPN on both ends.

The **undo ignore-mtu-match** command enables the check.

By default, the PE checks whether MTUs of the L2VPN instances on both ends are consistent.

Format

ignore-mtu-match

undo ignore-mtu-match

Parameters

None

Views

MPLS-L2VPN instance view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In a Kompella VLL networking, if a Huawei device connects to a non-Huawei device that does not support MTU matching check, run the **ignore-mtu-match** command to configure the Huawei device to ignore the check.

Prerequisites

vpn-target is not configured for the L2VPN instance.

Precautions

By default, a PE checks whether MTUs of the L2VPN instances at both ends are consistent. If not, the VC cannot be in the Up state.

Example

# Ignore the check of MTU of the L2VPN instance named vpn1.

```
<HUAWEI> system-view
[HUAWEI] mpls l2vpn vpn1
[HUAWEI-mpls-l2vpn-vpn1] ignore-mtu-match
```

10.5.24 l2vpn-family

Function

The **l2vpn-family** command displays the BGP-L2VPN address family view.

The **undo l2vpn-family** command deletes all configurations in the BGP-L2VPN address family view.

NOTE

You can run this command on the S5731S-S or S6730S-S to enter the BGP-L2VPN address family view but cannot configure VLL configuration commands in this view.

Only MPLS-capable devices support the VLL configuration commands in the BGP-L2VPN address family view. For the S5731-S and S6730-S, when the MPLS function license is not obtained, you can run this command to enter the BGP-L2VPN address family view but cannot configure VLL configuration commands in this view.

Format

l2vpn-family

undo l2vpn-family

Parameters

None

Views

BGP view

Default Level

2: Configuration level

Usage Guidelines

In Kompella VLL networking, you can run the **l2vpn-family** command to enter the BGP-L2VPN address family view.

Example

# Display the BGP-L2VPN address family view.

```
<HUAWEI> system-view
[HUAWEI] bgp 100
[HUAWEI-bgp] l2vpn-family
[HUAWEI-bgp-af-l2vpn]
```

10.5.25 manual-set pw-ac-fault

Function

The **manual-set pw-ac-fault** command simulates a fault on the primary or secondary PW.

The **undo manual-set pw-ac-fault** command cancels the fault that is simulated on a primary or secondary PW.

By default, no fault is simulated on a PW.

Format

manual-set pw-ac-fault [**secondary**]

undo manual-set pw-ac-fault [**secondary**]

Parameters

Parameter	Description	Value
secondary	Simulates a fault on the secondary PW. If this parameter is not specified, a fault is simulated on the primary PW.	-

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On a network where the primary and secondary PWs need to be configured, you can run the **manual-set pw-ac-fault** command to simulate a fault on the primary or secondary PW to check whether services can be switched between the primary and secondary PWs.

Prerequisites

A VC has been created.

Example

# Simulate a fault on the PW.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 10
[HUAWEI-Vlanif10] mpls l2vc 2.2.2.2 100
[HUAWEI-Vlanif10] manual-set pw-ac-fault
```

10.5.26 mpls l2vc

Function

The **mpls l2vc** command creates a Martini VLL.

The **undo mpls l2vc** command deletes the Martini VLL from an interface.

By default, no Martini L2VPN connection is created.

Format

mpls l2vc { *ip-address* | **pw-template** *pw-template-name* } * *vc-id* [**group-id** *group-id* | **tunnel-policy** *policy-name* | [**control-word** | **no-control-word**] | [**raw** | **tagged**] | **mtu** *mtu-value* | [**secondary** | **bypass**] | **ignore-standby-state**] *

undo mpls l2vc { *ip-address* | **pw-template** *pw-template-name* } * *vc-id* [**group-id** *group-id* | **tunnel-policy** *policy-name* | [**control-word** | **no-control-word**] | [**raw** | **tagged**] | **mtu** *mtu-value* | [**secondary** | **bypass**] | **ignore-standby-state**] *

undo mpls l2vc [**secondary** | **bypass**]

Parameters

Parameter	Description	Value
ip-address	Specifies the LSR ID of a peer device on the PW.	The value is in dotted decimal notation.
pw-template *pw-template-name*	Specifies the name of a PW template.	The value is a string of 1 to 19 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
vc-id	Specifies a L2VC ID.	The value is an integer that ranges from 1 to 4294967295.

Parameter	Description	Value
group-id *group-id*	Specifies a VC group ID. With the VC group ID specified, the system can execute the same operation on a group of VCs; therefore, fewer packets are exchanged between PEs. Only the VCs with the same attribute can be configured with the same VC group ID; otherwise, the PW may be torn down by mistake. This parameter is valid only on sub-interfaces.	The value is an integer that ranges from 1 to 4294967295.
tunnel-policy *policy-name*	Specifies the name of a tunnel policy.	The value is a string of 1 to 39 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
raw	Removes the provider-tag (P-Tag) from a packet. **NOTE** This parameter can be used only for Ethernet links. If neither **raw** nor **tagged** is specified, this command sets the **raw** mode on a main interface and the **tagged** mode on a sub-interface.	-
tagged	Retains the P-Tag in a packet. **NOTE** This parameter can be used only for Ethernet links. If neither **raw** nor **tagged** is specified, this command sets the **raw** mode on a main interface and the **tagged** mode on a sub-interface.	-

Parameter	Description	Value
control-word	Enables the control word function.	-
no-control-word	Disables the control word function.	-
mtu *mtu-value*	Specifies the MTU value. **NOTE** This parameter can be configured only on VLANIF interfaces. The MTU of another type of interface or its sub-interface can be configured in the PW template.	The value is an integer that ranges from 46 to 9600. The default value is 1500.
secondary	Indicates a secondary VC. If this parameter is not specified, a primary VC is created. You can configure a secondary VC only when the primary VC exists on the local device.	-
bypass	Indicates that the VC is a bypass VC. The encapsulation type of the bypass VC must be the same as that of the primary VC.	-
ignore-standby-state	Indicates that the PW ignores standby state information sent by the remote device.	-

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In a Martini VLL networking, you can run this command to create a VC connection for a Martini VLL.

According to different encapsulation modes on the AC interfaces, the system processes user packets in different ways, as shown in the following tables.

- Packet processing on the inbound interface in the VLL or PWE3 scenario.

AC Interface Type	Encapsulation Mode of raw	Encapsulation Mode of tagged
Dot1q termination sub-interface	Removes a tag.	No action is required.
Ethernet main interfaces	No action is required.	Adds a tag.
QinQ stacking sub-interface	No action is required.	Adds a tag.
QinQ termination sub-interface (in symmetrical mode)	Removes the outer tag.	No action is required.
QinQ termination sub-interface (in asymmetrical mode)	Removes two tags.	Removes the outer tag.
VLANIF interface (added to the VLAN in default mode)	No action is required.	Adds a tag (default VLAN ID of the interface).
VLANIF interface (added to the VLAN in non-default mode)	Removes the outer tag.	No action is required.

- Packet processing on the outbound interface in the VLL or PWE3 scenario.

AC Interface Type	Encapsulation Mode of raw	Encapsulation Mode of tagged
Dot1q termination sub-interface	Adds a tag.	No action is required.
Ethernet main interfaces	Adds a tag.	Replaces the tag with the tag that is encapsulated on the outbound interface.
QinQ stacking sub-interface	No action is required.	Removes a tag.
QinQ termination sub-interface (in symmetrical mode)	Adds the outer tag.	Replaces the outer tag with the tag that is encapsulated on the outbound interface.

AC Interface Type	Encapsulation Mode of raw	Encapsulation Mode of tagged
QinQ termination sub-interface (in asymmetrical mode)	Adds two tags.	Removes the outer tag and then adds two tags that are encapsulated on the outbound interface.
VLANIF interface (added to the VLAN in default mode)	No action is required.	Removes a tag.
VLANIF interface (added to the VLAN in non-default mode)	Adds the outer tag.	Replaces the tag with the tag that is encapsulated on the outbound interface.

Precautions

- An interface cannot function as an L2VPN AC interface and L3VPN AC interface at the same time. After an interface is bound to an L2VPN, Layer 3 features such as the IP address and routing protocol on this interface become invalid.
- You must create dynamic VCs on PEs at both ends of a PW to connect the PEs. The destination address of a VC is the LSR ID of the peer PE.
- You can set attributes for a PW template, including the remote peer, tunnel policy, control word, and VCCV. When configuring an LDP PW, you can directly apply the PW template without specifying attributes for the PW. After setting attributes for a PW template, you can update the PW template at any time. The modified PW template takes effect only after the **reset pw** command is run.
- If a PW attribute is specified in the **mpls l2vc** command, the corresponding PW attribute in the same PW template is invalid.
- If you do not specify a tunnel policy for a Martini connection, the default tunnel policy is used. By default, the LSP tunnel is preferentially selected and only one tunnel is used for load balancing. If a tunnel policy name is specified but the tunnel policy is not configured, the default tunnel policy is used.
- The MTU value is specified when you create Martini or PWE3 VLLs and is used for interconnection between the switch and other devices.
- You must configure the primary PW before configuring the secondary PW and delete the secondary PW before deleting the primary PW.
- When creating VCs dynamically, the latest configurations of some parameters override the previous ones. The parameters include **tunnel-policy** *tnl-policy-name*, **control-word**, and **no-control-word**.
- By default, link type negotiation is enabled globally on the device. If a VLANIF interface is used as an AC-side interface for L2VPN, the configuration conflicts with link type negotiation. In this case, run the **lnp disable** command in the system view to disable link type negotiation.
- When configuring BFD for static PW, the VC ID must be specified.

NOTE

- If a sub-interface is bound to a VLL, the sub-interface can be deleted only after the sub-interface is unbound from the VLL.
- If a sub-interface is bound to a VLL, you cannot change the encapsulation type of the main interface.

Example

# Create a Martini connection on the VLANIF interface.

```
<HUAWEI> system-view
[HUAWEI] vlan batch 10
[HUAWEI] interface vlanif 10
[HUAWEI-Vlanif10] mpls l2vc 10.2.2.9 100
```

# Create a Martini connection on the GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] mpls l2vc 10.2.2.9 100
```

10.5.27 mpls l2vpn

Function

The **mpls l2vpn** command enables MPLS L2VPN and displays the MPLS L2VPN view.

The **undo mpls l2vpn** command disables MPLS L2VPN and deletes all the L2VPN configurations.

By default, the MPLS L2VPN function is disabled.

Format

mpls l2vpn

undo mpls l2vpn

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To configure MPLS L2VPN functions or perform configurations in the MPLS L2VPN view on the MPLS L2VPN network, run the **mpls l2vpn** command to enable MPLS L2VPN and enter the MPLS L2VPN view.

Prerequisites

Basic MPLS functions have been configured. For details, see the **mpls lsr-id** and **mpls** commands.

Precautions

When the command is configured, a P device does not need to be enabled with the MPLS L2VPN function.

After the **mpls l2vpn** command is executed:

- If MPLS L2VPN is disabled on the device, MPLS L2VPN is enabled and the MPLS L2VPN view is displayed.
- If MPLS L2VPN is enabled on the device, the MPLS L2VPN view is displayed.

NOTICE

After the **undo mpls l2vpn** command is run in the system view, L2VPN services may be interrupted, and all L2VPN configurations are cleared. If you want to restore the L2VPN configurations, re-run all the deleted commands.

Example

# Enable MPLS L2VPN.

```
<HUAWEI> system-view
[HUAWEI] mpls lsr-id 10.1.1.1
[HUAWEI] mpls
[HUAWEI-mpls] quit
[HUAWEI] mpls l2vpn
[HUAWEI-l2vpn]
```

10.5.28 mpls l2vpn alarm verification disable

Function

The **mpls l2vpn alarm verification disable** command disables MPLS L2VPN alarm verification.

The **undo mpls l2vpn alarm verification disable** command enables MPLS L2VPN alarm verification.

By default, MPLS L2VPN alarm verification is enabled.

Format

mpls l2vpn alarm verification disable

undo mpls l2vpn alarm verification disable

Parameters

None

Views

MPLS-L2VPN view

Default Level

2: Configuration level

Usage Guidelines

If MPLS L2VPN alarm verification is enabled on a device, the device regularly sends service alarms to the fault management (FM) module until these alarms are cleared. The FM then compares received alarms with locally stored alarms. If a received alarm is different from any of the locally stored alarms, the FM module reports the alarm to the NMS. If a received alarm is the same as a locally stored alarm, the FM module does not report this alarm.

Sometimes, alarms cleared on the device may still be displayed on the NMS. To ensure alarm consistency between the device and NMS, the FM module ages out such alarms after three alarm verification intervals and then instructs the NMS to delete these alarms. This function effectively eliminates alarm residue to improve alarm reliability.

If a large number of services exist, MPLS L2VPN alarm verification may regularly drive the CPU usage to a high level, affecting service performance. In this case, you can run the **mpls l2vpn alarm verification disable** command to disable MPLS L2VPN alarm verification. After MPLS L2VPN alarm verification is disabled, the device sends service alarms to the FM module only once, and the FM module cannot age out cleared alarms.

Example

# Disable MPLS L2VPN alarm verification.

```
<HUAWEI> system-view
[HUAWEI] mpls l2vpn
[HUAWEI-l2vpn] mpls l2vpn alarm verification disable
```

10.5.29 mpls l2vpn default martini

Function

The **mpls l2vpn default martini** command configures the dynamic VC signaling not to carry status information.

The **undo mpls l2vpn default martini** command restores the default configuration.

By default, the dynamic VC signaling carries status information.

Format

mpls l2vpn default martini

undo mpls l2vpn default martini

Parameters

None

Views

MPLS-L2VPN view

Default Level

2: Configuration level

Usage Guidelines

To configure the dynamic VC signaling not to carry status information in VLL scenarios, run the **mpls l2vpn default martini** command. In other scenarios, do not run this command.

NOTE

- If the dynamic VC signaling carries status information, the local end can send Notification messages to the peer end. For details about Notification messages, see Chapter "PWE3 Principles" in the "PWE3 Configuration".
- Before using the **mpls l2vpn default martini** command, you must delete the configurations of VCs (including PWE3 VCs and VPLS VCs) that support Notification messages.

Example

# Configure the dynamic VC signaling not to carry status information.

```
<HUAWEI> system-view
[HUAWEI] mpls l2vpn
[HUAWEI-l2vpn] mpls l2vpn default martini
```

# Restore the default dynamic VC signaling configuration.

```
<HUAWEI> system-view
[HUAWEI] mpls l2vpn
[HUAWEI-l2vpn] undo mpls l2vpn default martini
```

10.5.30 mpls l2vpn flow-label

Function

The **mpls l2vpn flow-label** command enables flow label-based load balancing for PWs on an interface.

The **undo mpls l2vpn flow-label** command disables flow label-based load balancing for PWs on an interface.

By default, flow label-based load balancing is disabled for PWs on an interface.

NOTE

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

Format

mpls l2vpn flow-label { **both** | **send** | **receive** } [**secondary**] [**static**]

undo mpls l2vpn flow-label { **both** | **send** | **receive** } [**secondary**] [**static**]

undo mpls l2vpn flow-label [**secondary**]

Parameters

Parameter	Description	Value
both	Enables flow label-based load balancing for outgoing traffic and incoming traffic.	-
send	Enables flow label-based load balancing for outgoing traffic.	-
receive	Enables flow label-based load balancing for incoming traffic.	-
secondary	Enables flow label-based load balancing for the secondary PW. If **secondary** is not configured, flow label-based load balancing is configured for the primary PW. Flow label-based load balancing can be configured for a secondary PW only if the secondary PW exists.	-
static	Statically configures flow label-based load balancing. For dynamic PWs, if **static** is not configured, the flow label-based load balancing capability of the local end is negotiated by the remote end. For static PWs, the flow label-based load balancing capability is statically configured, irrespective of whether **static** is configured.	-

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When multiple links exist between provider (P) devices, configure flow label-based load balancing to improve L2VPN traffic forwarding efficiency. After flow label-based load balancing is enabled on a PE, the PE adds different labels for different

L2VPN data flows to distinguish the data flows. After a P device receives a data packet carrying a flow label, it performs the Hash calculation and selects a forwarding path based on the flow label in the data packet. This processing implements load balancing. You can run the **mpls l2vpn flow-label** command to enable flow label-based load balancing for L2VPN on an interface.

Prerequisites

Before you enable flow label-based load balancing for an interface, create a VC connection on this interface and enable Multiprotocol Label Switching (MPLS) L2VPN.

Precautions

Flow label-based load balancing can be enabled only when any of the following conditions is true:

- The **receive** parameter is configured on the local PE, and the **send** parameter is configured on the remote PE.
- The **send** parameter is configured on the local PE, and the **receive** parameter is configured on the remote PE.
- Both the **send** and **receive** parameters are configured on the local and remote PEs.

The **secondary** parameter indicates that flow label-based load balancing takes effect only for the secondary PW. If you specify **secondary** parameter, flow label-based load balancing takes effect only for the primary PW.

Example

# Enable flow label-based load balancing for PWs on Vlanif 100.

```
<HUAWEI> system-view
[HUAWEI] interface Vlanif 100
[HUAWEI-Vlanif100] mpls l2vc 2.2.2.2 100
[HUAWEI-Vlanif100] mpls l2vpn flow-label both
```

10.5.31 mpls l2vpn ip-parse enable

Function

The **mpls l2vpn ip-parse enable** command enables the IP packet parsing function of the MPLS L2VPN module.

The **undo mpls l2vpn ip-parse enable** command disables the IP packet parsing function of the MPLS L2VPN module.

By default, the IP packet parsing function of the MPLS L2VPN module is enabled.

Format

mpls l2vpn ip-parse enable

undo mpls l2vpn ip-parse enable

NOTE

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

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In a Layer 2 VPN scenario, if a traffic policy is configured in the inbound direction of an AC-side interface on a device, L2VPN traffic forwarded from a PE may incorrectly match the traffic policy. As a result, traffic fails to be forwarded. To ensure normal traffic forwarding, run the **undo mpls l2vpn ip-parse enable** command to disable the IP packet parsing function of the MPLS L2VPN module.

Precautions

If the enhanced load balancing mode is configured for an Eth-Trunk, it is recommended that the IP packet parsing function of the MPLS L2VPN module be enabled.

Example

# Disable the IP packet parsing function of the MPLS L2VPN module.

```
<HUAWEI> system-view
[HUAWEI] undo mpls l2vpn ip-parse enable
```

10.5.32 mpls l2vpn l2vpn-name

Function

The **mpls l2vpn** *l2vpn-name* command creates a L2VPN instance in the Kompella mode.

The **undo mpls l2vpn** *l2vpn-name* command deletes the L2VPN instance.

By default, no Kompella L2VPN instance is created.

Format

mpls l2vpn *l2vpn-name* [**encapsulation** *encapsulation* [**control-word** | **no-control-word**]]

undo mpls l2vpn *l2vpn-name*

Parameters

Parameter	Description	Value
l2vpn-name	Specifies a L2VPN instance name.	The value must be an existing VPN instance name.
encapsulation *encapsulation*	Indicates the encapsulation type of the L2VPN instance. The encapsulation type can be **ethernet** or **vlan**.	-
control-word | **no-control-word**	Enables or disables the control word. By default, the control word is disabled.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In a Kompella VLL networking, you can use this command to create a VPN.

Precautions

The specified encapsulation of an L2VPN must be the same as that of the CE interface.

Example

# Create a VPN in Kompella mode.

```
<HUAWEI> system-view
[HUAWEI] mpls l2vpn vpn1 encapsulation vlan
[HUAWEI-mpls-l2vpn-vpn1]
```

# Enter the MPLS-L2VPN instance view.

```
<HUAWEI> system-view
[HUAWEI] mpls l2vpn vpn1
[HUAWEI-mpls-l2vpn-vpn1]
```

10.5.33 mpls l2vpn pw bfd

Function

The **mpls l2vpn pw bfd** command enables dynamic BFD for PWs and adjusts BFD parameters on an AC interface.

The **undo mpls l2vpn pw bfd** command restores default BFD parameters of dynamic BFD for PWs on an AC interface.

By default, dynamic BFD for PWs is not configured on an AC interface.

Format

mpls l2vpn pw bfd [**detect-multiplier** *multiplier* | **min-rx-interval** *rx-interval* | **min-tx-interval** *tx-interval*] * [**remote-vcid** *vc-id*] [**secondary**]

undo mpls l2vpn pw bfd [**detect-multiplier** | **min-rx-interval** | **min-tx-interval**] * [**secondary**]

undo mpls l2vpn pw bfd [**detect-multiplier** *multiplier* | **min-rx-interval** *rx-interval* | **min-tx-interval** *tx-interval*] * [**remote-vcid** *vc-id*] [**secondary**]

Parameters

Parameter	Description	Value
detect-multiplier *multiplier*	Specifies the local detection multiplier.	The value is an integer that ranges from 3 to 50. The default value is 3.
min-rx-interval *rx-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-S, S5731-H and S5731S-H, the value ranges from 3 to 1000. ● After the **set service-mode enhanced-bfd** command is configured on the S5732-H, S6730-S, S6730-H, and S6730S-H, the value ranges from 3 to 1000.

Parameter	Description	Value
min-tx-interval *tx-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-S, S5731-H and S5731S-H, the value ranges from 3 to 1000. ● After the **set service-mode enhanced-bfd** command is configured on the S5732-H, S6730-S, S6730-H, and S6730S-H, the value ranges from 3 to 1000.
remote-vcid *vc-id*	Specifies the VC ID of the peer device.	This parameter is mandatory when a multi-hop PW is detected. The value of this parameter is the VC ID of the remote end of the PW. The value is an integer that ranges from 1 to 4294967295.
secondary	Configures BFD and its parameters on the secondary PW. By default, BFD and its parameters are configured on the primary PW. **NOTE** The **secondary** parameter cannot be run on Loopback interface view.	-

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On a network where BFD is used to detect faults, run the **mpls l2vpn pw bfd** command to enable dynamic BFD for PWs and adjust BFD parameters on an AC interface.

Precautions

To reduce usage of system resources, when a BFD session is detected in Down state, the system changes the minimum interval for receiving BFD packets and the minimum interval for sending BFD packets to random values between 1000 ms and 3000 ms. When the BFD session becomes Up, the configured intervals are restored.

Example

# Enable dynamic BFD for PWs on VLANIF 10 and set BFD parameters.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 10
[HUAWEI-Vlanif10] mpls l2vc 2.2.2.2 100
[HUAWEI-Vlanif10] mpls l2vpn pw bfd min-rx-interval 100 min-tx-interval 100
```

10.5.34 mpls l2vpn reroute

Function

The **mpls l2vpn reroute** command configures the revertive switchover policy for the primary and secondary PWs in FRR or PW redundancy master/slave mode.

The **undo mpls l2vpn reroute** command restores the default revertive switchover policy.

By default, delayed revertive switchover is configured in FRR or PW redundancy master/slave mode.

Format

mpls l2vpn reroute { { **delay** *delay-time* | **immediately** } [**resume** *resume-time*] | **never** }

undo mpls l2vpn reroute

Parameters

Parameter	Description	Value
delay *delay-time*	Specifies the revertive switchover policy for the primary and secondary PWs as delayed revertive switchover, and sets the duration for delayed switchover.	The value is an integer that ranges from 10 to 1800, in seconds. The default value is 30.

Parameter	Description	Value
immediately	Specifies the revertive switchover policy for the primary and secondary PWs as immediate revertive switchover.	-
resume *resume-time*	Specifies a delay after which the local device notifies the peer PE on the secondary PW of the recovery. You can set this parameter only in VLL FRR mode.	The value is an integer that ranges from 0 to 600, in seconds. The default value is 10.
never	Specifies the revertive switchover policy for the primary and secondary PWs to none revertive switchover. After the primary PW recovers, traffic is not switched to it until the secondary PW is faulty.	-

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **mpls l2vpn reroute** command configures the revertive switchover policy for the primary and secondary PWs in FRR or PW redundancy master/slave mode.

Prerequisites

The primary and secondary PWs have been configured in FRR or PW redundancy master/slave mode. The revertive switchover policy cannot be configured for PW redundancy independent mode.

Precautions

In VLL FRR mode and in PW redundancy master/slave mode, the PW revertive switchover policy is classified into the following modes:

- Immediate revertive switchover: When the primary PW recovers from a fault, the local PE switches traffic back to the primary PW immediately and notifies the peer PE on the secondary PW of the fault. In FRR mode, the local PE notifies the peer PE on the secondary PW of the recovery after a delay of *resume-time*. In PW redundancy master/slave mode, the parameter *resume-time* is not supported.

  This revertive switchover applies to scenarios in which users hope traffic to be restored as soon as possible.

- Delayed revertive switchover: When the primary PW recovers from a fault, traffic is switched back to the primary PW after a period specified by *delay-time*. After traffic is switched back, the local device immediately notifies the peer device on the secondary PW of the fault. If *resume-time* is configured in FRR mode, the local device notifies the peer device on the secondary PW of the recovery after a delay of *resume-time*.

  On a large-scale network, packet loss caused by incomplete route convergence may occur during the switchback. To prevent this problem, configure traffic to be switched back after a delay.
- None revertive switchover: When the primary PW recovers from a fault, traffic is not switched back to the primary PW until the secondary PW becomes faulty.

  If you do not want traffic to be frequently switched between the primary and secondary PWs, you can use the non-revertive switchover.

In a CE asymmetrical networking, if the Ethernet OAM function is configured on a PE interface connected to a CE, and a revertive switchover policy is configured, the value of *resume-time* cannot be 0 seconds. The value must be equal to or greater than 1 second.

Example

# Configure the device to switch traffic back to the primary PW 15 seconds after the primary PW recovers from a fault, notify the peer PE on the secondary PW of the fault when a switchover is performed, and notify the peer PE of the secondary PW of the recovery 20 seconds later.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] mpls l2vc 10.1.1.9 100
[HUAWEI-Vlanif100] mpls l2vc 10.2.2.9 200 secondary
[HUAWEI-Vlanif100] mpls l2vpn reroute delay 15 resume 20
```

10.5.35 mpls l2vpn service-name

Function

The **mpls l2vpn service-name** command sets the name of an SVC or Martini VLL service or a PWE3 service.

The **undo mpls l2vpn service-name** command deletes the configured L2VPN service name.

By default, no L2VPN service name is configured in the system.

Format

mpls l2vpn service-name *service-name*

undo mpls l2vpn service-name

Parameters

Parameter	Description	Value
service-name	Specifies the name of an L2VPN service. This parameter uniquely identifies an L2VPN service on a PE.	The value is a string of 1 to 15 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

By default, an SVC or Martini VLL service or a PWE3 service is uniquely identified by the combination of the VC ID and VC type, which are hard to remember and make maintenance complex. When a service name is used to uniquely identify an L2VPN service, the name can be defined based on requirements and the NMS operator can maintain the L2VPN service by clicking the name on the NMS graphical user interface (GUI). This simplifies operation and maintenance.

Prerequisites

An SVC or Martini VLL service or a PWE3 service has been configured on a service interface. A primary PW and a secondary PW can be configured for a Martini VLL or PWE3 service.

Precautions

On each PE, an L2VPN service name is unique. If an L2VPN service name has been used by a PW, it cannot be configured for another PW, or the system will display an error message.

If an L2VPN service already has a service name, this service name will be overwritten when a new name is configured for the L2VPN service. Therefore, when changing an L2VPN service name, you can directly configure a new service name without deleting the original one.

- Because the primary and secondary PWs are configured on the same interface, they are regarded as one PW, and a service name is configured for both of them.
- On each PE, an L2VPN service name is unique.

Example

# Set an L2VPN service name to **pw1** on a service interface.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 10
[HUAWEI-Vlanif10] mpls l2vc 10.1.1.1 1
[HUAWEI-Vlanif10] mpls l2vpn service-name pw1
```

10.5.36 mpls l2vpn vlan-stacking

Function

The **mpls l2vpn vlan-stacking** command configures the stacked VLAN ID for a main interface.

The **undo mpls l2vpn vlan-stacking** command deletes the stacked VLAN ID from a main interface.

By default, the system does not add a VLAN ID to a packet passing through the main interface.

Format

mpls l2vpn vlan-stacking stack-vlan *vlan-id*

undo mpls l2vpn vlan-stacking stack-vlan

Parameters

Parameter	Description	Value
stack-vlan *vlan-id*	Indicates the outer VLAN ID.	The value is an integer that ranges from 1 to 4094.

Views

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

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the following conditions are met, run the **mpls l2vpn vlan-stacking stack-vlan** command to specify a VLAN for a main interface:

- The VLL or VSI using VLAN encapsulation is configured on the two PEs.
- The remote PE accepts packets with one more VLAN tag.
- The local PE is connected to a computer by using a GE interface, XGE interface, 25GE interface, MultiGE interface, 40GE interface, 100GE interface, or Eth-Trunk interface as the AC interface.

In this scenario, the computer sends and receives all packets. After a VLAN is specified for the main interface, the local PE performs the following operations:

- The local PE adds VLAN tags to the packets sent by the computer. The VLAN tags are encapsulated in the user packets, and are transparently transmitted to the remote PE.
- The local PE removes the outer VLAN tags from the packets sent by the remote PE, and forwards the packets to the computer.

Precautions

Before binding the main interface to the VLL or VSI, run the **mpls l2vpn vlan-stacking stack-vlan** command to specify a VLAN for the main interface.

To use an XGE interface, a GE interface, a 25GE interface, a MultiGE interface, a 40GE interface, a 100GE interface, or an Eth-Trunk interface of the device as the AC interface of the PE, run the **undo portswitch** command to change a Layer 2 interface to a Layer 3 interface.

Example

# Configure MPLS VLL on the main interface and add VLAN tag 80 to incoming packets.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/13
[HUAWEI-GigabitEthernet0/0/13] undo portswitch
[HUAWEI-GigabitEthernet0/0/13] mpls l2vpn vlan-stacking stack-vlan 80
[HUAWEI-GigabitEthernet0/0/13] mpls l2vc 10.0.0.17 20 tagged
```

10.5.37 mpls l2vpn traffic-statistics enable

Function

The **mpls l2vpn traffic-statistics enable** command enables the system to collect VLL traffic statistics.

The **undo mpls l2vpn traffic-statistics enable** command disables the system from collecting VLL traffic statistics.

By default, the system is disabled from collecting VLL traffic statistics.

Format

mpls l2vpn traffic-statistics enable

undo mpls l2vpn traffic-statistics enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To collect traffic statistics in a VLL networking, use this command to the system to collect VLL traffic statistics.

Precautions

The system collects traffic statistics only for VLLs that are created after this command is executed.

You can view traffic statistics by running the **display traffic-statistics l2vpn interface** command.

Example

# Enable the function that collects L2VPN traffic statistics.

```
<HUAWEI>system-view
[HUAWEI] mpls l2vpn traffic-statistics enable
Info: The modification can only take effect for newly created VC.
```

10.5.38 mpls l2vpn trigger if-down

Function

The **mpls l2vpn trigger if-down** command enables the notification of physical layer faults.

The **undo mpls l2vpn trigger if-down** command disables the notification of physical layer faults.

By default, the notification of physical layer faults is disabled.

Format

mpls l2vpn trigger if-down

undo mpls l2vpn trigger if-down

Parameters

None

Views

25GE interface view, 40GE interface view,100GE interface view, GE interface view, MultiGE interface view, or XGE interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In a VLL FRR networking, an AC must detect failures of the corresponding PW to trigger link switching. This command enables the notification of physical layer faults so that ACs can detect failures of PWs.

Precautions

After the notification of physical layer faults is enabled:

- When a physical layer fault occurs on the PW side, the local AC interface is Down.
- When a physical layer fault occurs on the AC side, the local PE notifies the peer PE of the fault and the peer AC interface is Down.

After the fault is rectified, the Down AC interface automatically becomes Up.

Example

# Enable the notification of physical layer faults.

```
<HUAWEI> system-view
[HUAWEI] mpls l2vpn
[HUAWEI-l2vpn] quit
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] mpls l2vc 1.1.1.1 1
[HUAWEI-GigabitEthernet0/0/1] mpls l2vpn trigger if-down
```

10.5.39 mpls static-l2vc

Function

The **mpls static-l2vc** command creates a static VC.

The **undo mpls static-l2vc** command deletes the static VCs.

By default, no static VC is created.

Format

mpls static-l2vc { { **destination** *ip-address* | **pw-template** *pw-template-name vc-id* } * | **destination** *ip-address vc-id* } **transmit-vpn-label** *transmit-label-value* **receive-vpn-label** *receive-label-value* [**tunnel-policy** *tnl-policy-name* | [**control-word** | **no-control-word**] | [**raw** | **tagged**]] *

undo mpls static-l2vc

undo mpls static-l2vc { { **destination** *ip-address* | **pw-template** *pw-template-name vc-id* } * | **destination** *ip-address vc-id* } **transmit-vpn-label** *transmit-label-value* **receive-vpn-label** *receive-label-value* [**tunnel-policy** *tnl-policy-name* | [**control-word** | **no-control-word**] | [**raw** | **tagged**]] *

Parameters

Parameter	Description	Value
destination *ip-address*	Specifies the LSR ID of a peer device on the PW.	The value is in dotted decimal notation.
pw-template *pw-template-name*	Specifies the name of a static PW template.	The value is a string of 1 to 19 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
vc-id	Specifies the VC ID.	The value is an integer that ranges from 1 to 4294967295.
transmit-vpn-label *transmit-label-value*	Specifies the value of a transmit label.	The value is an integer that ranges from 0 to 1048575.
receive-vpn-label *receive-label-value*	Specifies the value of a receive label.	The value is an integer that ranges from 16 to 1023.
tunnel-policy *tnl-policy-name*	Specifies the name of a tunnel policy.	The value is a string of 1 to 39 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
control-word | **no-control-word**	Enables or disables the control word function. By default, the control word function is disabled.	-
raw	Removes the provider-tag (P-Tag) from a packet.	-
tagged	Retains the P-Tag in a packet.	-

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In an L2VPN networking, you can use this command to create a static VC between two PEs connected to CEs.

Precautions

- An interface cannot function as an L2VPN AC interface and L3VPN AC interface at the same time. After an interface is bound to an L2VPN, Layer 3 features such as the IP address and routing protocol on this interface become invalid.
- You can set attributes for a static PW template, including the remote peer, tunnel policy, control word, and VCCV. When configuring a static PW, you can directly use the static PW template without specifying attributes for the PW. After setting attributes for a static PW template, you can update the static PW template at any time. The modified static PW template takes effect only after the **reset pw** command is run.
- Static VCs must be created on PEs at both ends. The destination address of a VC is the LSR ID of the peer PE. The transmit label of the PE at one end is the receive label of the PE at the other end. If the labels do not match, traffic may fail to be forwarded even though the **static-l2vc** field is displayed as Up.
- If no tunnel policy is specified, the default tunnel policy is used. The default policy specifies that traffic is forwarded along the LSP and only one tunnel is used for load balancing. If a tunnel policy name is specified but the tunnel policy is not configured, the default tunnel policy is used.
- When configuring a static VC, note that the value of the transmit label ranges from 0 to 1048575. This ensures the communication between the device and different types of devices.
- When creating static VCs, the latest configurations of some parameters override the previous ones. The parameters include **tunnel-policy** *tnl-policy-name*, **control-word**, and **no-control-word**.
- By default, link type negotiation is enabled globally on the device. If a VLANIF interface is used as an AC-side interface for L2VPN, the configuration conflicts with link type negotiation. In this case, run the **lnp disable** command in the system view to disable link type negotiation.

NOTE

- If a sub-interface is bound to a VLL, the sub-interface can be deleted only after the sub-interface is unbound from the VLL.
- If a sub-interface is bound to a VLL, you cannot change the encapsulation type of the main interface.

Example

# Configure a static VC. Set the LSR ID of the peer device to 1.1.1.1, transmit label to 100, and receive label to 100.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 10
[HUAWEI-Vlanif10] mpls static-l2vc destination 1.1.1.1 transmit-vpn-label 100 receive-vpn-label 100
```

# Configure a static VC by applying a PW template and set values of the VC ID, transmit label, and receive label to 100 respectively.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 10
[HUAWEI-Vlanif10] mpls static-l2vc pw-template pwt 100 transmit-vpn-label 100 receive-vpn-label 100
```

# Delete a static VC.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 10
[HUAWEI-Vlanif10] undo mpls static-l2vc
```

10.5.40 mtu (MPLS-L2VPN instance view)

Function

The **mtu** command sets the Maximum Transmission Unit (MTU) of a L2VPN instance.

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

By default, the MTU of a L2VPN instance is 1500 bytes.

Format

mtu *mtu-value*

undo mtu

Parameters

Parameter	Description	Value
mtu-value	Specifies the MTU of a L2VPN instance.	The value is a decimal integer that ranges from 46 to 16352 bytes.

Views

MPLS-L2VPN instance view

Default Level

2: Configuration level

Usage Guidelines

The VPN MTU must be unique on the whole network.

If MTUs, which belong to the same VPN, on two PEs are different, the PEs cannot exchange VC information and set up connections.

After **vpn-target** is configured for the MPLS L2VPN instance, the MTU of the MPLS L2VPN cannot be changed.

In Kompella interworking with other venders' devices that do not support the MTU matching check, to ensure the VC keeps the Up state, you can perform the following configuration on the S300, S500, S2700, S5700, and S6700:

- Configuring an MTU the same as that of other venders' devices
- Using the **ignore-mtu-match** command for the system to ignore the MTU matching check

Example

# Set the MTU.

```
<HUAWEI> system-view
[HUAWEI] mpls l2vpn vpn1
[HUAWEI-mpls-l2vpn-vpn1] mtu 1000
```

10.5.41 ping vc

Function

The **ping vc** command detects the status of a PW.

Format

ping vc *pw-type pw-id* [*peer-address*] [**-c** *echo-number* | **-m** *time-value* | **-s** *data-bytes* | **-t** *timeout-value* | **-exp** *exp-value* | **-r** *reply-mode* | **-v**] * **control-word** [**remote** *remote-ip-address peer-pw-id* | **draft6**] * [**ttl** *ttl-value*] [**pipe** | **uniform**]

ping vc *pw-type pw-id* [*peer-address*] [**-c** *echo-number* | **-m** *time-value* | **-s** *data-bytes* | **-t** *timeout-value* | **-exp** *exp-value* | **-r** *reply-mode* | **-v**] * **control-word** **remote** *remote-ip-address peer-pw-id* **sender** *sender-address* [**ttl** *ttl-value*] [**pipe** | **uniform**]

ping vc *pw-type pw-id* [*peer-address*] [**-c** *echo-number* | **-m** *time-value* | **-s** *data-bytes* | **-t** *timeout-value* | **-exp** *exp-value* | **-r** *reply-mode* | **-v**] * **label-alert** [**no-control-word**] [**remote** *remote-ip-address* | **draft6**] * [**pipe** | **uniform**]

ping vc *pw-type pw-id* [*peer-address*] [**-c** *echo-number* | **-m** *time-value* | **-s** *data-bytes* | **-t** *timeout-value* | **-exp** *exp-value* | **-r** *reply-mode* | **-v**] * **normal** [**no-control-word**] [**remote** *remote-ip-address peer-pw-id*] [**ttl** *ttl-value*] [**pipe** | **uniform**]

Parameters

Parameter	Description	Value
pw-type	Specifies the encapsulation type of a local PW.	Currently, PWs of the following types are supported: **ethernet**, **ip-interworking**, and **vlan**.

Parameter	Description	Value
pw-id	Specifies the ID of a local PW.	The value is an integer that ranges from 1 to 4294967295.
peer-address	Specifies the peer LSR ID of a local PW. In PWE3 and Martini VLL scenarios, if the VC IDs of the primary and secondary VCs are the same, this parameter must be specified to uniquely identify a PW.	The value is in dotted decimal notation.
-c *echo-number*	Specifies the number of Echo Request messages to be sent. If the network works unstably, you can set this parameter to a larger value to test network quality based on the packet loss ratio.	The value is an integer that ranges from 1 to 4294967295. The default value is 5.
-m *time-value*	Specifies the interval for sending Echo Request messages. Each time after the source sends an Echo Request message by using the **ping vc** command, it waits a period of time (2000 ms by default) before sending the next Echo Request message. You can set the interval for sending Echo Request messages through the parameter *time-value*. If the network works unstably, the value should be greater than or equal to 2000 ms.	The value is an integer that ranges from 1 to 10000, in milliseconds. The default value is 2000.
-s *data-bytes*	Specifies the number of bytes of the sent Echo Request messages.	The value is an integer that ranges from 65 to 8100, in bytes. The default value is 100.
-t *timeout-value*	Specifies the timeout period for sending Echo Request messages.	The value is an integer that ranges from 0 to 65535, in milliseconds. The default value is 2000.

Parameter	Description	Value
-exp *exp-value*	Specifies the EXP value of the sent Echo Request messages. **NOTE** If DSCP priority has been configured by running the **set priority** command, the *exp-value* parameter does not take effect.	The value is an integer that ranges from 0 to 7. The default value is 0.
-r *reply-mode*	Specifies the mode in which the peer returns MPLS Echo Reply messages. ● 1: No MPLS Echo Reply message is returned. ● 2: MPLS Echo Reply messages are encapsulated into IPv4/IPv6 UDP packets. ● 3: MPLS Echo Reply messages are encapsulated into IPv4/IPv6 UDP packets carrying the Router Alert option. ● 4: MPLS Echo Reply messages are returned through the control channel of the application plane.	The value is an integer that ranges from 1 to 4. The default value is 2.
-v	Displays the detailed information.	-
no-control-word	Disables the control word function.	-
control-word	Enables the control word function. The switching node along a multi-segment PW does not transmit ping packets. When the control word function is enabled, you can ping only the termination node of the PW. Before using the control word to ping the PW, you must enable the control word for a PW.	-
remote	Specifies information about the PW on the remote PE. Information specified by the remote PE is finally encapsulated into the ping packets. The PW can be searched on the remote PE based on the specified information. By default, information contained in the ping packets is the information about the PW on the local end, which applies to single-segment PWs.	-

Parameter	Description	Value
peer-pw-id	Specifies the ID of the PW on the peer.	The value is an integer that ranges from 1 to 4294967295. By default, the peer PW ID is the same as the local PW ID.
draft6	Specifies the command version. If this parameter is specified, the ping operation is performed based on "draft-ietf-mpls-lsp-ping-06". By default, the ping operation is performed based on RFC 4379.	-
pipe	Specifies the pipe mode. When a probe packet passes through the MPLS domain, the entire MPLS domain is considered as one hop and the IP TTL of the probe packet is reduced by one on the ingress and egress respectively.	-
uniform	Specifies the uniform mode. The IP TTL of the probe packet is reduced by one each time it passes through one hop in the MPLS domain.	-
remote-ip-address	Specifies the remote IP address. By default, the system searches for the IP address of the next hop based on the PW on the local PE. In the case of a multi-segment PW, if the ping operation is performed in control word mode, the IP address of the termination node must be specified. In MPLS router alert mode, the IP address of any switching node or the termination node can be specified. Then, the Echo Request message is sent to the peer and then sent back.	-
label-alert	Specifies the label alert mode. The switching node along a multi-segment PW sends ping packets forcibly. In MPLS router alert mode, you can ping any switching node along the PW.	-

Parameter	Description	Value
normal	Specifies the normal mode, that is, the TTL detection mode. In this mode, control word and router alert are not encapsulated in to MPLS Echo Request messages, and TTL values are used to detect PW connectivity.	-
ttl *ttl-value*	Specifies the TTL value.	The value is an integer that ranges from 1 to 255. The default value is 64.
sender *sender-address*	Specifies a source address. For end-to-end detection of a multi-segment PW, a source IP address needs to be specified for a public network device that communicates with the remote PE. Generally, the source IP address is the address of the adjacent SPE or UPE.	-

Views

All views

Default Level

0: Visit level

Usage Guidelines

Usage Scenario

If a PW is Up, the **ping vc** command can be used to locate the fault on the PW. For example, a forwarding entry is abnormally lost or incorrect.

The **ping vc** command can be used to check a PW in the following scenarios:

VLL networking

Based on VLL types, the VLL PW ping can be classified into the following types:

- PWE3 VLL PW ping: In a PWE3 VLL networking, a PW ping is initiated to check the connectivity of a PW. A PWE3 VLL PW ping can be performed in control word mode, TTL mode, or label alert mode. In a ping test, a local PE sends an Echo Request message to the peer PE. After receiving the message, the peer PE abstracts and sends FEC information to the L2VPN module to determine whether the message has reached the egress. If so, the peer PE returns an Echo Reply message.
- Kompella VLL PW ping: A VLL PW ping is initiated to check the connectivity of a PW. Different from the PWE3 networking, the Kompella VLL does not need the PW template and supports the control word, TTL, and label alert modes.

VPLS networking

Based on the VPLS types, the VPLS PW ping can be classified into the following types:

- Martini VPLS PW ping: The Martini VPLS PW ping supports only the label alert mode. On a Hierarchical Virtual Private LAN Service (HVPLS) network, the Martini VPLS PW ping can only detect single-segment PWs. If an optional PW ID is configured and specified, the PW with the PW ID is detected. If the PW ID is not specified, the PW with a specified VSI ID is detected.
- Kompella VPLS PW ping: The Kompella VPLS PW ping supports only the label alert mode.

If a PW fault is detected by using the **ping vc** command, the **tracert vc** command can be used to locate the fault. Both the **ping vc** command and the **tracert vc** command can properly check the connectivity of PWs and locate faults.

Prerequisites

The MPLS module has been enabled on the device and works properly.

Precautions

control-word is recommended to detect the entire PW. Even though **label-alert** can be used to check the entire PW, the whole process is the same as the forwarding process only when **control-word** is used.

The execution of the **ping vc** command terminates when either of the following situations occurs:

- The ping packet reaches the egress.
- The TTL value of the ping packet reaches the upper threshold.

When a PE is single-homed to an SPE and two multi-segment PWs are deployed for PW redundancy, end-to-end detection cannot be performed for the secondary PW if services are transmitted over the primary PW. If services are transmitted over the secondary PW, the primary PW can only be detected segment by segment.

Example

# Run the **ping vc** command in label alert mode on the device to check the connectivity of an Ethernet PW.

```
<HUAWEI> ping vc ethernet 100 -c 10 -m 10 -s 65 -t 100 -v label-alert remote 2.2.2.2
  Reply from 2.2.2.2: bytes=65 Sequence=1 time = 31 ms Return Code 3, Subcode 1
  Reply from 2.2.2.2: bytes=65 Sequence=2 time = 15 ms Return Code 3, Subcode 1
  Reply from 2.2.2.2: bytes=65 Sequence=3 time = 32 ms Return Code 3, Subcode 1
  Reply from 2.2.2.2: bytes=65 Sequence=4 time = 15 ms Return Code 3, Subcode 1
  Reply from 2.2.2.2: bytes=65 Sequence=5 time = 32 ms Return Code 3, Subcode 1
  Reply from 2.2.2.2: bytes=65 Sequence=6 time = 15 ms Return Code 3, Subcode 1
  Reply from 2.2.2.2: bytes=65 Sequence=7 time = 15 ms Return Code 3, Subcode 1
  Reply from 2.2.2.2: bytes=65 Sequence=8 time = 16 ms Return Code 3, Subcode 1
  Reply from 2.2.2.2: bytes=65 Sequence=9 time = 15 ms Return Code 3, Subcode 1
  Reply from 2.2.2.2: bytes=65 Sequence=10 time = 32 ms Return Code 3, Subcode 1

--- FEC: FEC 128 PSEUDOWIRE (NEW). Type = ethernet, ID = 100 ping statistics
  10 packet(s) transmitted
  10 packet(s) received
  0.00% packet loss
  round-trip min/avg/max = 15/21/32 ms
```

10.5.42 ping vc vpn-instance

Function

The **ping vc vpn-instance** command detects the status of a PW and locates the faulty node when a PW goes Down.

Format

ping vc vpn-instance *vpn-name local-ce-id remote-ce-id* [**-c** *echo-number* | **-m** *time-value* | **-s** *data-bytes* | **-t** *timeout-value* | **-exp** *exp-value* | **-r** *reply-mode* | **-v**] * { **label-alert** [**no-control-word**] | **control-word** }

Parameters

Parameter	Description	Value
vpn-instance *vpn-name*	Specifies the VPN name.	The value is an existing VPN instance name.
local-ce-id	Specifies the ID of the local CE.	The value is a decimal integer ranging from 0 to 249.
remote-ce-id	Specifies the ID of the local CE.	The value is a decimal integer ranging from 0 to 249.
-c *echo-number*	Specifies the number of the sent Echo Request packets.	The value is a decimal integer that ranges from 1 to 4294967295. The default value is 5.
-m *time-value*	Indicates the interval for sending Echo Request packets.	The value is a decimal integer that ranges from 1 to 10000, in milliseconds. By default, the value is 2000.
-s *data-bytes*	Specifies the number of bytes of an Echo Request packet.	The value is a decimal integer ranging from 65 to 8100. By default, the value is 100.
-t *timeout-value*	Specifies the timeout period for sending Echo Request packets.	The value is a decimal integer ranging from 0 to 65535. By default, the value is 2000.
-exp *exp-value*	Specifies the EXP value in an outer label in an Echo Request packet.	The value is an integer ranging from 0 to 7.

Parameter	Description	Value
-r *reply-mode*	Specifies the mode of sending Echo Reply packets. The meaning of each value is as follows: ● 1: indicates no reply. ● 2: indicates a reply with an IPv4 or IPv6 UDP datagram. ● 3: indicates a reply with an IPv4 or IPv6 datagram carrying an MPLS router alert label. ● 4: indicates a reply through the control channel of the application plane.	The value is a decimal integer ranging from 1 to 4. By default, the value is 2.
-v	Displays detailed information.	-
label-alert	Indicates that in the case of a multi-hop PW, ping packets are forcibly sent on the transit node. In Label Alert mode, you can ping all transit nodes of a PW.	-
no-control-word	Disables the control word mode.	-
control-word	Indicates that in the case of a multi-hop PW, ping packets are forwarded without being resolved. In the control word mode, you can ping only the egress of the PW. The ping in control word mode can be performed only after the control word of a PW is enabled.	-

Views

All views

Default Level

0: Visit level

Usage Guidelines

If the control-word is enabled for a PW, it is recommended that you specify the **control-word** parameter to detect the connectivity of the PW. This ensures that ping packets are transmitted in the same manner as data packets on the PW.

Example

# Run the **ping vc vpn-instance** command in label-alert mode on the PE to detect the connectivity of the Kompella PW.

```
<HUAWEI> ping vc vpn-instance vpn1 1 2 -v label-alert
   Reply from 4.4.4.4: bytes=100 Sequence=1 time = 110 ms Return Code 3, Subcode 1
   Reply from 4.4.4.4: bytes=100 Sequence=2 time = 90 ms Return Code 3, Subcode 1
   Reply from 4.4.4.4: bytes=100 Sequence=3 time = 60 ms Return Code 3, Subcode 1
   Reply from 4.4.4.4: bytes=100 Sequence=4 time = 60 ms Return Code 3, Subcode 1
   Reply from 4.4.4.4: bytes=100 Sequence=5 time = 90 ms Return Code 3, Subcode 1

 --- FEC: L2 VPN ENDPOINT. Sender VEID = 1, Remote VEID = 2 ping statistics ---
   5 packet(s) transmitted
   5 packet(s) received
   0.00% packet loss
   round-trip min/avg/max = 60/82/110 ms
```

Table 10-73 Description of the ping vc vpn-instance command output

Item	Description
Reply from	IP address of the Echo Reply packet
bytes	Length of the Echo Reply packet
sequence	Sequence number of the Echo Reply packet
return code	Return code of the Echo Reply packet: ● 1: Malformed echo request received ● 2: One or more of the TLVs was not understood ● 3: Replying router is an egress for the FEC at stack-depth ● 4: Replying router has no mapping for the FEC at stack-depth ● 5: Downstream Mapping Mismatch ● 6: Upstream Interface Index Unknown ● 7: Reserved ● 8: Label switched at stack-depth ● 9: Label switched but no MPLS forwarding at stack-depth ● 10: Mapping for this FEC is not the given label at stack-depth ● 11: No label entry at stack-depth ● 12: Protocol not associated with interface at FEC stack-depth ● 13: Premature termination of ping due to label stack shrinking to a single label
Subcode	Subcode of the Echo Reply packet (indicating the depth of the label stack in the packet)
FEC	FEC TLV type (L2 VPN ENDPOINT indicates the Kompella PW that is negotiated by BGP)
Sender VEID	ID of the local CE
Remote VEID	ID of the remote CE

10.5.43 reset bgp l2vpn

Function

The **reset bgp l2vpn** command resets the TCP connection of the BGP L2VPN.

Format

reset bgp l2vpn { *as-number* | *peer-ip-address* | **all** | **internal** | **external** }

Parameters

Parameter	Description	Value
as-number	Indicates the number of the AS to which an L2VPN peer belongs.	-
peer-ip-address	Indicates the IP address of an L2VPN peer.	-
all	Resets all the L2VPN BGP connections.	-
internal	Resets the L2VPN BGP connection in the same AS.	-
external	Resets the L2VPN BGP connection across ASs.	-

Views

User view

Default Level

2: Configuration level

Usage Guidelines

After the parameters configured in the BGP-L2VPN address family view are modified, you can run the **reset bgp l2vpn** command to reset the TCP connection of the BGP L2VPN. After that, BGP re-negotiates parameters, re-sends label information, and re-establishes the session.

If the BGP L2VPN application and other applications share the same TCP connection, the **reset bgp l2vpn** command resets BGP neighbor relationship of all applications on this TCP connection.

Example

# Reset all the L2VPN BGP connections.

```
<HUAWEI> reset bgp l2vpn all
```

10.5.44 reset traffic-statistics l2vpn interface

Function

The **reset traffic-statistics l2vpn interface** command resets VLL traffic statistics on a specified interface.

Format

reset traffic-statistics l2vpn interface *interface-type interface-number*

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Specifies the type and number of a VLL AC interface. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number.	-

Views

User view

Default Level

2: Configuration level

Usage Guidelines

To collect new VLL traffic statistics in a VLL networking, run the **reset traffic-statistics l2vpn interface** command to reset the current VLL traffic statistics on the specified interface, and collect VLL traffic statistics again

Example

# Reset VLL traffic statistics on VLANIF10.

```
<HUAWEI> reset traffic-statistics l2vpn interface vlanif 10
```

10.5.45 route-distinguisher (MPLS-L2VPN instance view)

Function

The **route-distinguisher** command configures an RD for an MPLS L2VPN instance.

By default, no RD is configured in the MPLS L2VPN instance view.

Format

route-distinguisher *route-distinguisher*

Parameters

Parameter	Description	Value
route-distinguisher	Specifies the value of an RD. The formats of an RD are as follows: ● 16-bit AS number:32-bit user-defined number For example, 102:3. An AS number ranges from 0 to 65535. A user-defined number ranges from 0 to 4294967295. The AS number and the user-defined number cannot be 0s at the same time. That is, an RD cannot be 0:0. ● 32-bit IP address:16-bit user-defined number For example, 192.168.122.15:1. An IP address ranges from 0.0.0.0 to 255.255.255.255. A user-defined number ranges from 0 to 65535. ● Integral 4-byte AS number:2-byte user-defined number, for example, 65537:3. An AS number ranges from 65536 to 4294967295. A user-defined number ranges from 0 to 65535. The AS number and user-defined number cannot be both 0s. That is, an RD cannot be 0:0. ● 4-byte AS number in dotted notation:2-byte user-defined number, for example, 0.0:3 or 0.1:0. A 4-byte AS number in dotted notation is in the format of *x.y*, where *x* and *y* are integers that both range from 0 to 65535. A user-defined number ranges from 0 to 65535. The AS number and user-defined number cannot be both 0s. That is, an RD cannot be 0.0:0.	-

Views

MPLS-L2VPN instance view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In a Kompella VLL networking, an L2VPN instance takes effect only after an RD is configured.

Precautions

VPNs on the same PE have different RDs. The same VPN can have the same RD or different RDs on different PEs.

To change the RD of an L2VPN instance, delete the L2VPN instance and create a new L2VPN instance.

Kompella VLL and Kompella VPLS must use different RDs.

Example

# Set the RD of an MPLS L2VPN instance to 300:1.

```
<HUAWEI> system-view
[HUAWEI] mpls l2vpn vpn1 encapsulation vlan
[HUAWEI-mpls-l2vpn-vpn1] route-distinguisher 300:1
```

# Set the RD of an MPLS L2VPN instance to 1.1.1.1:5.

```
<HUAWEI> system-view
[HUAWEI] mpls l2vpn vpn2 encapsulation vlan
[HUAWEI-mpls-l2vpn-vpn2] route-distinguisher 1.1.1.1:5
```

# Set the RD of an MPLS L2VPN instance to 16.30:50.

```
<HUAWEI> system-view
[HUAWEI] mpls l2vpn vpn2 encapsulation vlan
[HUAWEI-mpls-l2vpn-vpn2] route-distinguisher 16.30:50
```

10.5.46 tracert vc

Function

The **tracert vc** command detects the status of a PW or locates a faulty node on a PW in Down state.

Format

tracert vc *pw-type pw-id* [*peer-address*] [**-exp** *exp-value* | **-f** *first-ttl* | **-m** *max-ttl* | **-r** *reply-mode* | **-t** *timeout-value*] * **control-word** [**draft6**] [**full-lsp-path**] [**pipe** | **uniform**]

tracert vc *pw-type pw-id* [*peer-address*] [**-exp** *exp-value* | **-f** *first-ttl* | **-m** *max-ttl* | **-r** *reply-mode* | **-t** *timeout-value*] * **control-word remote** *remote-ip-address* [**ptn-mode** | **full-lsp-path**] [**pipe** | **uniform**]

tracert vc *pw-type pw-id* [*peer-address*] [**-exp** *exp-value* | **-f** *first-ttl* | **-m** *max-ttl* | **-r** *reply-mode* | **-t** *timeout-value*] * **control-word remote** *remote-pw-id* **draft6** [**full-lsp-path**] [**pipe** | **uniform**]

tracert vc *pw-type pw-id* [*peer-address*] [**-exp** *exp-value* | **-f** *first-ttl* | **-m** *max-ttl* | **-r** *reply-mode* | **-t** *timeout-value*] * **label-alert** [**no-control-word**] [**remote** *remote-ip-address*] [**full-lsp-path**] [**draft6**] [**pipe** | **uniform**]

tracert vc *pw-type pw-id* [*peer-address*] [**-exp** *exp-value* | **-f** *first-ttl* | **-m** *max-ttl* | **-r** *reply-mode* | **-t** *timeout-value*] * **normal** [**no-control-word**] [**remote** *remote-ip-address*] [**full-lsp-path**] [**draft6**] [**pipe** | **uniform**]

Parameters

Parameter	Description	Value
pw-type	Specifies the PW type.	Currently, PWs of the following types are supported: **ethernet**, **vlan**, and **ip-interworking**.
pw-id	Specifies the local PW ID.	The value is an integer that ranges from 1 to 4294967295.
peer-address	Specifies a peer LSR ID for the local PW. In a PWE3 or Martini VLL scenario, if the primary and secondary VCs are configured with the same VC ID, this parameter must be specified to determine a unique PW to be monitored.	The value is in dotted decimal notation.
-exp *exp-value*	Specifies the EXP value in the outer label of an MPLS Echo Request packet. The default value is 0. **NOTE** If DSCP priority has been configured by running the **set priority** command, the *exp-value* parameter does not take effect.	The value is an integer that ranges from 0 to 7.
-f *first-ttl*	Specifies the initial Time-to-Live (TTL).	The value is an integer that ranges from 1 to 255, and must be smaller than the value of *max-ttl*. The default value is 1.
-m *max-ttl*	Specifies the maximum TTL.	The value is an integer that ranges from 1 to 255, and must be larger than the value of *first-ttl*. The default value is 30.

Parameter	Description	Value
-r *reply-mode*	Specifies the mode in which the peer returns MPLS Echo Reply packets. ● 1: No MPLS Echo Reply packet is returned. ● 2: The MPLS Echo Reply packet is encapsulated in IPv4/IPv6 UDP packets. ● 3: MPLS Echo Reply packets are encapsulated in IPv4/IPv6 /IPv6 UDP packets carrying the Router Alert option. ● 4: MPLS Echo Reply packets are returned through the control channel of the application plane.	The value is an integer that ranges from 1 to 4.
-t *timeout-value*	Specifies the timeout interval of an MPLS Echo Reply packet.	The value is an integer that ranges from 0 to 65535, in milliseconds. The default value is 5.
control-word	Indicates that the control word is encapsulated in the MPLS Echo Request packet.	-
label-alert	Indicates that the router alert label is encapsulated in the MPLS Echo Request packet.	-
no-control-word	Indicates that the control word is not encapsulated in the MPLS Echo Request packet.	-
normal	Indicates the normal mode where the router alert label and control word are not encapsulated in the MPLS Echo Request packet.	-
remote	Specifies information about the PW on the remote PE.	-

Parameter	Description	Value
remote-ip-address	Specifies the remote IP address. By default, the system searches for the IP address of the next hop based on the PW on the local PE. If **label-alert** is configured, you can specify the IP address of any switching node or the termination node.	-
remote-pw-id	Specifies the ID of the remote PW. By default, the ID of the local PW is used. If the tracert operation is performed in control word mode for a multi-segment PW, the IP address of the termination node must be specified.	-
ptn-mode	Specifies the PTN mode. In a multi-segment PW scenario, this parameter is indicated that trace VC packets are replied. You need to run the **lspv pw reply ptn-mode** command on both the SPE and TPE.	-
full-lsp-path	Displays the responses from all nodes along the LSP that the MPLS Echo Request packets pass through. If this parameter is not specified, only the responses from the PW nodes along the LSP are displayed.	-
pipe	Specifies the pipe mode. When a probe packet passes through the MPLS domain, the entire domain is regarded as one hop and the IP TTL of the probe packet is reduced by one on both the ingress and egress.	-
uniform	Specifies the uniform mode. The IP TTL of the probe packet is reduced by one each time it passes through one hop in the MPLS domain.	-

Parameter	Description	Value
draft6	Specifies the version of the **tracert vc** command. If this parameter is specified, the tracert operation is performed according to "draft-ietf-mpls-lsp-ping-06". By default, the tracert operation is performed according to RFC 4379. **NOTE** Tracert VC based on **draft6** is applied only to VLL over LDP scenarios.	-

Views

All views

Default Level

0: Visit level

Usage Guidelines

Usage Scenario

If a fault occurs on the PW, the **ping vc** command can be used to check the connectivity of the network, and the **tracert vc** command can be used to locate the fault and provide reference for fault diagnosis. If a PW is Up, the **ping vc** command can be used to locate the fault on the PW. For example, a forwarding entry is abnormally lost or incorrect. If a PW is down, the **tracert vc** command must be used to locate the faulty node on the PW.

The **tracert vc** command applies to the following networking scenarios:

- PWE3 VLL PW tracert

  In PWE3 VLL networking, PW tracert can help you obtain information about SPEs and Ps along the path that the message travels from the source to the destination, check the connectivity of the PW, and locate the fault of the PW.

  A PWE3 VLL PW tracert can be performed in control word mode, label alert mode, or TTL mode. The default mode is label alert. The TTL mode and control word mode are mutually exclusive.

  To detect faults on a VLL network with control word enabled, run the **tracert vc** *pw-type pw-id* **control-word** command.

  To encapsulate packets with the router alert label and detect faults on a VLL network, run the **tracert vc** *pw-type pw-id* **label-alert** command.

  If control word is not enabled and packets are not encapsulated with the router alert label, to detect faults on a VLL network, run the **tracert vc** *pw-type pw-id* command.

  The TTL value of the PW Tracert Request message is incremented by 1 each time. Each time the transit node (P) receives an Echo Request message after the TTL value of the message expires, it sends the Echo Request message to the LSPV module. Then the transit node returns an Echo Reply message carrying the next hop information.

Prerequisite

- The UDP module of each node works properly; otherwise, the tracert operation will fail.
- The MPLS module has been enabled on each node and works properly.
- The ICMP module of each node works properly; otherwise, " * * * " is displayed.

Procedure

The execution process of the **tracert vc** command is as follows:

1. The source sends an MPLS Echo Request packet with the TTL being 1. After the TTL times out, the first hop sends an MPLS Echo Reply packet to the source.
2. The source sends an MPLS Echo Request packet with the TTL being 2. After the TTL times out, the second hop sends an MPLS Echo Reply packet to the source.
3. The source sends an MPLS Echo Request packet with the TTL being 3. After the TTL times out, the third hop sends an MPLS Echo Reply packet to the source.
4. The preceding steps continue until the MPLS Echo Request packet reaches the destination.

When the device on each hop receives the MPLS Echo Request packet, it will respond with an MPLS Echo Reply packet, indicating that the tracert test ends. In the command output information of the source device, you can view the path that the packet passes through.

Configuration Impact

In control word mode, if a transit node receives an MPLS Echo Request packet whose TTL does not time out, it does not send the packet to the CPU. In this mode, the source obtains only a little PW information and cannot obtain information about the downstream devices of the transit node. This mode is recommended when the traffic volume is heavy.

In router alert mode, a transit node sends the received MPLS Echo Request packets to the CPU. In this mode, the source obtains a lot of PW information; therefore, device performance is affected when the traffic volume is heavy. This mode is recommended when the traffic volume is light.

Information specified by **remote** is encapsulated in MPLS Echo Request packets. The PW can be searched on the remote PE based on the specified information. By default, information contained in the MPLS Echo Request packets is about the PW on the local PE. This applies to single-segment PWs.

Precautions

- When the probe packet reaches the egress or the TTL reaches the upper threshold, the PW tracert is terminated.
- You can press **Ctrl + C** to terminate the execution of the **tracert vc** command.

When a PE is single-homed to an SPE and two multi-segment PWs are deployed for PW redundancy, end-to-end detection cannot be performed for the secondary PW if services are transmitted over the primary PW. If services are transmitted over the secondary PW, the primary PW can only be detected segment by segment.

Example

# Trace a multi-segment PW. The encapsulation type, local PW ID, and remote PW ID of the PW is ethernet, 100, and 200.

```
<HUAWEI> tracert vc ethernet 100 control-word remote 200 draft6 full-lsp-path
  TTL   Replier           Time    Type      Downstream
  0                                Ingress   10.1.1.2/[1025 ]
  1     10.1.1.2          230 ms  Transit   10.2.1.2/[3 ]
  2     10.2.1.2          230 ms  Transit   10.3.1.2/[3 ]
  3     10.3.1.2          100 ms  Transit   10.4.1.2/[3 ]
  4     10.4.1.2          150 ms  Egress
```

Table 10-74 Description of the **tracert vc** command output

Item	Description
TTL	TTL value in an Echo Request packet. It represents the number of hops along the path through which an Echo Request packet passes.
Replier	IP address of the node sending MPLS Echo Reply packets.
Time	Time when the packet is processed.
Type	Node type. The value can be: ● Ingress: indicates an ingress node. ● Transit: indicates a transit node. ● Egress: indicates an egress node.
Downstream	IP address and label of the downstream node.

10.5.47 tracert vc vpn-instance

Function

The **tracert vc vpn-instance** command detects the hop-by-hop connectivity of the LSP between PEs in the Kompella networking.

Format

tracert vc -vpn-instance *vpn-name local-ce-id remote-ce-id* [**-exp** *exp-value* | **-f** *first-ttl* | **-m** *max-ttl* | **-r** *reply-mode* | **-t** *timeout-value*] * { **control-word** | **label-alert** [**no-control-word**] | **draft6** } [**full-lsp-path**]

Parameters

Parameter	Description	Value
-vpn-instance *vpn-name*	Specifies the VPN instance name.	The value is an existing VPN instance name.
local-ce-id	Specifies the ID of the local CE.	It is a decimal integer ranging from 0 to 249.
remote-ce-id	Specifies the ID of the remote CE.	It is a decimal integer ranging from 0 to 249.
-exp *exp-value*	specifies value of the EXP field in an outer label in an Echo Request packet.	It is a decimal integer ranging from 0 to 7.
-f *first-ttl*	Specifies the value of the first TTL.	It is a decimal integer ranging from 1 to 255 and must be smaller than *max-ttl*. By default, the value is 1.
-m *max-ttl*	Specifies the value of the maximum TTL.	It is a decimal integer ranging from 1 to 255 and must be greater than the value of *first-ttl*. By default, the value is 30.
-r *reply-mode*	Specifies the mode in which the peer responds to the Echo Reply packet. The meaning of each value is as follows: ● 1: indicates no reply. ● 2: indicates a reply with an IPv4 or IPv6 UDP datagram. ● 3: indicates a reply with an IPv4 or IPv6 datagram carrying an MPLS router alert label. ● 4: indicates a reply through the control channel of the application plane.	It is a decimal integer ranging from 1 to 4.
-t *timeout-value*	Specifies the timeout period for waiting for MPLS Echo Reply packets.	The value is a decimal integer ranging from 0 ms to 65535 ms. By default, the value is 5.

Parameter	Description	Value
control-word	Indicates the control word encapsulated in packets.	-
label-alert	Indicates the router alert label encapsulated in packets.	-
no-control-word	Disables the control word mode.	-
draft6	Indicates the version of the command. If the parameter is specified, the command is implemented according to draft-ietf-mpls-lsp-ping-06. By default, the command is implemented according to RFC 4379.	-
full-lsp-path	Displays information about responses of all nodes along the LSP that an Echo Request packet passes. If this parameter is not specified, only the response of each PW node along the LSP is displayed.	-

Views

All views

Default Level

0: Visit level

Usage Guidelines

Usage Scenario

In a Kompella networking, if any node on the backbone network fails, use this command to identify the faulty node.

The **tracert vc vpn-instance** command applies to the following networking scenarios:

- Kompella VLL PW tracert

  In Kompella VLL networking, you can start a VLL PW tracert to check PW connectivity.

  A VLL PW tracert can help you obtain information about PEs and Ps along the path that the message travels from the source to the destination, check the connectivity of the Layer 2 forwarding link, and locate faults of the PW.

  Different from the PWE3 VLL PW tracert, the Kompella VLL tracert does not need the PW template and can be performed in control word mode or label alert mode. The default mode is label alert. Like PWE3 VLL PW tracert, Kompella VLL tracert can be enabled using a command.

Precautions

If the control word is encapsulated in MPLS echo request packets on a multi-hop PW, the packets on the switch node are not sent to the CPU for processing until the TTL times out. In control word mode, the source obtains less PW information, but the performance of the node is seldom affected and the source is unaware of the downstream information about this transit node. When there are a large number of packets, the control word mode is recommended.

After the router alert is encapsulated, in the case of a multi-hop PW, on the transit node, the Echo Request packet is sent to the CPU. In Label Alert mode, the source obtains more PW information. However, when a large number of packets are transmitted, the performance of the node degrades severely. The Label Alert mode is recommended when a small number of packets are transmitted on the network.

Example

# Perform the Tracert test on the VPN instance named vpn1 in label-alert mode.

```
<HUAWEI> tracert vc -vpn-instance vpn1 1 2 label-alert full-lsp-path
  TTL   Replier            Time    Type      Downstream
  0                             Ingress   20.1.1.1/[21505 1026 ]
  1     20.1.1.1          60 ms   Transit   30.1.1.1/[1026 ]
  2     30.1.1.1          50 ms   Transit   40.1.1.1/[3 ]
  3     4.4.4.4           70 ms   Egress
```

Table 10-75 Description of the **tracert vc vpn-instance** command output

Item	Description
TTL	TTL of MPLS Echo Request packets, indicating the number of hops along the tunnel that the packets pass.
Replier	Source IP address in an Echo Reply packet.
Time	How long a packet is processed
Type	Type of a node: ● Ingress ● Transit ● Egress
Downstream	Address and label of the downstream node

10.5.48 vpn-target (MPLS-L2VPN instance view)

Function

The **vpn-target** command specifies VPN targets for an L2VPN.

The **undo vpn-target** command deletes the VPN targets specified for an L2VPN.

By default, no VPN target is specified for an L2VPN.

Format

vpn-target *vpn-target* &<1-16> [**both** | **export-extcommunity** | **import-extcommunity**]

undo vpn-target { **all** | *vpn-target* &<1-16> [**both** | **export-extcommunity** | **import-extcommunity**] }

Parameters

Parameter	Description	Value
vpn-target	Adds a VPN target to the VPN. A VPN target can use any of the following formats: ● 16-bit AS number:32-bit user-defined number For example, 1:3. An AS number ranges from 0 to 65535. A user-defined number ranges from 0 to 4294967295. The AS number and the user-defined number cannot be 0s at the same time. That is, a VPN target cannot be 0:0. ● 32-bit IP address:16-bit user-defined number For example, 192.168.122.15:1. An IP address ranges from 0.0.0.0 to 255.255.255.255. A user-defined number ranges from 0 to 65535. ● Integral 4-byte AS number:2-byte user-defined number, for example, 65537:3. An AS number ranges from 65536 to 4294967295. A user-defined number ranges from 0 to 65535. The AS number and user-defined number cannot be both 0s. That is, a VPN target cannot be 0:0. ● 4-byte AS number in dotted notation:2-byte user-defined number, for example, 0.0:3 or 0.1:0. A 4-byte AS number in dotted notation is in the format of *x.y*, where *x* and *y* are integers that range from 0 to 65535. A user-defined number ranges from 0 to 65535. The AS number and user-defined number cannot be both 0s. That is, a VPN target cannot be 0.0:0.	-
import-extcommunity	Receives routing information carrying specified extended community attributes.	-
export-extcommunity	Specifies the extended community attributes carried in routing information to be sent.	-

Parameter	Description	Value
both	Specifies the extended community attributes of the received and the sent routing information.	-
all	Deletes all the VTs.	-

Views

MPLS-L2VPN instance view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In a Kompella VLL networking, you can use this command to set the VPN target attribute for an L2VPN instance. The VPN target is used to set up a remote PW.

Precautions

If you do not specify any keywords, **both** is used by default.

Before configuring a VPN target, configure the Route Distinguisher (RD) for the L2VPN instance.

Example

# Configure the VTs for an L2VPN named vpn1.

```
<HUAWEI> system-view
[HUAWEI] mpls l2vpn vpn1 encapsulation vlan
[HUAWEI-mpls-l2vpn-vpn1] vpn-target 100:1
[HUAWEI-mpls-l2vpn-vpn1] vpn-target 1:1 2:2 export-extcommunity
[HUAWEI-mpls-l2vpn-vpn1] vpn-target 1.2.3.4:11 12:12 import-extcommunity
```

# Delete the VT of vpn1.

```
<HUAWEI> system-view
[HUAWEI] mpls l2vpn vpn1 encapsulation vlan
[HUAWEI-mpls-l2vpn-vpn1] undo vpn-target 12:12 import-extcommunity
```

# Delete all the VTs of vpn1.

```
<HUAWEI> system-view
[HUAWEI] mpls l2vpn vpn1 encapsulation vlan
[HUAWEI-mpls-l2vpn-vpn1] undo vpn-target all
```

10.6 PWE3 Configuration Commands

10.6.1 Command Support

Only the following switch models support PWE3:

S5731-S, S5731-H, S5731S-H, S5732-H, S6720-EI, S6720S-EI, S6730-S, S6730S-H, and S6730-H

10.6.2 bfd bind pw

Function

The **bfd bind pw** command configures a BFD session to detect a PW.

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

By default, no BFD session is configured to detect a PW.

Format

bfd *cfg-name* **bind pw interface** *interface-type interface-number* [**secondary**]

undo bfd *cfg-name*

Parameters

Parameter	Description	Value
cfg-name	Specifies the name of the BFD session.	The value is a string of 1 to 15 case-insensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
interface *interface-type interface-number*	Specifies the type and number of the interface where the PW to be detected resides, namely, the AC interface. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number.	-
secondary	Indicates that the BFD session detects the secondary PW.	-

Views

System 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 detection mechanism on an interface. On networks demanding fast fault detection, run the **bfd bind pw** command to configure a BFD session to detect a PW.

Prerequisites

- A PW has been configured on an AC interface by running the **mpls l2vc** command.
- BFD has been enabled globally by running the **bfd** command.
- A single-segment or multi-segment PW has been configured.

Precautions

- When detecting a PW, BFD sessions must be bound to the source and destination ends of a PW.
- You need to create a BFD session to detect primary and secondary PWs separately.

NOTE

When running the **bfd bind pw** command to detect a multi-segment PW, ensure that the first-segment PW is a VLL PW configured on a non-SPE node.

When running the **bfd bind pw** command to detect a single-segment PW, ensure that the single-segment PW is configured on a non-SPE node.

Example

# Create a BFD session to detect a PW.

```
<HUAWEI> system-view
[HUAWEI] bfd pe2 bind pw interface vlanif 10
```

10.6.3 bfd-detect

Function

The **bfd-detect** command enables dynamic BFD for PW in a PW template and adjusts the sending interval, receiving interval, and local detection multiplier of BFD detection packet.

The **undo bfd-detect** command restores the default configuration.

By default, dynamic BFD for PW is not enabled in a PW template.

Format

bfd-detect [**min-tx-interval** *tx-interval* | **min-rx-interval** *rx-interval* | **detect-multiplier** *multiplier*] *

undo bfd-detect

Parameters

Parameter	Description	Value
min-tx-interval *tx-interval*	Specifies the interval at which BFD packets are sent.	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-S, S5731-H and S5731S-H, the value ranges from 3 to 1000. - After the **set service-mode enhanced-bfd** command is configured on the S5732-H, S6730-S, S6730-H, and S6730S-H, the value ranges from 3 to 1000.
min-rx-interval *rx-interval*	Specifies the interval at which BFD packets are received.	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-S, S5731-H and S5731S-H, the value ranges from 3 to 1000. - After the **set service-mode enhanced-bfd** command is configured on the S5732-H, S6730-S, S6730-H, and S6730S-H, the value ranges from 3 to 1000.
detect-multiplier *multiplier*	Specifies the local detection multiplier value of a BFD session.	An integer ranging from 3 to 50. The value is 3 by default.

Views

PW template view

Default Level

2: Configuration level

Usage Guidelines

If the BFD session is found to be Down, the system automatically adjusts the receiving interval and sending interval of the local end to a random value ranging from 1000 ms to 3000 ms to reduce system resource utilization. When the BFD session restores the Up state, the user-defined interval is used again.

Example

# Enable dynamic BFD detection, and set *min-tx-interval*, *min-rx-interval*, and *multiplier* to 100 ms, 100 ms, and 4 respectively in the PW template.

```
<HUAWEI> system-view
[HUAWEI] pw-template pwt
[HUAWEI-pw-template-pwt] bfd-detect min-rx-interval 100 min-tx-interval 100 detect-multiplier 4
```

10.6.4 bfd for pw enable

Function

The **bfd for pw enable** command enables the device to send BFD for PW packets to the protocol stack.

The **undo bfd for pw enable** command disables the device from sending BFD for PW packets to the protocol stack.

By default, the device does not send BFD for PW packets to the protocol stack, but discards or forwards the packets.

Format

bfd for pw enable

undo bfd for pw enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To configure a BFD session to detect a PW on a network requiring short link detection, run the **bfd for pw enable** command to enable the device to send BFD for PW packets to the protocol stack. If this command is not used, the device discards or forwards BFD for PW packets.

Precautions

The **bfd for pw enable** command must have been executed to configure a BFD session to detect a PW. If this command is not used, the **bfd for pw enable** command does not take effect.

Example

# Enable the device to send BFD for PW packets to the protocol stack.

```
<HUAWEI> system-view
[HUAWEI] bfd for pw enable
```

10.6.5 control-word

Function

The **control-word** command enables the control word in a PW template.

The **undo control-word** command disables the control word in a PW template.

By default, the control word is disabled in a PW template.

Format

control-word

undo control-word

Parameters

None

Views

PW template view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In the case of load balancing, packets received by a device may be out of order. With the control word function, the device can reassemble the packets.

PW templates simplify the configuration of PWs with similar attributes. The control word attribute can be set using commands or a PW template. If the control word is configured using both commands and a PW template, only the control word configured using commands takes effect.

Prerequisites

- MPLS L2VPN has been enabled.
- A PW template has been created.

Configuration Impact

After a PW is established using a PW template where the control word function is enabled, the control word enabling status on both ends of the PW may be different after the PW template is restarted. As a result, system performance may be affected.

Follow-up Procedure

When configuring MPLS L2VPN on an interface, use a configured PW template.

Precautions

After the control word attribute is changed in a PW template:

- If the PW is in use, you do not need to reset the PW.
- If the PW template is being referenced by PWs, the configuration takes effect only after you run the **reset pw** command. Running the **reset pw** command may cause the disconnection and re-connection of related PWs. If multiple PWs use this template at the same time, the system operation is affected.

Example

# Enable the control word in the PW template named **pwt**.

```
<HUAWEI> system-view
[HUAWEI] pw-template pwt
[HUAWEI-pw-template-pwt] control-word
```

# Disable the control word in the PW template named **pwt**.

```
<HUAWEI> system-view
[HUAWEI] pw-template pwt
[HUAWEI-pw-template-pwt] undo control-word
```

10.6.6 display mpls l2vc

Function

The **display mpls l2vc** command displays information about virtual circuits (VCs) in LDP mode.

Format

display mpls l2vc [*vc-id* | **interface** *interface-type interface-number* | **remote-info** [*vc-id* | **verbose**] | **state** { **down** | **up** }]

Parameters

Parameter	Description	Value
interface *interface-type* *interface-number*	Specifies the type and number of the AC interface connected to the CE. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number.	-
remote-info	Displays information about the VC on the remote end.	-
vc-id	Displays static PW information with a specified VC ID.	The value is an integer that ranges from 1 to 4294967295.
verbose	Displays the detailed information about the VC on the remote end.	-
state { **down** | **up** }	Displays VC information based on the VC status. ● **down**: Displays information about the VC in Down state. ● **up**: Displays information about the VC in Up state.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The **display mpls l2vc** command displays information about the VCs in LDP signaling mode, including the Martini VC and PWE3 VC.

- If the interface is specified, information about VCs on the specified AC interface is displayed.
- If **remote-info** is specified but *vc-id* is not specified, information about all VCs set up by the remote and local peers is displayed.

Example

# Display information about all the LDP VCs configured on the switch.

```
<HUAWEI> display mpls l2vc
 Total LDP VC : 1     1 up       0 down
```

```
*client interface       : Vlanif1111 is up
  Administrator PW       : no
  session state          : up
  AC status              : up
  Ignore AC state        : disable
  VC state               : up
  Label state            : 0
  Token state            : 0
  VC ID                  : 101
  VC type                : VLAN
  destination            : 10.3.3.9
  local VC label         : 1026         remote VC label      : 1026
  control word           : disable
  remote control word    : disable
  forwarding entry       : exist
  local group ID         : 0
  remote group ID        : 0
  local AC OAM State     : up
  local PSN OAM State    : up
  local forwarding state : forwarding
  local status code      : 0x0
  remote AC OAM state    : up
  remote PSN OAM state   : up
  remote forwarding state: forwarding
  remote status code     : 0x0
  ignore standby state   : no
  BFD for PW             : unavailable
  VCCV State             : up
  manual fault           : not set
  active state           : active
  link state             : up
  local VC MTU           : 1500         remote VC MTU        : 1500
  local VCCV             : alert ttl lsp-ping bfd
  remote VCCV            : alert ttl lsp-ping bfd
  tunnel policy name     : --
  PW template name       : --
  primary or secondary   : primary
  load balance type      : flow
  Access-port            : false
  Switchover Flag        : false
  VC tunnel/token info   : 1 tunnels/tokens
    NO.0  TNL type       : lsp   , TNL ID : 0x48000020
    Backup TNL type      : lsp   , TNL ID : 0x0
  create time            : 0 days, 0 hours, 6 minutes, 50 seconds
  up time                : 0 days, 0 hours, 6 minutes, 34 seconds
  last change time       : 0 days, 0 hours, 6 minutes, 34 seconds
  VC last up time        : 2013/09/24 18:23:35
  VC total up time       : 0 days, 0 hours, 6 minutes, 34 seconds
  CKey                   : 16
  NKey                   : 15
  PW redundancy mode     : frr
  AdminPw interface      : --
  AdminPw link state     : --
  Diffserv Mode          : uniform
  Service Class          : be
  Color                  : --
  DomainId               : --
  Domain Name            : --
```

Table 10-76 Description of the **display mpls l2vc** command output

Item	Description
Total LDP VC	Total number of established LDP VCs, including the number of LDP VCs in Up and Down state.
client interface	AC interface and its status.

Item	Description
Administrator PW	Whether the PW is an mPW. The PW can be an mPW only when the AC interface is a loopback interface. This field can be displayed as **yes** or **no**.
session state	Status of the LDP session established between both ends of the VC: ● up: The LDP session has been established. ● down: The LDP session is not established.
AC status	Status of the AC: ● up: An AC has been established. ● down: An AC is not established.
Ignore AC state	Whether the AC status change affects the status of services on the active or standby PWE3. ● enable: The impact of the AC status change on the status of services on the active or standby PWE3 is ignored. ● disable: The AC status change affects the status of services on the active or standby PWE3.
VC state	Status of the VC: ● up: A VC has been established. ● down: A VC is not established.
Label state	Label status: ● 0: The label can be used. ● 1: Wait for the SMB to confirm the label status. ● 2: The label is released. ● 3: SMB confirmation failed.
Token state	Token status: ● 0: The token can be used. ● 1: Wait for the SMB to confirm the token status. ● 2: The token is released. ● 3: SMB confirmation failed.
VC ID	ID of the VC, which uniquely identifies a VC. **NOTE** If the VC IDs on both ends are different, run the **mpls l2vc** command in the interface view to change the VC ID on one end to be the same as that on the other end.

Item	Description
VC type	Encapsulation type of the VC: ● VLAN ● Ethernet The PW can go Up only when the local and remote encapsulation types are the same.
destination	LSR ID of the VC peer device.
local VC label	Local VC label.
remote VC label	Remote VC label.
control word	Whether the control word is enabled: ● enable: The control word is enabled. ● disable: The control word is disabled.
forwarding entry	Whether forwarding entries exist.
local group ID	Local group ID.
remote group ID	Remote group ID.
manual fault	Whether a PW fault is simulated.
active state	Whether the PW is in active state. A PW in active state can forward packets.
link state	Integrative PW status: ● up ● down If any of the following status is Down, the PW link state is Down: ● Service PW status ● Status of the mPW associated with service PWs ● Status of the BFD session associated with service PWs ● PW state code ● PW status detected by VCCV ● OAM status
local VC MTU	MTU of the local VC.
remote VC MTU	MTU of the remote VC.
tunnel policy name	Name of the tunnel policy.
PW template name	Name of the PW template.
primary or secondary	Whether the VC is a primary VC or a secondary VC.

Item	Description
load balance type	Load balancing mode of Martini VLL: ● flow: indicates flow-based load balancing. ● packet: indicates packet-based load balancing.
Access-port	Whether the interface supports the access-port attribute: ● true: indicates that the interface supports the access-port attribute. ● false: indicates that the interface does not support the access-port attribute.
Switchover Flag	Whether a switchover has occurred.
create time	How long the VC has been created.
up time	How long the VC keeps the Up state. If the current PW status is Down, the value is 0.
last change time	How long the VC status remains unchanged.
VC last up time	Last time when the VC became Up.
VC total up time	Total duration of the VC in Up state.
CKey	Index of the public tunnel for VPN QoS.
NKey	Index of the public tunnel.
AdminPw interface	AC interface on which the mPW is bound to the PW. The AC interface must be a loopback interface. This field is displayed only when the PW is not an mPW: ● Name of the loopback interface. ● --: indicates that the PW is not bound to an mPW.
AdminPw link state	Status of the mPW bound to the PW. This field is displayed only when the PW is not an mPW. This field can be displayed as: ● Up ● Down ● --: indicates that the PW is not bound to an mPW.
Diffserv Mode	QoS DiffServ mode.
Service Class	QoS service class.
Color	QoS color.
DomainId	ID of a domain.

Item	Description
Domain Name	Name of a domain.

# Display LDP VC information about the AC interface VLANIF 100.

```
<HUAWEI> display mpls l2vc interface vlanif 100
 *client interface       : Vlanif100  is up
  Administrator PW       : no
  session state          : up
  AC status              : up
  Ignore AC state        : disable
  VC state               : up
  Label state            : 0
  Token state            : 0
  VC ID                  : 1
  VC type                : VLAN
  destination            : 10.2.2.2
  local group ID         : 0            remote group ID      : 0
  local VC label         : 16400        remote VC label      : 16400
  local AC OAM State     : up
  local PSN OAM State    : up
  local forwarding state : forwarding
  local status code      : 0x0
  remote AC OAM state    : up
  remote PSN OAM state   : up
  remote forwarding state: forwarding
  remote status code     : 0x20
  ignore standby state   : no
  BFD for PW             : unavailable
  VCCV State             : up
  manual fault           : not set
  active state           : active
  forwarding entry       : exist
  link state             : up
  local VC MTU           : 1500         remote VC MTU        : 1500
  local VCCV             : cw alert ttl lsp-ping bfd
  remote VCCV            : cw alert ttl lsp-ping bfd
  local control word     : enable       remote control word  : enable
  tunnel policy name     : --
  PW template name       : --
  primary or secondary   : primary
  load balance type      : flow
  Access-port            : false
  Switchover Flag        : false
  VC tunnel/token info   : 1 tunnels/tokens
    NO.0  TNL type       : lsp   , TNL ID : 0x800802
    Backup TNL type      : lsp   , TNL ID : 0x0
  create time            : 0 days, 0 hours, 0 minutes, 29 seconds
  up time                : 0 days, 0 hours, 0 minutes, 6 seconds
  last change time       : 0 days, 0 hours, 0 minutes, 6 seconds
  VC last up time        : 2011/07/04 20:25:50
  VC total up time       : 0 days, 0 hours, 0 minutes, 6 seconds
  CKey                   : 2
  NKey                   : 1
  PW redundancy mode     : frr
  AdminPw interface      : --
  AdminPw link state     : --
  Diffserv Mode          : uniform
  Service Class          : --
  Color                  : --
  DomainId               : --
  Domain Name            : --
```

Table 10-77 Description of the **display mpls l2vc interface** command output

Item	Description
local AC OAM State	OAM status of the local AC. ● up ● down
local PSN OAM State	Status of the local device on the Packet Switch Network (PSN) side. ● up ● down
local forwarding state	Status of the local forwarding table. ● forwarding ● down
local status code	Status code of the local PW: ● 0x0: indicates that the local PW functions as the master PW and is in Up state. ● 0x20: indicates that the local PW functions as the backup PW and is in Up state. ● 0x1: indicates that the local PW functions as the master PW and is in Down state. ● 0x21: indicates that the local PW functions as the backup PW and is in Down state.
remote AC OAM state	OAM status of the remote AC. ● up ● down
remote PSN OAM state	Status of the remote device on the PSN side. ● up ● down
remote forwarding state	Status of the remote forwarding table. ● forwarding ● down
remote status code	Status code of the remote PW: ● 0x0: indicates that the remote PW functions as the master PW and is in Up state. ● 0x20: indicates that the remote PW functions as the backup PW and is in Up state. ● 0x1: indicates that the remote PW function as the master PW and is in Down state. ● 0x21: indicates that the remote PW function as the backup PW and is in Down state.

Item	Description
BFD for PW	Whether BFD for PW is enabled: ● available ● unavailable
VCCV State	Whether Virtual Circuit Connectivity Verification (VCCV) is enabled.
local VCCV	Type of VCCV supported on the local device. ● By default, the VCCV type is **alert ttl lsp-ping bfd**, indicating that the control word function is disabled and LSP ping and BFD are supported for the alert channel. ● If the control word function is enabled, the VCCV type is **cw alert ttl lsp-ping bfd**, indicating that LSP ping and BFD are supported for both the control word channel and the alert channel.
remote VCCV	Type of VCCV supported on the remote device. ● By default, the VCCV type is **alert ttl lsp-ping bfd**, indicating that the control word function is disabled and LSP ping and BFD are supported for the alert channel. ● If the control word function is enabled, the VCCV type is **cw alert ttl lsp-ping bfd**, indicating that LSP ping and BFD are supported for both the control word channel and the alert channel.
local control word	Whether the control word is enabled on the local device: ● Disable ● Enable
remote control word	Whether the control word is enabled on the remote device: ● Disable ● Enable
ignore standby state	Whether the status of the secondary PW is ignored.
VC Tunnel/token info: 1 tunnels/tokens	Information about the tunnel or token used by the VC. The value **1 tunnels/tokens** indicates that the PW uses one tunnel or token.
TNL type	Type of the tunnel used by the PW.
TNL ID	ID of the tunnel used by the PW.

Item	Description
Backup TNL Type	Type of the backup tunnel when PW over LDP FRR is used.
PW redundancy mode	PW redundancy mode. By default, the mode is FRR. ● Independent: indicates that the PW is in negotiation mode. ● frr: indicates that the PW is in FRR mode. ● --: indicates that the PW is in master/slave mode.

# Display the LDP VC information received from the remote peer.

```
<HUAWEI> display mpls l2vc remote-info
Total remote ldp vc : 1

Transport  Group      Peer           Remote        Remote     C   MTU/  N   S
VC ID      ID         Addr           Encap         VC Label   Bit CELLS Bit Bit

101        0          10.3.3.9       ethernet      1024       0   1500  0   0
```

# Display the detailed LDP VC information received from the remote peer.

```
<HUAWEI> display mpls l2vc remote-info verbose
Total remote LDP VC : 1

VC ID              : 1
VC Type            : vlan
VC Label           : 1025
Peer Address       : 10.5.5.5
Group ID           : 0
MTU                : 1500
Control Word       : 0
Notification       : 1
Status Code        : 0
Match Local VC     : MATCH
Max ATM CELLS      : --
TDM RTP Header     : --
TDM Encap Num      : --
TDM Bit Rate       : --
```

Table 10-78 Description of the **display mpls l2vc remote-info** command output

Item	Description
Total remote ldp vc	Total number of created remote LDP VCs.
Transport VC ID	VC ID, which uniquely identifies a VC.
Group ID	ID of the group to which the L2VPN belongs. The default value is 0.
Peer Addr and Peer Address	IP address of the remote peer.

Item	Description
Remote Encap	Encapsulation type of the remote VC. ● vlan ● ethernet
Remote VC Label	Remote VC label.
C Bit	Whether the control word is enabled: ● 1: indicates that the control word is enabled. ● 0: indicates that the control word is disabled.
MTU/CELLS	MTU of the L2VPN.
N Bit and Notification	Whether the Notification message is supported: ● 1: indicates the message is supported. ● 0: indicates the message is not supported.
S Bit and Status Code	Status code: ● 0: indicates the forwarding state. ● 1: indicates the non-forwarding state. ● 32: indicates the backup state.
Match Local VC	Whether the local VC ID matches the remote VC ID: ● MATCH ● NOT-MATCH
Max ATM CELLS	Maximum number of ATM cells that can be transmitted. If ATM encapsulation is used, the value ranges from 1 to 28, and the default value is 28. If non-ATM encapsulation is used, double hyphens (--) are displayed.
TDM RTP Header	Whether the RTP-header option is enabled: ● enable: The RTP header is added to TDM packets to be transparently transmitted. ● disable: The RTP header is not added to TDM packets to be transparently transmitted. This is the default value. ● --: Non-TDM encapsulation is used.
TDM Encap Num	Number of frames in a TDM packet. If TDM encapsulation is used, the value is 8, 16, 24, 32 or 40, and the default value is 32. If non-TDM encapsulation is used, double hyphens (--) are displayed.

Item	Description
TDM Bit Rate	Number of timeslots in a TDM packet. Number of timeslots in a TDM packet = Number of bytes in a TDM packet/Number of frames in a TDM packet

# Display information about the VCs in Up state.

```
<HUAWEI> display mpls l2vc state up
 Total LDP VC : 1     1 up       0 down

 *client interface       : Vlanif1111 is up
  Administrator PW       : no
  session state          : up
  AC status              : up
  Ignore AC state        : disable
  VC state               : up
  Label state            : 0
  Token state            : 0
  VC ID                  : 100
  VC type                : VLAN
  destination            : 10.2.2.9
  local VC label         : 1024         remote VC label      : 1024
  control word           : disable
  remote control word    : disable
  forwarding entry       : exist
  local group ID         : 0
  remote group ID        : 0
  local AC OAM State     : up
  local PSN OAM State    : up
  local forwarding state : forwarding
  local status code      : 0x0
  remote AC OAM state    : up
  remote PSN OAM state   : up
  remote forwarding state: forwarding
  remote status code     : 0x0
  ignore standby state   : no
  BFD for PW             : unavailable
  VCCV State             : up
  manual fault           : not set
  active state           : active
  link state             : up
  local VC MTU           : 1500         remote VC MTU        : 1500
  local VCCV             : alert ttl lsp-ping bfd
  remote VCCV            : alert ttl lsp-ping bfd
  tunnel policy name     : --
  PW template name       : --
  primary or secondary   : primary
  load balance type      : flow
  Access-port            : false
  Switchover Flag        : false
  VC tunnel/token info   : 1 tunnels/tokens
    NO.0  TNL type       : lsp   , TNL ID : 0x12
    Backup TNL type      : lsp   , TNL ID : 0x0
  create time            : 0 days, 1 hours, 0 minutes, 17 seconds
  up time                : 0 days, 0 hours, 24 minutes, 56 seconds
  last change time       : 0 days, 0 hours, 24 minutes, 56 seconds
  VC last up time        : 2013/10/10 14:29:39
  VC total up time       : 0 days, 0 hours, 24 minutes, 56 seconds
  CKey                   : 10
  NKey                   : 9
  PW redundancy mode     : frr
  AdminPw interface      : --
  AdminPw link state     : --
  Diffserv Mode          : uniform
  Service Class          : --
  Color                  : --
  DomainId               : --
  Domain Name            : --
```

10.6.7 display mpls l2vc brief

Function

The **display mpls l2vc brief** command displays brief information about LDP Layer 2 virtual circuits (L2VCs) on the device.

Format

display mpls l2vc brief

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The **display mpls l2vc brief** command is recommended when many L2VCs are configured on a device. The command output is more concise than that of the **display mpls l2vc** command.

Example

# Display brief information about all LDP L2VCs on the device.

```
<HUAWEI> display mpls l2vc brief
 Total LDP VC : 1     1 up       0 down

 *Client Interface     : Vlanif1111
  Administrator PW     : no
  AC status            : up
  Ignore AC state      : disable
  VC state             : up
  Label state          : 0
  Token state          : 0
  VC ID                : 116119
  VC Type              : VLAN
  session state        : up
  Destination          : 10.6.6.6
  link state           : up
```

Table 10-79 Description of the **display mpls l2vc brief** command output

Item	Description
Total LDP VC	Total number of LDP VCs, including the number of LDP VCs in Up and Down state.
Client Interface	AC interface and its status.
Administrator PW	Whether the PW is an mPW. The PW can be an mPW only when the AC interface is a loopback interface.
AC status	Status of the AC: ● up ● down
Ignore AC state	Whether the AC status change affects the status of services on the active or standby PWE3. ● enable: The impact of the AC status change on the status of services on the active or standby PWE3 is ignored. ● disable: The AC status change affects the status of services on the active or standby PWE3.
VC state	Status of the VC: ● up ● down
Label state	Label status: ● 0: The label can be used. ● 1: Wait for the SMB to confirm the label status. ● 2: The label is released. ● 3: SMB confirming failed.
Token state	Token status: ● 0: The label can be used. ● 1: Wait for the SMB to confirm the label status. ● 2: The label is released. ● 3: SMB confirming failed.
VC ID	ID of the VC, which uniquely identifies a VC.
VC Type	Encapsulation type of the VC.
session state	Status of the session between peers: ● up ● down
Destination	Peer address.

Item	Description
link state	Status of the VC: ● up ● down

10.6.8 display mpls l2vc track admin-vc

Function

The **display mpls l2vc track admin-vc** command displays information about service PWs or switching PWs that are associated with an mPW.

Format

display mpls l2vc track admin-vc interface loopback *interface-number* [**upe**]

Parameters

Parameter	Description	Value
interface loopback *interface-number*	Specifies the loopback interface on which the mPW is configured.	-
upe	Displays information about switching PWs of the UPE type.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After service PWs or switching PWs are associated with an mPW, you can run the **display mpls l2vc track admin-vc** command to view information about these PWs, facilitating configuration and management.

Example

# Display information about service PWs or switching PWs that are associated with the mPW configured on loopback 0.

```
<HUAWEI> display mpls l2vc track admin-vc interface loopback 0
Total VC          :  0    2 up      0 down

 Admin-PW state   :  up
 Peer IP          :  1.1.1.1
```

```
PW type          : UPE
Total VC         :  2    2 up      0 down

*Client Interface     : Vlanif10
 VC State            : up
 VC ID              : 1113
 VC Type             : Ethernet
 Link State          : up

*Client Interface     : Vlanif10
 VC State            : up
 VC ID              : 2223
 VC Type             : Ethernet
 Link State          : up
```

Table 10-80 Description of the display mpls l2vc track admin-vc command output

Item	Description
Total VC	Number of all the service PWs and switching PWs that are associated with the mPW.
Admin-PW state	Status of the mPW. ● down ● up
Peer IP	IP address of an mPW peer. The peers of the service or switching PWs must have the same IP address as that of the mPW.
PW type	PW type. Currently, only UPE is supported.
*Client Interface	AC interface of the service PW or switching PW.
VC State	VC status. ● down ● up
VC ID	VC ID. The VC ID uniquely identifies a VC together with the VC type.
VC Type	Encapsulation type of the VC. ● ethernet ● ip-interworking ● vlan
Link State	Forwarding status of the PW. ● down ● up

10.6.9 display mpls static-l2vc

Function

The **display mpls static-l2vc** command displays information about static VCs on the device.

Format

display mpls static-l2vc [*vc-id* | **interface** *interface-type interface-number* | **state** { **down** | **up** }]

Parameters

Parameter	Description	Value
vc-id	Displays information about a static VC with a specified VC ID.	The value is an integer that ranges from 1 to 4294967295.
interface *interface-type interface-number*	Displays information about all static PWs on a specified interface. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number.	-
state { **down** | **up** }	Displays VC information based on the VC status. ● **down**: Displays information about the VC in Down state. ● **up**: Displays information about the VC in Up state.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

If you run the **display mpls static-l2vc** command with the interface name specified, information about static VCs on the interface connected to a CE is displayed. If no interface is specified, information about static VCs on all interfaces is displayed.

Example

# Display information about static VCs on the device.

```
<HUAWEI> display mpls static-l2vc
 Total svc connections:  1,  1 up,  0 down

 *Client Interface     : Vlanif10 is up
  AC Status            : down
  VC State             : up
  VC ID                : 1
  VC Type              : VLAN
  Destination          : 2.2.2.2
  Transmit VC Label    : 400
  Receive VC Label     : 600
  Label Status         : 0
  Token Status         : 0
  Control Word         : Enable
  VCCV Capability      : cw alert ttl lsp-ping bfd
  active state         : active
  Link State           : down
  Tunnel Policy Name   : tun
  PW Template Name     : --
  Main or Secondary    : Main
  load balance type    : flow
  Access-port          : false
  VC tunnel/token info : 1 tunnels/tokens
  NO.0  TNL type       : lsp   , TNL ID : 0x800802
  Backup TNL type      : lsp   , TNL ID : 0x0
  Create time          : 0 days, 0 hours, 0 minutes, 34 seconds
  UP time              : 0 days, 0 hours, 0 minutes, 31 seconds
  Last change time     : 0 days, 0 hours, 0 minutes, 31 seconds
  VC last up time      : 2011/07/04 20:29:18
  VC total up time     : 0 days, 0 hours, 0 minutes, 33 seconds
  CKey                 : 2
  NKey                 : 1
  BFD for PW           : unavailable
```

Table 10-81 Description of the **display mpls static-l2vc** command output

Item	Description
Total svc connections	Number of established SVCs, including the number of SVCs in Up and Down states.
Client Interface	AC interface and its status.
AC Status	Status of the AC: ● up ● down
VC State	Status of the VC: ● up ● down
VC ID	ID of the VC, which uniquely identifies a VC. If you run the **mpls static-l2vc** command without the VC ID specified, the value of this field is displayed as 0.

Item	Description
VC Type	Encapsulation type of the VC: ● VLAN ● Ethernet
Destination	LSR ID of the remote end on the VC.
Transmit VC Label	Local VC label.
Receive VC Label	Remote VC label.
Label Status	Whether the label can be used: ● 0: The label can be used. ● 1: Wait for the SMB to confirm the label status. ● 2: The label is released. ● 3: SMB confirmation failed.
Token Status	Whether the token can be used: ● 0: The token can be used. ● 1: Wait for the SMB to confirm the token status. ● 2: The token is released. ● 3: SMB confirmation failed.
Control Word	Whether the control word function is enabled: ● enable ● disable
VCCV Capability	Whether VCCV is enabled.
active state	Whether the PW is in active state. A PW in active state can forward packets. ● active ● inactive
Link State	Integrative PW status: ● up ● down If any of the following status is Down, the PW link state is Down: ● Service PW status ● OAM status
Tunnel Policy Name	Name of the tunnel policy.
PW Template Name	Name of the PW template.
Main or Secondary	Whether the VC is a primary VC or a secondary VC.

Item	Description
load balance type	Load balancing mode of Martini VLL: ● flow: indicates flow-based load balancing. ● packet: indicates packet-based load balancing.
Access-port	Whether the interface supports the access-port attribute: ● true: indicates that the interface supports the access-port attribute. ● false: indicates that the interface does not support the access-port attribute.
VC Tunnel/token info	Information about the VC tunnel or token used by the VC. The value **1 tunnels/tokens** indicates that the PW uses one tunnel or token.
NO.0 TNL Type	Type of the tunnel used by the PW
Backup TNL Type	Type of the backup tunnel when PW over LDP FRR is used.
Create time	How long the VC has been created.
UP time	How long the VC keeps the Up state.
Last change time	How long the VC status remains unchanged.
VC last up time	Last time when the VC became Up.
VC total up time	Total duration of the VC in Up state.
CKey	Index of the public tunnel for VPN QoS.
NKey	Index of the public tunnel.
BFD for PW	Whether BFD is configured. ● unavailable: indicates that BFD is not configured. ● available: indicates that BFD is configured. ● timeout: timeout period after which a BFD session fails to be established

# Display information about static VCs on VLANIF 10.

```
<HUAWEI> display mpls static-l2vc interface vlanif 10
 *Client Interface     : Vlanif10 is up
  AC Status            : down
  VC State             : up
  VC ID                : 1
  VC Type              : VLAN
  Destination          : 2.2.2.2
  Transmit VC Label    : 400
  Receive VC Label     : 600
  Label Status         : 0
  Token Status         : 0
  Control Word         : Enable
```

```
VCCV Capability      : cw alert ttl lsp-ping bfd
active state         : active
Link State           : down
Tunnel Policy        : tun
PW Template Name     : --
Main or Secondary    : Main
load balance type    : flow
Access-port          : false
VC tunnel/token info : 1 tunnels/tokens
NO.0  TNL Type       : lsp   , TNL ID : 0x56
Backup TNL Type      : lsp   , TNL ID : 0x0
Create time          : 0 days, 0 hours, 0 minutes, 34 seconds
UP time              : 0 days, 0 hours, 0 minutes, 31 seconds
Last change time     : 0 days, 0 hours, 0 minutes, 31 seconds
VC last up time      : 2011/07/04 20:29:18
VC total up time     : 0 days, 0 hours, 0 minutes, 33 seconds
CKey                 : 2
NKey                 : 1
Diffserv Mode        : uniform
Service Class        : be
Color                : --
DomainId             : --
Domain Name          : --
BFD for PW           : unavailable
```

Table 10-82 Description of the **display mpls static-l2vc interface** command output

Item	Description
Client Interface	AC interface and its status.
AC Status	Status of the link between the PE and its directly connected CE.
VC State	Status of the VC.
VC ID	ID of the VC, which uniquely identifies a VC.
VC Type	Encapsulation type of the VC.
Destination	LSR ID of the remote end on the VC.
Transmit VC Label	VC label sent by the local device.
Receive VC Label	VC label received by the local device.
Control Word	Whether the control word function is enabled.
VCCV Capability	Whether VCCV is enabled.
Tunnel Policy	Name of the tunnel policy. The value -- indicates that no tunnel policy is configured.
PW Template Name	Name of the PW template. The value -- indicates that no PW template is configured.
Main or Secondary	Whether the VC is a primary VC or a secondary VC.
VC tunnel/token info	Information about the tunnel or token used by the VC. The value **1 tunnels/tokens** indicates that the PW uses one tunnel or token.

Item	Description
Create time	How long the VC has been created.
UP time	How long the VC keeps the Up state.
Last change time	How long the VC status remains unchanged.
VC last up time	Last time when the VC became Up.
VC total up time	Total duration of the VC in Up state.
CKey	Index of the public tunnel for VPN QoS.
NKey	Index of the public tunnel.
Diffserv Mode	QoS DiffServ mode for VLL services.
Service Class	QoS service class for VLL services.
Color	QoS color for VLL services.
DomainId	ID of a domain.
Domain Name	Name of a domain.
BFD for PW	Whether BFD is configured. ● unavailable: indicates that BFD is not configured. ● available: indicates that BFD is configured. ● timeout: timeout period after which a BFD session fails to be established

# Display information about SVCs in Up state between peers.

```
<HUAWEI> display mpls static-l2vc state up
 Total svc connections:  1,  1 up,  0 down
 *Client Interface     : Vlanif10 is up
  AC Status            : up
  VC State             : up
  VC ID                : 0
  VC Type              : Ethernet
  Destination          : 2.2.2.2
  Transmit VC Label    : 100
  Receive VC Label     : 200
  Label Status         : 0
  Token Status         : 0
  Control Word         : Disable
  VCCV Capability      : alert ttl lsp-ping bfd
  active state         : active
  Link State           : up
  Tunnel Policy Name   : --
  PW Template Name     : --
  Main or Secondary    : Main
  load balance type    : flow
  Access-port          : false
  VC tunnel/token info : 1 tunnels/tokens
  NO.0  TNL Type       : lsp   , TNL ID : 0x56
  Backup TNL Type      : lsp   , TNL ID : 0x0
  Create time          : 0 days, 4 hours, 55 minutes, 41 seconds
  UP time              : 0 days, 4 hours, 55 minutes, 40 seconds
  Last change time     : 0 days, 4 hours, 55 minutes, 40 seconds
```

```
VC last up time      : 2011/09/09 10:25:22
VC total up time     : 0 days, 4 hours, 55 minutes, 40 seconds
CKey                 : 19
NKey                 : 1
BFD for PW           : unavailable
```

Table 10-83 Description of the **display mpls static-l2vc state** command output

Item	Description
Total svc connections	Number of established SVCs, including the number of SVCs in Up and Down states.
Client Interface	AC interface and its status.
AC Status	Status of the AC.
VC State	Status of the VC.
VC ID	ID of the VC, which uniquely identifies a VC.
VC Type	Encapsulation type of the VC.
Destination	LSR ID of the remote end on the VC.
Transmit VC Label	Local VC label.
Receive VC Label	Remote VC label.
Control Word	Whether the control word function is enabled.
VCCV Capability	Whether VCCV is enabled.
Tunnel Policy Name	Name of the tunnel policy.
PW Template Name	Name of the PW template.
Main or Secondary	Whether the VC is a primary VC or a secondary VC.
Create time	How long the VC has been created.
UP time	How long the VC keeps the Up state.
Last change time	How long the VC status remains unchanged.
VC last up time	Last time when the VC became Up.
VC total up time	Total duration of the VC in Up state.
CKey	Index of the public tunnel for VPN QoS.
NKey	Index of the public tunnel.
BFD for PW	Whether BFD is configured. ● unavailable: indicates that BFD is not configured. ● available: indicates that BFD is configured. ● timeout: timeout period after which a BFD session fails to be established

10.6.10 display mpls static-l2vc brief

Function

The **display mpls static-l2vc brief** command displays brief information about static VCs on the device.

Format

display mpls static-l2vc brief

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The **display mpls static-l2vc brief** command is recommended when a large number of static VCs are configured on the device.

Example

# Display brief information about static VCs on the device.

```
<HUAWEI> display mpls static-l2vc brief
Total svc connections:  2,  1 up,  1 down

 *Client Interface            : Eth-Trunk2  is up
  AC Status                   : up
  VC State                    : up
  VC ID                       : 0
  VC Type                     : VLAN
  Destination                 : 10.1.1.1

 *Client Interface            : Eth-Trunk3  is down
  AC Status                   : down
  VC State                    : down
  VC ID                       : 100
  VC Type                     : Ethernet
  Destination                 : 10.1.1.2
```

Table 10-84 Description of the **display mpls static-l2vc brief** command output

Item	Description
Total SVC Connections	Number of established SVCs, including the number of SVCs in Up and Down states.

Item	Description
Client Interface	AC interface and its status.
AC Status	Status of the AC: ● up: An AC has been established. ● down: An AC is not established.
VC State	Status of the VC: ● up: A VC has been established. ● down: A VC is not established.
VC ID	ID of the static VC. If you run the **mpls static-l2vc** command without the VC ID specified, the value of this field is displayed as 0.
VC Type	Encapsulation type of the VC: ● VLAN ● Ethernet
Destination	IPv4 address of the peer. Generally, the value is the loopback address of the peer.

10.6.11 display mpls switch-l2vc

Function

The **display mpls switch-l2vc** command displays information about PW switching, including static, dynamic, and mix PW switching.

Format

display mpls switch-l2vc [*ip-address vc-id* **encapsulation** *encapsulation-type* | **state** { **down** | **up** }]

Parameters

Parameter	Description	Value
ip-address	Specifies the LSR ID of the peer PE.	-
vc-id	Specifies the VC ID.	The value is an integer that ranges from 1 to 4294967295.

Parameter	Description	Value
encapsulation *encapsulation-type*	Specifies the PW encapsulation type.	Currently, the device supports the following types encapsulation types: **ethernet**, **vlan**, and **ip-interworking**.
state { **down** | **up** }	Displays VC information based on the VC status. ● **down**: Displays information about the VC in Down state. ● **up**: Displays information about the VC in Up state.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

If parameters in the **display mpls switch-l2vc** command are not specified, information about all PW switching is displayed.

Example

# Display information about the specified PW switching.

```
<HUAWEI> display mpls switch-l2vc 1.1.1.9 100 encapsulation ethernet
*Switch-l2vc type              : SVC<---->SVC
 Peer IP Address               : 3.3.3.9, 1.1.1.9
 VC ID                         : 100, 100
 VC Type                       : Ethernet
 VC State                      : up
 In/Out Label                  : 200/200, 100/100
 InLabel Status                : 0 , 0
 Control Word                  : Disable, Disable
 VCCV Capability               : alert ttl lsp-ping bfd, alert ttl lsp-ping bfd
 Switch-l2vc tunnel info       :
                                 1 tunnels for peer 5.5.5.9
                                 NO.0  TNL Type : lsp   , TNL ID : 0x11
                                 1 tunnels for peer 1.1.1.9
                                 NO.0  TNL Type : lsp   , TNL ID : 0xb
 CKey                          : 44, 1
 NKey                          : 43, 3
 Tunnel policy                 : --,--
 Control-Word transparent      : YES
 Create time                   : 0 days, 0 hours, 7 minutes, 2 seconds
 UP time                       : 0 days, 0 hours, 7 minutes, 2 seconds
 Last change time              : 0 days, 0 hours, 7 minutes, 2 seconds
 VC last up time               : 2008/07/24 12:31:31
 VC total up time              : 0 days, 2 hours, 12 minutes, 51 seconds
```

Table 10-85 Description of the **display mpls switch-l2vc** command output (SVC-SVC)

Item	Description
Switch-l2vc Type	Switching type: ● LDP-LDP ● LDP-SVC ● SVC-SVC When primary/secondary PWs and PW switching are configured, the value of this field must be LDP-LDP. ● LDP: indicates a dynamic PW. ● SVC: indicates a static PW.
Peer ip address	IP addresses of the peers at two ends of a switching PW, which are displayed in left and right columns respectively.
VC ID	ID of the VC, which uniquely identifies a VC. Here, the field indicates the two switched VC IDs.
VC Type	Encapsulation type of the VC.
VC State	Status of the VC: ● Up: A VC has been established. ● Down: A VC is not established.
In/Out Label	Incoming or outgoing label.
InLabel Status	Status of the inner label.
Control Word	Whether the control word function is enabled on both ends: ● Disable ● Enable
VCCV Capability	Type of VCCV supported on the local device. ● By default, the VCCV type is **alert ttl lsp-ping bfd**, indicating that the control word function is disabled and LSP ping and BFD are supported for the alert channel. ● If the control word function is enabled, the VCCV type is **cw alert ttl lsp-ping bfd**, indicating that LSP ping and BFD are supported for both the control word channel and the alert channel.

Item	Description
Switch-l2vc tunnel info: 1 tunnels for peer 3.3.3.9 NO.0 TNL Type : lsp , TNL ID : 0x11	Information about the tunnels on both ends: ● TNL Type: indicates the type of the tunnel. ● TTNL ID: indicates the tunnel ID.
CKey	Index of the public tunnel for VPN QoS.
NKey	Index of the public tunnel.
Tunnel policy	Name of the tunnel policy.
Control-Word transparent	Whether transparent transmission of the control word is enabled: ● yes ● no
Create Time	How long the VC has been created.
Up Time	How long the VC keeps the Up state.
Last Change Time	How long the VC status remains unchanged.
VC last up time :	Last time when the AC became Up.
VC total up time:	Total duration when the AC interface is Up.

# Display information about the switched L2VCs in Up state between peers.

```
<HUAWEI> display mpls switch-l2vc state up
Total Switch VC : 1, 1 up, 0 down
*Switch-l2vc type             : LDP<---->LDP
 Peer IP Address              : 5.5.5.9, 1.1.1.9
 VC ID                        : 200, 100
 VC Type                      : Ethernet
 VC State                     : up
 VC StatusCode                |PSN |OAM | FW |    |PSN |OAM | FW |
                 -Local VC :| UP | UP | UP |    | UP | UP |DOWN|
                 -Remote VC:| UP | UP |DOWN|    | UP | UP | UP |
 Session State                : up, up
 Local/Remote Label           : 1025/1024, 1024/1025
 InLabel Status               : 0 , 0
 Local/Remote MTU             : 1500/1500, 1500/1500
 Local/Remote Control Word    : Disable/Disable, Disable/Disable
 Local/Remote VCCV Capability : alert ttl lsp-ping bfd /alert ttl lsp-ping bfd, alert ttl lsp-ping bfd/alert ttl lsp-ping bfd
 Switch-l2vc tunnel info      :
                              1 tunnels for peer 5.5.5.9
                              NO.0  TNL Type : lsp   , TNL ID : 0x12
                              1 tunnels for peer 1.1.1.9
                              NO.0  TNL Type : lsp   , TNL ID : 0x15
 CKey                         : 44, 1
 NKey                         : 43, 3
 Tunnel policy                : --, --
 Control-Word transparent     : YES
 Create time                  : 0 days, 0 hours, 3 minutes, 54 seconds
 UP time                      : 0 days, 0 hours, 3 minutes, 12 seconds
 Last change time             : 0 days, 0 hours, 3 minutes, 12 seconds
 VC last up time              : 2008/07/24 12:31:31
 VC total up time             : 0 days, 2 hours, 12 minutes, 51 seconds
```

Table 10-86 Description of the **display mpls switch-l2vc** command output (LDP-LDP)

Item	Description
VC StatusCode	VC status code: ● PSN: indicates the fault status at the public network side. ● OAM: indicates the fault status at the AC side. ● FW: indicates the forwarding status. -Local VC: indicates the local VC status. -Remote VC: indicates the remote VC status.
Session State	Status of the session: ● Up: indicates that the session is successfully set up. ● Down: indicates that the session is not set up. ● None: indicates that no session exists.
Local/Remote Label	Incoming or outgoing label.
Local/Remote MTU	Local and remote MTU values of the PWs on two ends: ● For LDP, both the local and remote MTU values are displayed. ● For SVC, only the local MTU value is displayed.
Local/Remote Control Word	Whether the control word is enabled on both ends: ● disable: indicates that the control word is disabled. ● enable: indicates that the control word is enabled.
Local/Remote VCCV Capability	Whether VCCV is enabled on both ends: ● CC: specifies the control channel type, which can be CW, alert, or TTL. ● CV: specifies the connectivity verification mode, which can be LSP ping or BFD.
Control-Word transparent	Whether transparent transmission of the control word is enabled: ● yes ● no

# Display information about all the switched L2VCs between peers.

```
<HUAWEI> display mpls switch-l2vc
Total Switch VC : 1, 1 up, 0 down

*Switch-l2vc type              : LDP<---->SVC
 Peer IP Address               : 1.1.1.9, 5.5.5.9
 VC ID                         : 100, 200
 VC Type                       : Ethernet
 VC State                      : up
 Session State                 : up, None
 Local(In)/Remote(Out) Label   : 1027/1028, 100/200
 InLabel Status                : 0 , 0
 Local/Remote MTU              : 1500/1500, 1500
 Local/Remote Control Word     : Disable/Disable, Disable
 Local/Remote VCCV Capability : alert ttl lsp-ping bfd /alert ttl lsp-ping bfd, alert ttl lsp-ping bfd
 Switch-l2vc tunnel info       :
                                 1 tunnels for peer 1.1.1.9
                                 NO.0  TNL Type : lsp   , TNL ID : 0x9
                                 1 tunnels for peer 5.5.5.9
                                 NO.0  TNL Type : lsp   , TNL ID : 0xa
 CKey                          : 44, 1
 NKey                          : 43, 3
 Tunnel policy                 : --, --
 Create time                   : 0 days, 0 hours, 3 minutes, 48 seconds
 UP time                       : 0 days, 0 hours, 3 minutes, 48 seconds
 Last change time              : 0 days, 0 hours, 3 minutes, 48 seconds
 VC last up time               : 2008/07/24 12:31:31
 VC total up time              : 0 days, 2 hours, 12 minutes, 51 seconds
```

10.6.12 display mpls switch-l2vc brief

Function

The **display mpls switch-l2vc brief** command displays brief information about all switching PWs, including static, dynamic, and mixed switching PWs.

Format

display mpls switch-l2vc brief

Parameters

None.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

When many switching PWs are configured on the device, you can run this command to view brief information about the switching PWs. The command output of the **display mpls switch-l2vc brief** command is more concise than that of the **display mpls switch-l2vc** command.

Example

# Display brief information about switching PWs.

```
<HUAWEI> display mpls switch-l2vc brief
Total Switch VC : 1,   1 up,   0 down
*Switch-l2vc Type            : LDP<---->LDP
 Peer IP Address             : 10.1.1.9, 10.2.2.9
 VC ID                       : 200, 100
 VC Type                     : VLAN
 VC State                    : up
 Session State               : up, up
```

Table 10-87 Description of the display mpls switch-l2vc brief command output

Item	Description
Total Switch VC	Number of established Martini VCs (using the LDP signaling), including the number of Martini VCs in Up and Down states.
Switch-l2vc Type	Switching type, which can be LDP-LDP, LDP-SVC, or SVC-SVC. If the primary and secondary switching VCs are configured, the switching types of these VCs can only be LDP-LDP. ● LDP: indicates a dynamic PW. ● SVC: indicates a static PW.
Peer IP Address	IP address of the peer.
VC ID	ID of the VC, which uniquely identifies a VC. Here, the field indicates the two switched VC IDs.
VC Type	Encapsulation type of the VC.
VC State	Status of the VC: ● up: A VC has been established. ● down: A VC is not established.
Session state	Status of the session between peers: ● up: indicates that the session is successfully set up. ● down: indicates that the session is not set up. ● none: indicates that no session exists.

10.6.13 display pw-template

Function

The **display pw-template** command displays information about PW templates.

Format

display pw-template [*pw-template-name*]

Parameters

Parameter	Description	Value
pw-template-name	Specifies the PW template name. If this parameter is not specified, information about all PW templates is displayed.	The value is an existing PW template name.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

If *pw-template-name* is not specified, information about all PW templates is displayed.

Example

# Display information about all PW templates.

```
<HUAWEI> display pw-template
Total PW template number : 2
  PW Template Name : PWT
  PeerIP           : 2.2.2.2
  Tnl Policy Name  : --
  CtrlWord         : Enable
  MTU              : 1500
  Max Atm Cells    : 28
  ATM Pack Overtime: 1000
  Seq-Number       : Disable
  Transmit ATM Cells      : 28
  TDM Encapsulation Number: 32
  Jitter-Buffer           : 20
  Jitter-Buffer-Cep       : 1125
  Payload-Compression DBA : UNEQ
  Idle-Code               : ff
  Rtp-Header              : Disable
  VCCV Capability  : cw alert ttl lsp-ping bfd
  Total PW         : 6, Static PW : 1, LDP PW : 5

  PW Template Name : pwt
  PeerIP           : --
  Tnl Policy Name  : --
  CtrlWord         : Disable
  MTU              : 1500
  Max Atm Cells    : 28
  ATM Pack Overtime: 1000
  Seq-Number       : Disable
  Transmit ATM Cells      : 28
  TDM Encapsulation Number: 32
```

```
Jitter-Buffer            : 20
Jitter-Buffer-Cep        : 1125
Payload-Compression DBA : UNEQ
Idle-Code                : ff
Rtp-Header               : Disable
VCCV Capability  : alert ttl lsp-ping bfd
Total PW         : 0, Static PW : 0, LDP PW : 0
```

Table 10-88 Description of the **display pw-template** command output

Item	Description
Total PW template number	Total number of PW templates.
PW Template Name	PW template name.
PeerIP	Peer IP address.
Tnl Policy Name	Name of the public network tunnel policy applied to the PW.
CtrlWord	Whether the control word is enabled in the PW template. ● Disable ● Enable
MTU	Maximum transmission unit.
Max ATM cells	Maximum number of transmitted ATM cells.
ATM pack overtime	Delay in packaging ATM cells.
Seq-Number	Sequence number in the control word of the PW: ● If the sequence number function is enabled, the device checks the sequence number of each packet and discards any packet with an incorrect sequence number. ● If the sequence number function is disabled, the device does not check the sequence number when processing packets.
Transmit ATM Cells	Number of ATM cells sent by the local device.
TDM Encapsulation Number	Number of encapsulated TDM frames.
Jitter-Buffer	Maximum jitter buffer depth for TDM.
Jitter-Buffer-Cep	Maximum jitter buffer depth for TDM (with CEP encapsulation).
Payload-Compression DBA	Payload compression dynamic bandwidth allocation (DBA): ● UNEQ: Send DBA packets when unequipped circuit indications are detected. ● --: Payload compression DBA is not configured.

Item	Description
Idle-Code	Idle code that is filled when a jitter buffer underflow occurs.
Rtp-Header	Whether the RTP header is added to the transparently transmitted TDM frame.
VCCV Capability	VC connection verification mode. ● By default, the VCCV type is **alert ttl lsp-ping bfd**, indicating that the control word function is disabled and LSP ping and BFD are supported for the alert channel. ● If the control word function is enabled, the VCCV type is **cw alert ttl lsp-ping bfd**, indicating that LSP ping and BFD are supported for both the control word channel and the alert channel.
Total PW	Total number of PWs using this PW template, including static and dynamic PWs.

10.6.14 lspv pw reply ptn-mode

Function

The **lspv pw reply ptn-mode** command configures the SPE and TPE to reply trace VC packets in a multi-segment PW scenario.

The **undo lspv pw reply ptn-mode** command restores the default configuration.

By default, the **lspv pw reply ptn-mode** command is not configured.

Format

lspv pw reply ptn-mode

undo lspv pw reply ptn-mode

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

When the source end starts a tracert test in PTN mode to detect the connectivity of the multi-hop PW, the **lspv mpls-pw reply ptn-mode** command needs to be run on the SPE and TPE. If the PTN mode is not specified, the **lspv mpls-pw reply ptn-mode** command is not required.

Example

# Run **lspv pw reply ptn-mode** command to enable the SPE and TPE to respond to tracert VC packets in PTN mode.

```
<HUAWEI> system-view
[HUAWEI] lspv pw reply ptn-mode
```

10.6.15 manual-set pw-ac-fault

Function

The **manual-set pw-ac-fault** command simulates a fault on the primary or secondary PW.

The **undo manual-set pw-ac-fault** command cancels the fault that is simulated on a primary or secondary PW.

By default, no fault is simulated on a PW.

Format

manual-set pw-ac-fault [**secondary**]

undo manual-set pw-ac-fault [**secondary**]

Parameters

Parameter	Description	Value
secondary	Simulates a fault on the secondary PW. If this parameter is not specified, a fault is simulated on the primary PW.	-

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On a network where the primary and secondary PWs need to be configured, you can run the **manual-set pw-ac-fault** command to simulate a fault on the primary or secondary PW to check whether services can be switched between the primary and secondary PWs.

Prerequisites

A VC has been created.

Example

# Simulate a fault on the PW.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 10
[HUAWEI-Vlanif10] mpls l2vc 2.2.2.2 100
[HUAWEI-Vlanif10] manual-set pw-ac-fault
```

10.6.16 mpls l2vc

Function

The **mpls l2vc** command creates a Martini VLL.

The **undo mpls l2vc** command deletes the Martini VLL from an interface.

By default, no Martini L2VPN connection is created.

Format

mpls l2vc { *ip-address* | **pw-template** *pw-template-name* }* *vc-id* [**group-id** *group-id* | **tunnel-policy** *policy-name* | [**control-word** | **no-control-word**] | [**raw** | **tagged**] | **mtu** *mtu-value* | [**secondary** | **bypass**] | **ignore-standby-state**]*

undo mpls l2vc { *ip-address* | **pw-template** *pw-template-name* }* *vc-id* [**group-id** *group-id* | **tunnel-policy** *policy-name* | [**control-word** | **no-control-word**] | [**raw** | **tagged**] | **mtu** *mtu-value* | [**secondary** | **bypass**] | **ignore-standby-state**]*

undo mpls l2vc [**secondary** | **bypass**]

Parameters

Parameter	Description	Value
ip-address	Specifies the LSR ID of a peer device on the PW.	The value is in dotted decimal notation.
pw-template *pw-template-name*	Specifies the name of a PW template.	The value is a string of 1 to 19 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Parameter	Description	Value
vc-id	Specifies a L2VC ID.	The value is an integer that ranges from 1 to 4294967295.
group-id *group-id*	Specifies a VC group ID. With the VC group ID specified, the system can execute the same operation on a group of VCs; therefore, fewer packets are exchanged between PEs. Only the VCs with the same attribute can be configured with the same VC group ID; otherwise, the PW may be torn down by mistake. This parameter is valid only on sub-interfaces.	The value is an integer that ranges from 1 to 4294967295.
tunnel-policy *policy-name*	Specifies the name of a tunnel policy.	The value is a string of 1 to 39 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
raw	Removes the provider-tag (P-Tag) from a packet. **NOTE** This parameter can be used only for Ethernet links. If neither **raw** nor **tagged** is specified, this command sets the **raw** mode on a main interface and the **tagged** mode on a sub-interface.	-

Parameter	Description	Value
tagged	Retains the P-Tag in a packet. **NOTE** This parameter can be used only for Ethernet links. If neither **raw** nor **tagged** is specified, this command sets the **raw** mode on a main interface and the **tagged** mode on a sub-interface.	-
control-word	Enables the control word function.	-
no-control-word	Disables the control word function.	-
mtu *mtu-value*	Specifies the MTU value. **NOTE** This parameter can be configured only on VLANIF interfaces. The MTU of another type of interface or its sub-interface can be configured in the PW template.	The value is an integer that ranges from 46 to 9600. The default value is 1500.
secondary	Indicates a secondary VC. If this parameter is not specified, a primary VC is created. You can configure a secondary VC only when the primary VC exists on the local device.	-
bypass	Indicates that the VC is a bypass VC. The encapsulation type of the bypass VC must be the same as that of the primary VC.	-
ignore-standby-state	Indicates that the PW ignores standby state information sent by the remote device.	-

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In a Martini VLL networking, you can run this command to create a VC connection for a Martini VLL.

According to different encapsulation modes on the AC interfaces, the system processes user packets in different ways, as shown in the following tables.

- Packet processing on the inbound interface in the VLL or PWE3 scenario.

AC Interface Type	Encapsulation Mode of raw	Encapsulation Mode of tagged
Dot1q termination sub-interface	Removes a tag.	No action is required.
Ethernet main interfaces	No action is required.	Adds a tag.
QinQ stacking sub-interface	No action is required.	Adds a tag.
QinQ termination sub-interface (in symmetrical mode)	Removes the outer tag.	No action is required.
QinQ termination sub-interface (in asymmetrical mode)	Removes two tags.	Removes the outer tag.
VLANIF interface (added to the VLAN in default mode)	No action is required.	Adds a tag (default VLAN ID of the interface).
VLANIF interface (added to the VLAN in non-default mode)	Removes the outer tag.	No action is required.

- Packet processing on the outbound interface in the VLL or PWE3 scenario.

AC Interface Type	Encapsulation Mode of raw	Encapsulation Mode of tagged
Dot1q termination sub-interface	Adds a tag.	No action is required.
Ethernet main interfaces	Adds a tag.	Replaces the tag with the tag that is encapsulated on the outbound interface.

AC Interface Type	Encapsulation Mode of raw	Encapsulation Mode of tagged
QinQ stacking sub-interface	No action is required.	Removes a tag.
QinQ termination sub-interface (in symmetrical mode)	Adds the outer tag.	Replaces the outer tag with the tag that is encapsulated on the outbound interface.
QinQ termination sub-interface (in asymmetrical mode)	Adds two tags.	Removes the outer tag and then adds two tags that are encapsulated on the outbound interface.
VLANIF interface (added to the VLAN in default mode)	No action is required.	Removes a tag.
VLANIF interface (added to the VLAN in non-default mode)	Adds the outer tag.	Replaces the tag with the tag that is encapsulated on the outbound interface.

Precautions

- An interface cannot function as an L2VPN AC interface and L3VPN AC interface at the same time. After an interface is bound to an L2VPN, Layer 3 features such as the IP address and routing protocol on this interface become invalid.
- You must create dynamic VCs on PEs at both ends of a PW to connect the PEs. The destination address of a VC is the LSR ID of the peer PE.
- You can set attributes for a PW template, including the remote peer, tunnel policy, control word, and VCCV. When configuring an LDP PW, you can directly apply the PW template without specifying attributes for the PW. After setting attributes for a PW template, you can update the PW template at any time. The modified PW template takes effect only after the **reset pw** command is run.
- If a PW attribute is specified in the **mpls l2vc** command, the corresponding PW attribute in the same PW template is invalid.
- If you do not specify a tunnel policy for a Martini connection, the default tunnel policy is used. By default, the LSP tunnel is preferentially selected and only one tunnel is used for load balancing. If a tunnel policy name is specified but the tunnel policy is not configured, the default tunnel policy is used.
- The MTU value is specified when you create Martini or PWE3 VLLs and is used for interconnection between the switch and other devices.
- You must configure the primary PW before configuring the secondary PW and delete the secondary PW before deleting the primary PW.

- When creating VCs dynamically, the latest configurations of some parameters override the previous ones. The parameters include **tunnel-policy** *tnl-policy-name*, **control-word**, and **no-control-word**.
- By default, link type negotiation is enabled globally on the device. If a VLANIF interface is used as an AC-side interface for L2VPN, the configuration conflicts with link type negotiation. In this case, run the **lnp disable** command in the system view to disable link type negotiation.
- When configuring BFD for static PW, the VC ID must be specified.

NOTE

- If a sub-interface is bound to a VLL, the sub-interface can be deleted only after the sub-interface is unbound from the VLL.
- If a sub-interface is bound to a VLL, you cannot change the encapsulation type of the main interface.

Example

# Create a Martini connection on the VLANIF interface.

```
<HUAWEI> system-view
[HUAWEI] vlan batch 10
[HUAWEI] interface vlanif 10
[HUAWEI-Vlanif10] mpls l2vc 10.2.2.9 100
```

# Create a Martini connection on the GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] mpls l2vc 10.2.2.9 100
```

10.6.17 mpls l2vc admin

Function

The **mpls l2vc admin** command creates a management PW (mPW).

The **undo mpls l2vc admin** command deletes an mPW.

By default, no mPW is configured.

Format

mpls l2vc { *ip-address* | **pw-template** *pw-template-name* } * *vc-id* [**tunnel-policy** *policy-name* | **control-word** | **admin**] *

undo mpls l2vc [{ *ip-address* | **pw-template** *pw-template-name* } * *vc-id* [**tunnel-policy** *policy-name* | **control-word** | **admin**] *]

Parameters

Parameter	Description	Value
ip-address	Specifies the IP address of the mPW peer, which is usually the LSR ID of the remote device.	The value is in dotted decimal notation.
pw-template *pw-template-name*	Specifies the name of a PW template.	The value is a string of 1 to 19 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
vc-id	Specifies a VC ID. The VC ID must be unique on the local device, and identifies a VC together with the VC type. After a VC ID is configured, it cannot be modified. To modify a VC ID, delete the VC and configure it again. The VC IDs of the primary VC, secondary VC, and bypass VC must be different.	The value is an integer that ranges from 1 to 4294967295.
tunnel-policy *policy-name*	Specifies the name of a tunnel policy. ● If the name of the tunnel policy is specified but the tunnel policy is not configured, the default tunnel policy is used. ● If the name of the tunnel policy is not specified, the default tunnel policy is used. The LSP tunnel is preferred and only one LSP is used for load balancing in the default tunnel policy. **NOTE** Before importing a tunnel policy, define the name and attribute of the tunnel policy in the system view first.	The value is a string of 1 to 39 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
control-word	Enables the control word function. After the control word function is enabled, the device processes the Sequence Number, Length, and Layer-2 PDU fields in the packets.	-
admin	Designates the created PW as an mPW.	-

Views

Loopback interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

BFD is often configured for PWs to quickly detect PW faults. If there are a large number of service PWs with the same source and destination, you can configure mPWs with the same source and destination as those of the service PWs and associate the service PWs with the mPWs. By tracking the status of the mPWs, BFD can quickly detect faults on service PWs associated with the mPWs. BFD does not need to be configured for service PWs. This method reduces the number of BFD sessions and saves system resources and public network link bandwidth.

You can run the **mpls l2vc admin** command to create an mPW.

Prerequisites

MPLS L2VPN has been enabled using the **mpls l2vpn** command.

If **pw-template** *pw-template-name* is specified, a PW template has been created using the **pw-template** command.

Follow-up Procedure

Run the **mpls l2vc track admin-vc** command to associate service PWs with the mPWs.

Precautions

Generally, an mPW is configured on the primary PW path but not the secondary PW path.

Example

# Create an mPW on loopback 0 with the remote device LSR ID 1.1.1.1 and VC ID 1.

```
<HUAWEI> system-view
[HUAWEI] interface loopback 0
[HUAWEI-Loopback0] mpls l2vc 1.1.1.1 1 admin
```

10.6.18 mpls l2vc track admin-vc

Function

The **mpls l2vc track admin-vc** command associates service PWs with the mPWs.

The **undo mpls l2vc track admin-vc** command deletes the association between service PWs and mPWs.

By default, service PWs are not associated with the mPWs.

Format

mpls l2vc [**secondary** | **bypass**] **track admin-vc interface loopback** *interface-number*

undo mpls l2vc [**secondary** | **bypass**] **track admin-vc**

Parameters

Parameter	Description	Value
secondary	Associates the secondary service PW with the mPW.	-
bypass	Associates the bypass service PW with the mPW.	-
interface loopback *interface-number*	Specifies the loopback interface on which the mPW is configured.	The value is a decimal integer and must be the same as the number of the loopback interface on which the mPW is configured.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

BFD is often configured for PWs to quickly detect PW faults. If there are a large number of service PWs with the same source and destination, you can configure mPWs with the same source and destination as those of the service PWs and associate these service PWs with the mPWs. By tracking the status of the mPWs, BFD can quickly detect faults on service PWs associated with the mPWs. BFD does not need to be configured for service PWs. This method reduces the number of BFD sessions and saves system resources and public network link bandwidth.

You can run the **mpls l2vc track admin-vc** command to associate service PWs with mPWs for service PW status monitoring.

Prerequisites

Service PWs and mPWs have been created using the **mpls l2vc** and **mpls l2vc admin** commands.

- An mPW and its associated service PW must have the same peers.
- A service PW can be associated with only one mPW.
- Multiple service PWs with the same source and destination can be associated with only one mPW.

Precautions

After service PWs are associated with an mPW, the mPW detects public network link faults in a unified manner.

- If the mPW status remains unchanged, traffic can be properly forwarded over service PWs.
- If the mPW detects a public link fault, the mPW changes its status from Up to Down and notifies all its associated service PWs.
  - If both primary and secondary service PWs exist, the mPW triggers a switchover between the primary and secondary service PWs.
  - If only one service PW exists, the service PW changes its status from Up to Down and stops forwarding data.
- After the fault is rectified, the mPW changes its status from Down to Up. If both primary and secondary service PWs exist, a switchover will be performed between them based on the configured revertive switching policy. If only one service PW exists, the service PW changes its status from Down to Up. The service PW then starts to forward traffic again.

The **mpls l2vc track admin-vc** command applies to only single-hop primary and secondary PWs and does not apply to multi-hop PWs.

Example

# Associate the primary service PW with the mPW.

```
<HUAWEI> system-view
[HUAWEI] interface loopback 0
[HUAWEI-Loopback0] mpls l2vc 1.1.1.1 1 admin
[HUAWEI-Loopback0] quit
[HUAWEI] interface vlanif 10
[HUAWEI-Vlanif10] mpls l2vc 1.1.1.1 5
[HUAWEI-Vlanif10] mpls l2vc track admin-vc interface loopback 0
```

# Associate the secondary service PW with the mPW.

```
<HUAWEI> system-view
[HUAWEI] interface loopback 1
[HUAWEI-Loopback1] mpls l2vc 2.2.2.2 2 admin
[HUAWEI-Loopback1] quit
[HUAWEI] interface vlanif 20
[HUAWEI-Vlanif20] mpls l2vc 1.1.1.1 10
[HUAWEI-Vlanif20] mpls l2vc 2.2.2.2 6 secondary
[HUAWEI-Vlanif20] mpls l2vc secondary track admin-vc interface loopback 1
```

# Associate the bypass service PW with the mPW.

```
<HUAWEI> system-view
[HUAWEI] interface loopback 2
[HUAWEI-Loopback2] mpls l2vc 3.3.3.3 3 admin
[HUAWEI-Loopback2] quit
[HUAWEI] interface vlanif 30
[HUAWEI-Vlanif30] mpls l2vc 1.1.1.1 20 bypass
[HUAWEI-Vlanif30] mpls l2vc 3.3.3.3 7 bypass
[HUAWEI-Vlanif30] mpls l2vc bypass track admin-vc interface loopback 2
```

10.6.19 mpls l2vpn

Function

The **mpls l2vpn** command enables MPLS L2VPN and displays the MPLS L2VPN view.

The **undo mpls l2vpn** command disables MPLS L2VPN and deletes all the L2VPN configurations.

By default, the MPLS L2VPN function is disabled.

Format

mpls l2vpn

undo mpls l2vpn

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To configure MPLS L2VPN functions or perform configurations in the MPLS L2VPN view on the MPLS L2VPN network, run the **mpls l2vpn** command to enable MPLS L2VPN and enter the MPLS L2VPN view.

Prerequisites

Basic MPLS functions have been configured. For details, see the **mpls lsr-id** and **mpls** commands.

Precautions

When the command is configured, a P device does not need to be enabled with the MPLS L2VPN function.

After the **mpls l2vpn** command is executed:

- If MPLS L2VPN is disabled on the device, MPLS L2VPN is enabled and the MPLS L2VPN view is displayed.
- If MPLS L2VPN is enabled on the device, the MPLS L2VPN view is displayed.

NOTICE

After the **undo mpls l2vpn** command is run in the system view, L2VPN services may be interrupted, and all L2VPN configurations are cleared. If you want to restore the L2VPN configurations, re-run all the deleted commands.

Example

# Enable MPLS L2VPN.

```
<HUAWEI> system-view
[HUAWEI] mpls lsr-id 10.1.1.1
[HUAWEI] mpls
[HUAWEI-mpls] quit
[HUAWEI] mpls l2vpn
[HUAWEI-l2vpn]
```

10.6.20 mpls l2vpn flow-label

Function

The **mpls l2vpn flow-label** command enables flow label-based load balancing for PWs on an interface.

The **undo mpls l2vpn flow-label** command disables flow label-based load balancing for PWs on an interface.

By default, flow label-based load balancing is disabled for PWs on an interface.

NOTE

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

Format

mpls l2vpn flow-label { **both** | **send** | **receive** } [**secondary**] [**static**]

undo mpls l2vpn flow-label { **both** | **send** | **receive** } [**secondary**] [**static**]

undo mpls l2vpn flow-label [**secondary**]

Parameters

Parameter	Description	Value
both	Enables flow label-based load balancing for outgoing traffic and incoming traffic.	-
send	Enables flow label-based load balancing for outgoing traffic.	-
receive	Enables flow label-based load balancing for incoming traffic.	-

Parameter	Description	Value
secondary	Enables flow label-based load balancing for the secondary PW. If **secondary** is not configured, flow label-based load balancing is configured for the primary PW. Flow label-based load balancing can be configured for a secondary PW only if the secondary PW exists.	-
static	Statically configures flow label-based load balancing. For dynamic PWs, if **static** is not configured, the flow label-based load balancing capability of the local end is negotiated by the remote end. For static PWs, the flow label-based load balancing capability is statically configured, irrespective of whether **static** is configured.	-

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When multiple links exist between provider (P) devices, configure flow label-based load balancing to improve L2VPN traffic forwarding efficiency. After flow label-based load balancing is enabled on a PE, the PE adds different labels for different L2VPN data flows to distinguish the data flows. After a P device receives a data packet carrying a flow label, it performs the Hash calculation and selects a forwarding path based on the flow label in the data packet. This processing implements load balancing. You can run the **mpls l2vpn flow-label** command to enable flow label-based load balancing for L2VPN on an interface.

Prerequisites

Before you enable flow label-based load balancing for an interface, create a VC connection on this interface and enable Multiprotocol Label Switching (MPLS) L2VPN.

Precautions

Flow label-based load balancing can be enabled only when any of the following conditions is true:

- The **receive** parameter is configured on the local PE, and the **send** parameter is configured on the remote PE.
- The **send** parameter is configured on the local PE, and the **receive** parameter is configured on the remote PE.
- Both the **send** and **receive** parameters are configured on the local and remote PEs.

The **secondary** parameter indicates that flow label-based load balancing takes effect only for the secondary PW. If you specify **secondary** parameter, flow label-based load balancing takes effect only for the primary PW.

Example

# Enable flow label-based load balancing for PWs on Vlanif 100.

```
<HUAWEI> system-view
[HUAWEI] interface Vlanif 100
[HUAWEI-Vlanif100] mpls l2vc 2.2.2.2 100
[HUAWEI-Vlanif100] mpls l2vpn flow-label both
```

10.6.21 mpls l2vpn ip-parse enable

Function

The **mpls l2vpn ip-parse enable** command enables the IP packet parsing function of the MPLS L2VPN module.

The **undo mpls l2vpn ip-parse enable** command disables the IP packet parsing function of the MPLS L2VPN module.

By default, the IP packet parsing function of the MPLS L2VPN module is enabled.

Format

mpls l2vpn ip-parse enable

undo mpls l2vpn ip-parse enable

NOTE

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

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In a Layer 2 VPN scenario, if a traffic policy is configured in the inbound direction of an AC-side interface on a device, L2VPN traffic forwarded from a PE may incorrectly match the traffic policy. As a result, traffic fails to be forwarded. To ensure normal traffic forwarding, run the **undo mpls l2vpn ip-parse enable** command to disable the IP packet parsing function of the MPLS L2VPN module.

Precautions

If the enhanced load balancing mode is configured for an Eth-Trunk, it is recommended that the IP packet parsing function of the MPLS L2VPN module be enabled.

Example

# Disable the IP packet parsing function of the MPLS L2VPN module.

```
<HUAWEI> system-view
[HUAWEI] undo mpls l2vpn ip-parse enable
```

10.6.22 mpls l2vpn no-request-message

Function

The **mpls l2vpn no-request-message** command disables the device from sending L2VPN label request messages to a specified peer.

The **undo mpls l2vpn no-request-message** command re-enables the device to send L2VPN label request messages to a specified peer.

By default, the system sends L2VPN label request messages to all its peers.

Format

mpls l2vpn no-request-message peer *ip-address*

undo mpls l2vpn no-request-message peer *ip-address*

Parameters

Parameter	Description	Value
peer *ip-address*	Specifies the LSR ID of a peer device on the PW.	The value is in dotted decimal notation.

Views

MPLS-L2VPN view

Default Level

2: Configuration level

Usage Guidelines

On a PW in PWE3/Martini mode between two PEs with a Huawei device functioning as one PE and a non-Huawei device functioning as the other, if the non-Huawei device does not have the capability of processing L2VPN label requests, the **mpls l2vpn no-request-message** command needs to be run on the Huawei device to allow communication between the two devices. This command cannot be used in other cases.

Example

# Disable the device from sending L2VPN label request messages to a peer with the LSR ID being 10.2.2.9.

```
<HUAWEI> system-view
[HUAWEI] mpls l2vpn
[HUAWEI-l2vpn] mpls l2vpn no-request-message peer 10.2.2.9
```

10.6.23 mpls l2vpn pw bfd

Function

The **mpls l2vpn pw bfd** command enables dynamic BFD for PWs and adjusts BFD parameters on an AC interface.

The **undo mpls l2vpn pw bfd** command restores default BFD parameters of dynamic BFD for PWs on an AC interface.

By default, dynamic BFD for PWs is not configured on an AC interface.

Format

mpls l2vpn pw bfd [**detect-multiplier** *multiplier* | **min-rx-interval** *rx-interval* | **min-tx-interval** *tx-interval*] * [**remote-vcid** *vc-id*] [**secondary**]

undo mpls l2vpn pw bfd [**detect-multiplier** | **min-rx-interval** | **min-tx-interval**] * [**secondary**]

undo mpls l2vpn pw bfd [**detect-multiplier** *multiplier* | **min-rx-interval** *rx-interval* | **min-tx-interval** *tx-interval*] * [**remote-vcid** *vc-id*] [**secondary**]

Parameters

Parameter	Description	Value
detect-multiplier *multiplier*	Specifies the local detection multiplier.	The value is an integer that ranges from 3 to 50. The default value is 3.

Parameter	Description	Value
min-rx-interval *rx-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-S, S5731-H and S5731S-H, the value ranges from 3 to 1000. ● After the **set service-mode enhanced-bfd** command is configured on the S5732-H, S6730-S, S6730-H, and S6730S-H, the value ranges from 3 to 1000.
min-tx-interval *tx-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-S, S5731-H and S5731S-H, the value ranges from 3 to 1000. ● After the **set service-mode enhanced-bfd** command is configured on the S5732-H, S6730-S, S6730-H, and S6730S-H, the value ranges from 3 to 1000.
remote-vcid *vc-id*	Specifies the VC ID of the peer device.	This parameter is mandatory when a multi-hop PW is detected. The value of this parameter is the VC ID of the remote end of the PW. The value is an integer that ranges from 1 to 4294967295.

Parameter	Description	Value
secondary	Configures BFD and its parameters on the secondary PW. By default, BFD and its parameters are configured on the primary PW. **NOTE** The **secondary** parameter cannot be run on Loopback interface view.	-

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On a network where BFD is used to detect faults, run the **mpls l2vpn pw bfd** command to enable dynamic BFD for PWs and adjust BFD parameters on an AC interface.

Precautions

To reduce usage of system resources, when a BFD session is detected in Down state, the system changes the minimum interval for receiving BFD packets and the minimum interval for sending BFD packets to random values between 1000 ms and 3000 ms. When the BFD session becomes Up, the configured intervals are restored.

Example

# Enable dynamic BFD for PWs on VLANIF 10 and set BFD parameters.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 10
[HUAWEI-Vlanif10] mpls l2vc 2.2.2.2 100
[HUAWEI-Vlanif10] mpls l2vpn pw bfd min-rx-interval 100 min-tx-interval 100
```

10.6.24 mpls l2vpn redundancy

Function

The **mpls l2vpn redundancy** command specifies the PW negotiation mode.

The **undo mpls l2vpn redundancy** command restores the default PW mode.

By default, a device determines the primary and secondary PWs locally by using FRR, without negotiating with other nodes.

Format

mpls l2vpn redundancy { **independent** | **master** }

undo mpls l2vpn redundancy { **independent** | **master** }

Parameters

Parameter	Description	Value
independent	Indicates PW redundancy in independent mode.	-
master	Indicates PW redundancy in master/slave mode.	-

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After configuring the primary and secondary PWs on a PE, you can specify the PW redundancy mode. The following PW redundancy modes are supported:

- FRR mode:

  The FRR mode is the default PW redundancy mode and does not need to be configured.

  The FRR mode applies to VLL FRR and PWE3 FRR scenarios. The FRR mode must be used with PW OAM and AC OAM. End-to-end FRR can be performed only after OAM mapping is enabled on the PE.
- Master/slave mode:

  The master/slave mode is often used in scenarios where VLL accesses VPLS. After the **mpls l2vpn redundancy** command is configured on a PE, the PE determines the primary/secondary status of PWs based on its local configurations. The master/slave mode can use the bypass PW to isolate PW-side failures from AC-side failures.
- Independent mode:

  The independent mode is often used with E-Trunk, and VRRP. The independent mode can use the bypass PW to isolate PW-side failures, but cannot isolate AC-side failures.

Prerequisites

The primary and secondary PWs must have been configured on the PE.

Follow-up Procedure

The FRR mode and master/slave mode support revertive policies. You can run the **mpls l2vpn reroute** command to configure a revertive policy. By default, the revertive switching is performed after a delay.

The independent mode supports only immediate switchback.

Precautions

If the **mpls l2vpn redundancy** command is run more than once, the latest configuration overrides previous ones. The **undo mpls l2vpn redundancy** command restores the FRR mode. When using the **undo mpls l2vpn redundancy** command, ensure that the parameter in this command is the same as that in the corresponding **mpls l2vpn redundancy** command.

The FRR mode applies to VLL and PWE3. The master/slave mode and independent mode apply to PWE3.

- FRR mode: After the primary and secondary PW status is configured on a PE to which a CE is single-homed, the FRR PW redundancy mode is used by default. The local PE does not notify the remote PW of the primary/secondary PW status. As a result, the remote PE is unaware of the local primary/secondary status.
- Master/slave mode: After this mode is configured, the PE determines the primary/secondary status of PWs based on local configurations and sends the Forwarding (0x00) and Forwarding Standby (0x20) status signaling to the remote PE.
- Independent mode: After this mode is configured, the PE determines the primary/secondary status of the local PWs based on the status information sent by the remote PE and sends the Forwarding (0x00) status signaling to the remote PE.

Example

# Determine the primary and secondary PWs on VLANIF100 by using the PW negotiation mode.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] mpls l2vc 1.1.1.1 1
[HUAWEI-Vlanif100] mpls l2vc 2.2.2.2 2 secondary
[HUAWEI-Vlanif100] mpls l2vpn redundancy independent
```

10.6.25 mpls l2vpn reroute

Function

The **mpls l2vpn reroute** command configures the revertive switchover policy for the primary and secondary PWs in FRR or PW redundancy master/slave mode.

The **undo mpls l2vpn reroute** command restores the default revertive switchover policy.

By default, delayed revertive switchover is configured in FRR or PW redundancy master/slave mode.

Format

mpls l2vpn reroute { { **delay** *delay-time* | **immediately** } [**resume** *resume-time*] | **never** }

undo mpls l2vpn reroute

Parameters

Parameter	Description	Value
delay *delay-time*	Specifies the revertive switchover policy for the primary and secondary PWs as delayed revertive switchover, and sets the duration for delayed switchover.	The value is an integer that ranges from 10 to 1800, in seconds. The default value is 30.
immediately	Specifies the revertive switchover policy for the primary and secondary PWs as immediate revertive switchover.	-
resume *resume-time*	Specifies a delay after which the local device notifies the peer PE on the secondary PW of the recovery. You can set this parameter only in VLL FRR mode.	The value is an integer that ranges from 0 to 600, in seconds. The default value is 10.
never	Specifies the revertive switchover policy for the primary and secondary PWs to none revertive switchover. After the primary PW recovers, traffic is not switched to it until the secondary PW is faulty.	-

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **mpls l2vpn reroute** command configures the revertive switchover policy for the primary and secondary PWs in FRR or PW redundancy master/slave mode.

Prerequisites

The primary and secondary PWs have been configured in FRR or PW redundancy master/slave mode. The revertive switchover policy cannot be configured for PW redundancy independent mode.

Precautions

In VLL FRR mode and in PW redundancy master/slave mode, the PW revertive switchover policy is classified into the following modes:

- Immediate revertive switchover: When the primary PW recovers from a fault, the local PE switches traffic back to the primary PW immediately and notifies the peer PE on the secondary PW of the fault. In FRR mode, the local PE notifies the peer PE on the secondary PW of the recovery after a delay of *resume-time*. In PW redundancy master/slave mode, the parameter *resume-time* is not supported.

  This revertive switchover applies to scenarios in which users hope traffic to be restored as soon as possible.
- Delayed revertive switchover: When the primary PW recovers from a fault, traffic is switched back to the primary PW after a period specified by *delay-time*. After traffic is switched back, the local device immediately notifies the peer device on the secondary PW of the fault. If *resume-time* is configured in FRR mode, the local device notifies the peer device on the secondary PW of the recovery after a delay of *resume-time*.

  On a large-scale network, packet loss caused by incomplete route convergence may occur during the switchback. To prevent this problem, configure traffic to be switched back after a delay.
- None revertive switchover: When the primary PW recovers from a fault, traffic is not switched back to the primary PW until the secondary PW becomes faulty.

  If you do not want traffic to be frequently switched between the primary and secondary PWs, you can use the non-revertive switchover.

In a CE asymmetrical networking, if the Ethernet OAM function is configured on a PE interface connected to a CE, and a revertive switchover policy is configured, the value of *resume-time* cannot be 0 seconds. The value must be equal to or greater than 1 second.

Example

# Configure the device to switch traffic back to the primary PW 15 seconds after the primary PW recovers from a fault, notify the peer PE on the secondary PW of the fault when a switchover is performed, and notify the peer PE of the secondary PW of the recovery 20 seconds later.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] mpls l2vc 10.1.1.9 100
[HUAWEI-Vlanif100] mpls l2vc 10.2.2.9 200 secondary
[HUAWEI-Vlanif100] mpls l2vpn reroute delay 15 resume 20
```

10.6.26 mpls l2vpn service-name

Function

The **mpls l2vpn service-name** command sets the name of an SVC or Martini VLL service or a PWE3 service.

The **undo mpls l2vpn service-name** command deletes the configured L2VPN service name.

By default, no L2VPN service name is configured in the system.

Format

mpls l2vpn service-name *service-name*

undo mpls l2vpn service-name

Parameters

Parameter	Description	Value
service-name	Specifies the name of an L2VPN service. This parameter uniquely identifies an L2VPN service on a PE.	The value is a string of 1 to 15 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

By default, an SVC or Martini VLL service or a PWE3 service is uniquely identified by the combination of the VC ID and VC type, which are hard to remember and make maintenance complex. When a service name is used to uniquely identify an L2VPN service, the name can be defined based on requirements and the NMS operator can maintain the L2VPN service by clicking the name on the NMS graphical user interface (GUI). This simplifies operation and maintenance.

Prerequisites

An SVC or Martini VLL service or a PWE3 service has been configured on a service interface. A primary PW and a secondary PW can be configured for a Martini VLL or PWE3 service.

Precautions

On each PE, an L2VPN service name is unique. If an L2VPN service name has been used by a PW, it cannot be configured for another PW, or the system will display an error message.

If an L2VPN service already has a service name, this service name will be overwritten when a new name is configured for the L2VPN service. Therefore, when changing an L2VPN service name, you can directly configure a new service name without deleting the original one.

- Because the primary and secondary PWs are configured on the same interface, they are regarded as one PW, and a service name is configured for both of them.
- On each PE, an L2VPN service name is unique.

Example

# Set an L2VPN service name to **pw1** on a service interface.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 10
[HUAWEI-Vlanif10] mpls l2vc 10.1.1.1 1
[HUAWEI-Vlanif10] mpls l2vpn service-name pw1
```

10.6.27 mpls l2vpn stream-dual-receiving

Function

The **mpls l2vpn stream-dual-receiving** command configures an interface to receive packets from both the primary and secondary PWs.

The **undo mpls l2vpn stream-dual-receiving** command disables an interface from receiving packets from both the primary and secondary PWs.

By default, an interface cannot receive packets from the secondary PW.

Format

mpls l2vpn stream-dual-receiving

undo mpls l2vpn stream-dual-receiving

Parameters

None

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On a network configured with PW Redundancy, the **mpls l2vpn stream-dual-receiving** command must be run on a PE to which the CE is single homed, so that the PE can receive packets from both the primary and secondary PWs. This prevents packet loss during the PW switchover process.

If the command is not run, the PE receives packets only from the primary PW. This causes packet loss during a traffic switchover. After the primary PW recovers and a traffic switchover is triggered, the secondary PW on the PE becomes the primary PW and the PE notifies the peer of the status change. A delay in signaling transmission causes the peer PE to send packets along the secondary PW. After the PE receiving packets from the secondary PW, the PE discards the packets, resulting in packet loss.

Prerequisites

Primary and secondary PWs have been configured.

Precautions

The **mpls l2vpn stream-dual-receiving** command applies to only PWE3 L2VPN. If H-VPLS is configured, the command cannot be configured. If you configure this command, unidirectional broadcast traffic will be looped back.

Bypass PWs cannot be configured on a PE configured with the **mpls l2vpn stream-dual-receiving** command.

Kompella VLL FRR does not support the **mpls l2vpn stream-dual-receiving** command.

Example

# Enable the device to receive packets from both the primary and secondary PWs on VLANIF100.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] mpls l2vc 1.1.1.1 1
[HUAWEI-Vlanif100] mpls l2vc 2.2.2.2 2 secondary
[HUAWEI-Vlanif100] mpls l2vpn stream-dual-receiving
```

10.6.28 mpls l2vpn switchover

Function

The **mpls l2vpn switchover** command switches traffic from the primary PW to the secondary PW.

The **undo mpls l2vpn switchover** command disables traffic switchover and switches traffic back to the primary PW.

By default, traffic switchover is not configured.

Format

mpls l2vpn switchover

undo mpls l2vpn switchover

Parameters

None

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In master/slave PW redundancy mode, the traffic is transmitted over the primary PW in normal situations. If you want the traffic to be transmitted over the secondary PW due to reasons such as device upgrade or service re-deployment, you can use the **mpls l2vpn switchover** command to forcibly switch traffic from the primary PW to the secondary PW. After the device is upgraded or services are re-deployed, you can run the **undo mpls l2vpn switchover** command to forcibly switch traffic from the secondary PW to the primary PW.

- Before running the **mpls l2vpn switchover** command, ensure that the secondary PW is normal and can forward traffic.
- Before running the **undo mpls l2vpn switchover** command, ensure that the primary PW is normal and can forward traffic.

NOTE

If the secondary PW fails after traffic is forcibly switched to the secondary PW, the traffic will be switched back to the primary PW.

Prerequisites

The primary and secondary PWs have been established and are in the Up state.

Precautions

A PW switchover will be performed after you run the **mpls l2vpn switchover** or **undo mpls l2vpn switchover** command. If the PW to be switched to is Down or unavailable, the switchover fails.

Traffic cannot be switched from the primary PW to a bypass PW.

The two commands apply to only PWs working in master/slave mode. In a VLL FRR scenario, use the **manual-set pw-ac-fault** command to forcibly switch over PWs.

Example

# Switch traffic from the primary PW to the secondary PW.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] mpls l2vc 1.1.1.1 1
[HUAWEI-Vlanif100] mpls l2vc 2.2.2.2 2 secondary
```

```
[HUAWEI-Vlanif100] mpls l2vpn redundancy master
[HUAWEI-Vlanif100] mpls l2vpn switchover
```

10.6.29 mpls l2vpn vccv bfd-cv-negotiation fault-detection-only

Function

The **mpls l2vpn vccv bfd-cv-negotiation fault-detection-only** command sets the encapsulation type for BFD CV packets to be sent to remote peers.

The **undo mpls l2vpn vccv bfd-cv-negotiation fault-detection-only** command restores the default configuration.

By default, the device sends BFD CV packets with the encapsulation type 0x08 to all remote peers.

Format

mpls l2vpn vccv bfd-cv-negotiation fault-detection-only [**peer** *peer-address* { **enable** | **disable** }]

undo mpls l2vpn vccv bfd-cv-negotiation fault-detection-only [**peer** *peer-address*]

Parameters

Parameter	Description	Value
peer *peer-address*	Specifies the IP address of a remote peer.	The value is in dotted decimal notation.
enable	Sets the encapsulation type 0x04 for BFD CV packets to be sent to a specified remote peer.	-
disable	Set the encapsulation type 0x08 for BFD CV packets to be sent to a specified remote peer.	-

Views

MPLS L2VPN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Virtual Circuit Connectivity Verification (VCCV) is a mechanism to detect and diagnose end-to-end faults on PWs. VCCV provides a control channel between a PW's ingress and egress over which connectivity verification (CV) messages can be sent. A VCCV message includes a BFD control packet encapsulated as specified by the CV type. A BFD CV packet can be transmitted over a VCCV control channel after being encapsulated using BFD IP/UDP. As defined in RFC, BFD IP/UDP encapsulation for BFD CV packets are classified into two types:

- 0x04: used only for PW fault detection.
- 0x08: used for PW fault detection and AC/PW status signaling.

To control the encapsulation type of BFD CV packets to be sent to remote peers, run the **mpls l2vpn vccv bfd-cv-negotiation fault-detection-only** command.

- The **mpls l2vpn vccv bfd-cv-negotiation fault-detection-only** command sets the encapsulation type to 0x04 for BFD CV packets to be sent to all remote peers.
- The **undo mpls l2vpn vccv bfd-cv-negotiation fault-detection-only** command restores the default encapsulation type 0x08 for BFD CV packets to be sent to all remote peers.
- The **mpls l2vpn vccv bfd-cv-negotiation fault-detection-only peer** *peer-address* **enable** command sets the encapsulation type to 0x04 for BFD CV packets to be sent to a specified remote peer.
- The **mpls l2vpn vccv bfd-cv-negotiation fault-detection-only peer** *peer-address* **disable** command sets the encapsulation type to 0x08 for BFD CV packets to be sent to a specified remote peer.
- The **undo mpls l2vpn vccv bfd-cv-negotiation fault-detection-only peer** *peer-address* command restores the global encapsulation type for BFD CV packets to be sent to a specified remote peer.

Dynamic PWs support VCCV by default, and can use LDP signaling to advertise local attributes to remote peers. The default encapsulation type of BFD CV packets is 0x08. If a remote peer supports the encapsulation type 0x04 and BFD is used for communication, run the **mpls l2vpn vccv bfd-cv-negotiation fault-detection-only peer** *peer-address* **enable** command to change the encapsulation type of BFD CV packets to be sent to this peer to 0x04.

Precautions

After this command is run, PWs may be re-established, which causes a short service interruption.

Example

# Set the encapsulation type 0x04 for BFD CV packets to be sent to remote peers.

```
<HUAWEI> system-view
[HUAWEI] mpls l2vpn
[HUAWEI-l2vpn] mpls l2vpn vccv bfd-cv-negotiation fault-detection-only
```

# Set the encapsulation type 0x04 for BFD CV packets to be sent to a specified remote peer.

```
<HUAWEI> system-view
[HUAWEI] mpls l2vpn
[HUAWEI-l2vpn] mpls l2vpn vccv bfd-cv-negotiation fault-detection-only peer 10.10.10.1 enable
```

10.6.30 mpls static-l2vc

Function

The **mpls static-l2vc** command creates a static VC.

The **undo mpls static-l2vc** command deletes the static VCs.

By default, no static VC is created.

Format

mpls static-l2vc { { **destination** *ip-address* | **pw-template** *pw-template-name vc-id* } * | **destination** *ip-address vc-id* } **transmit-vpn-label** *transmit-label-value* **receive-vpn-label** *receive-label-value* [**tunnel-policy** *tnl-policy-name* | [**control-word** | **no-control-word**] | [**raw** | **tagged**]] *

undo mpls static-l2vc

undo mpls static-l2vc { { **destination** *ip-address* | **pw-template** *pw-template-name vc-id* } * | **destination** *ip-address vc-id* } **transmit-vpn-label** *transmit-label-value* **receive-vpn-label** *receive-label-value* [**tunnel-policy** *tnl-policy-name* | [**control-word** | **no-control-word**] | [**raw** | **tagged**]] *

Parameters

Parameter	Description	Value
destination *ip-address*	Specifies the LSR ID of a peer device on the PW.	The value is in dotted decimal notation.
pw-template *pw-template-name*	Specifies the name of a static PW template.	The value is a string of 1 to 19 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
vc-id	Specifies the VC ID.	The value is an integer that ranges from 1 to 4294967295.
transmit-vpn-label *transmit-label-value*	Specifies the value of a transmit label.	The value is an integer that ranges from 0 to 1048575.
receive-vpn-label *receive-label-value*	Specifies the value of a receive label.	The value is an integer that ranges from 16 to 1023.

Parameter	Description	Value
tunnel-policy *tnl-policy-name*	Specifies the name of a tunnel policy.	The value is a string of 1 to 39 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
control-word | **no-control-word**	Enables or disables the control word function. By default, the control word function is disabled.	-
raw	Removes the provider-tag (P-Tag) from a packet.	-
tagged	Retains the P-Tag in a packet.	-

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In an L2VPN networking, you can use this command to create a static VC between two PEs connected to CEs.

Precautions

- An interface cannot function as an L2VPN AC interface and L3VPN AC interface at the same time. After an interface is bound to an L2VPN, Layer 3 features such as the IP address and routing protocol on this interface become invalid.
- You can set attributes for a static PW template, including the remote peer, tunnel policy, control word, and VCCV. When configuring a static PW, you can directly use the static PW template without specifying attributes for the PW. After setting attributes for a static PW template, you can update the static PW template at any time. The modified static PW template takes effect only after the **reset pw** command is run.
- Static VCs must be created on PEs at both ends. The destination address of a VC is the LSR ID of the peer PE. The transmit label of the PE at one end is the

receive label of the PE at the other end. If the labels do not match, traffic may fail to be forwarded even though the **static-l2vc** field is displayed as Up.

- If no tunnel policy is specified, the default tunnel policy is used. The default policy specifies that traffic is forwarded along the LSP and only one tunnel is used for load balancing. If a tunnel policy name is specified but the tunnel policy is not configured, the default tunnel policy is used.
- When configuring a static VC, note that the value of the transmit label ranges from 0 to 1048575. This ensures the communication between the device and different types of devices.
- When creating static VCs, the latest configurations of some parameters override the previous ones. The parameters include **tunnel-policy** *tnl-policy-name*, **control-word**, and **no-control-word**.
- By default, link type negotiation is enabled globally on the device. If a VLANIF interface is used as an AC-side interface for L2VPN, the configuration conflicts with link type negotiation. In this case, run the **lnp disable** command in the system view to disable link type negotiation.

NOTE

- If a sub-interface is bound to a VLL, the sub-interface can be deleted only after the sub-interface is unbound from the VLL.
- If a sub-interface is bound to a VLL, you cannot change the encapsulation type of the main interface.

Example

# Configure a static VC. Set the LSR ID of the peer device to 1.1.1.1, transmit label to 100, and receive label to 100.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 10
[HUAWEI-Vlanif10] mpls static-l2vc destination 1.1.1.1 transmit-vpn-label 100 receive-vpn-label 100
```

# Configure a static VC by applying a PW template and set values of the VC ID, transmit label, and receive label to 100 respectively.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 10
[HUAWEI-Vlanif10] mpls static-l2vc pw-template pwt 100 transmit-vpn-label 100 receive-vpn-label 100
```

# Delete a static VC.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 10
[HUAWEI-Vlanif10] undo mpls static-l2vc
```

10.6.31 mpls switch-l2vc

Function

The **mpls switch-l2vc** command configures PW switching on the SPE to implement multi-segment PWs.

The **undo mpls switch-l2vc** command deletes PW switching.

The default policy is used for PW switching. In the default policy, LSP tunnels are used and the number of routes for load balancing is 1.

Format

# Static PW

mpls switch-l2vc *ip-address vc-id* **trans** *trans-label* **recv** *received-label* [**tunnel-policy** *policy-name*] [**oam-packet pop flow-label**] **between** *ip-address vc-id* **trans** *trans-label* **recv** *received-label* [**tunnel-policy** *policy-name*] [**oam-packet pop flow-label**] **encapsulation** *encapsulation-type* [**control-word** [**cc** { **alert** | **cw** } * **cv lsp-ping**] | [**no-control-word**] [**cc alert cv lsp-ping**]] [**control-word-transparent**]

undo mpls switch-l2vc *ip-address vc-id* **trans** *trans-label* **recv** *received-label* [**tunnel-policy** *policy-name*] [**oam-packet pop flow-label**] **between** *ip-address vc-id* **trans** *trans-label* **recv** *received-label* [**tunnel-policy** *policy-name*] [**oam-packet pop flow-label**] **encapsulation** *encapsulation-type* [**control-word** [**cc** { **alert** | **cw** } * **cv lsp-ping**] | [**no-control-word**] [**cc alert cv lsp-ping**]] [**control-word-transparent**]

# Dynamic PW

mpls switch-l2vc *ip-address vc-id* [**tunnel-policy** *policy-name*] [**oam-packet pop flow-label**] **between** *ip-address vc-id* [**tunnel-policy** *policy-name*] [**oam-packet pop flow-label**] **encapsulation** *encapsulation-type* [**control-word-transparent**]

undo mpls switch-l2vc *ip-address vc-id* [**tunnel-policy** *policy-name*] [**oam-packet pop flow-label**] **between** *ip-address vc-id* [**tunnel-policy** *policy-name*] [**oam-packet pop flow-label**] **encapsulation** *encapsulation-type* [**control-word-transparent**]

# Mixed PW

mpls switch-l2vc *ip-address vc-id* [**tunnel-policy** *policy-name*] [**oam-packet pop flow-label**] **between** *ip-address vc-id* **trans** *trans-label* **recv** *received-label* [**tunnel-policy** *policy-name*] [**oam-packet pop flow-label**] **encapsulation** *encapsulation-type* [**mtu** *mtu-value*] [**control-word** [**cc** { **alert** | **cw** } * **cv lsp-ping**] | [**no-control-word**] [**cc alert cv lsp-ping**]] [**flow-label** { **both** | **send** | **receive** }] [**control-word-transparent**]

undo mpls switch-l2vc *ip-address vc-id* [**tunnel-policy** *policy-name*] [**oam-packet pop flow-label**] **between** *ip-address vc-id* **trans** *trans-label* **recv** *received-label* [**tunnel-policy** *policy-name*] [**oam-packet pop flow-label**] **encapsulation** *encapsulation-type* [**mtu** *mtu-value*] [**control-word** [**cc** { **alert** | **cw** } * **cv lsp-ping**] | [**no-control-word**] [**cc alert cv lsp-ping**]] [**flow-label** { **both** | **send** | **receive** }] [**control-word-transparent**]

undo mpls switch-l2vc { *ip-address vc-id* **encapsulation** *encapsulation-type* | **all** }

Parameters

Parameter	Description	Value
ip-address	Specifies the LSR ID of a peer device on the PW.	The value is in dotted decimal notation.

Parameter	Description	Value
vc-id	Specifies the L2VC ID.	The value is an integer that ranges from 1 to 4294967295.
trans *trans-label*	Specifies the static label for sending packets.	The value is an integer that ranges from 0 to 1048575.
recv *received-label*	Specifies the static label for receiving packets.	The value is an integer that ranges from 16 to 1023.
tunnel-policy *policy-name*	Specifies the name of a tunnel policy. If this parameter is not specified, the default tunnel policy is used, which preferentially selects the LSP tunnel and only one tunnel is used for load balancing.	The value is a string of 1 to 39 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
oam-packet pop flow-label	Specifies that flow labels of OAM packets are popped out. If OAM packets received from remote devices carry flow labels, the **oam-packet pop flow-label** parameter must be configured to pop out flow labels so that the SPEs can process the OAM packets. **NOTE** Only the S5731-S, S5731S-S, S5731-H, S5731S-H, S5732-H, S6730-S, S6730S-S, S6730S-H, and S6730-H support this parameter.	-
between	Specifies the switching PW that corresponds to the PW	-

Parameter	Description	Value
encapsulation *encapsulation-type*	Specifies the encapsulation type of a static PW.	The encapsulation types supported by PW switching are **ethernet**, **vlan**, and **ip-interworking**. **NOTE** Static and mixed PWs support only Ethernet and VLAN encapsulation types.
mtu *mtu-value*	Specifies the MTU for negotiating dynamic PW signaling. If the non-default MTU is set when you configure a dynamic PW, you need to set the MTU manually when configuring mixed PW switching; otherwise, the signaling negotiation at the dynamic PW side may fail.	The value is an integer that ranges from 46 to 9600.
control-word	Enables the control word function. By default, the control word function is disabled.	-
no-control-word	Disable the control word function.	-
cw	Indicates the mode in which the control word function is enabled.	-
alert	Indicates the label alert tunnel for VCCV ping.	-
cv	Indicates connectivity verification, which is enabled by default.	-
lsp-ping	Indicates connectivity verification in LSP ping mode for VCs, which is enabled by default.	-

Parameter	Description	Value
control-word-transparent	Enables transparent transmission of the control word. In the scenario where a PE is dual homed to SPEs and BFD for PW is enabled, transparent transmission of the control word must be enabled on the SPEs; otherwise, the BFD negotiation fails. By default, transparent transmission of the control word is disabled.	-
all	Deletes all PW switching.	-
flow-label both	Enables flow label-based load balancing for outgoing traffic and incoming traffic. **NOTE** Only the S5731-S, S5731S-S, S5731-H, S5731S-H, S5732-H, S6730-S, S6730S-S, S6730S-H, and S6730-H support this parameter.	-
flow-label send	Enables flow label-based load balancing for outgoing traffic. **NOTE** Only the S5731-S, S5731S-S, S5731-H, S5731S-H, S5732-H, S6730-S, S6730S-S, S6730S-H, and S6730-H support this parameter.	-
flow-label receive	Enables flow label-based load balancing for incoming traffic. **NOTE** Only the S5731-S, S5731S-S, S5731-H, S5731S-H, S5732-H, S6730-S, S6730S-S, S6730S-H, and S6730-H support this parameter.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **mpls switch-l2vc** command configures PW switching on the SPE to implement multi-segment PWs.

PW switching can be classified into dynamic mode, static mode, and mixed mode. You can create PW switching of different types using different commands to meet site requirements:

- **Configuring static PW switching**: The two PW segments connected by an SPE are both static PWs. Static PW switching apples when static PWs are used on the entire network.
- **Configuring dynamic PW switching**: The two PW segments connected by an SPE are both dynamic PWs. Dynamic PW switching applies when dynamic PWs are used on the entire network.
- **Configuring mixed PW switching**: A mixed PW switching applies when an SPE connects a dynamic PW and a static PW.

Precautions

You need to configure the PW label for the static PW switching and for the static PW in the mixed PW switching.

The configuration of dynamic PW switching is simple. The remote label is sent from two neighboring ends (UPE or SPE) to the SPE through signaling. The CW and the VCCV are sent from two UPE nodes to the SPE through signaling.

When you configure mixed PW switching, the value of *ip-address vc-id* before **between** in the command is for the dynamic PW, and the value of *ip-address vc-id* after **between** in the command is for the static PW. The two values cannot be interchanged.

NOTE

- The VC IDs for PW switching can be different.
- The combination of the PW ID and PW type must be unique on each node. The PW IDs at two ends of PW switching can be the same.
- When creating PW switching, the latest configurations of some parameters override the previous ones. The parameters include **tunnel-policy** *policy-name*, **control-word-transparent**, **control-word**, **no-control-word**, **mtu** *mtu-value*, **oam-packet pop flow-label**, and **flow-label** { **both** | **send** | **receive** }.

Example

# Configure dynamic PW switching.

```
<HUAWEI> system-view
[HUAWEI] mpls switch-l2vc 1.1.1.9 100 between 3.3.3.9 100 encapsulation vlan
```

# Configure static PW switching.

```
<HUAWEI> system-view
[HUAWEI] mpls switch-l2vc 1.1.1.9 100 trans 100 recv 100 between 3.3.3.9 100 trans 200 recv 200
encapsulation vlan
```

# Configure mixed PW switching.

```
<HUAWEI> system-view
[HUAWEI] mpls switch-l2vc 1.1.1.9 100 between 3.3.3.9 100 trans 200 recv 200 encapsulation vlan mtu
1500
```

# Delete PW switching.

```
<HUAWEI> system-view
[HUAWEI] undo mpls switch-l2vc 1.1.1.9 100 encapsulation vlan
```

10.6.32 mtu (PW template view)

Function

The **mtu** command specifies the MTU in a PW template.

The **undo mtu** command restores the default setting.

By default, the MTU in a PW template is 1500.

Format

mtu *mtu-value*

undo mtu

Parameters

Parameter	Description	Value
mtu-value	Specifies the MTU in a PW template.	The value is an integer that ranges from 46 to 9600.

Views

PW template view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When creating a PW template, run the **mtu** command to specify the MTU for the PW template.

Precautions

When creating a Martini VLL or PWE3 VLL, if you set the MTU value by specifying **mtu** *mtu-value* in the **mpls l2vc** command. If you do not specify **mtu** *mtu-value*, the MTU in the PW template takes effect. If you do not specify **mtu** *mtu-value* in the **mpls l2vc** command and do not set the MTU in the PW template, the device uses the default MTU value 1500.

Example

# Configure the MTU for the PW template **pw1**.

```
<HUAWEI> system-view
[HUAWEI] pw-template pw1
[HUAWEI-pw-template-pw1] mtu 1600
```

10.6.33 peer-address

Function

The **peer-address** command assigns a remote IP address to a PW template.

The **undo peer-address** command deletes the remote IP address assigned to a PW template.

By default, a PW template is not configured with a remote IP address.

Format

peer-address *ip-address*

undo peer-address

Parameters

Parameter	Description	Value
ip-address	Specifies the IPv4 address of the peer. Generally, *ip-address* is a loopback address of the peer and needs be the same as the destination address of the tunnel.	The value is in dotted decimal notation.

Views

PW template view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The peer IP address can be set either using a PW template or the **mpls l2vc** command. The PW template allows you to modify the peer IP address in real time. If you want to change the peer IP address using the **mpls l2vc** command, you must delete the existing peer IP address first.

After the peer IP address is changed:

- If the PW template is in use, you must run the **reset pw pw-template** command for the change to take effect. This, however, may disconnect and re-establish the PWs that apply the PW template.
- If the PW template is not in use, it does not need to restart.

Prerequisites

- MPLS L2VPN has been enabled in the system view.
- A PW template has been created in the system view.

Precautions

If the peer IP address has been configured using both a PW template and the **mpls l2vc** command, only the peer IP address configured using the **mpls l2vc** command takes effect.

Example

# Assign a remote IP address to a PW template.

```
<HUAWEI> system-view
[HUAWEI] pw-template pwt
[HUAWEI-pw-template-pwt] peer-address 1.1.1.1
```

# Modify a remote IP address in a PW template.

```
<HUAWEI> system-view
[HUAWEI] pw-template pwt
[HUAWEI-pw-template-pwt] undo peer-address
[HUAWEI-pw-template-pwt] peer-address 2.2.2.2
```

10.6.34 ping vc

Function

The **ping vc** command detects the status of a PW.

Format

ping vc *pw-type pw-id* [*peer-address*] [**-c** *echo-number* | **-m** *time-value* | **-s** *data-bytes* | **-t** *timeout-value* | **-exp** *exp-value* | **-r** *reply-mode* | **-v**] * **control-word** [**remote** *remote-ip-address peer-pw-id* | **draft6**] * [**ttl** *ttl-value*] [**pipe** | **uniform**]

ping vc *pw-type pw-id* [*peer-address*] [**-c** *echo-number* | **-m** *time-value* | **-s** *data-bytes* | **-t** *timeout-value* | **-exp** *exp-value* | **-r** *reply-mode* | **-v**] * **control-word** **remote** *remote-ip-address peer-pw-id* **sender** *sender-address* [**ttl** *ttl-value*] [**pipe** | **uniform**]

ping vc *pw-type pw-id* [*peer-address*] [**-c** *echo-number* | **-m** *time-value* | **-s** *data-bytes* | **-t** *timeout-value* | **-exp** *exp-value* | **-r** *reply-mode* | **-v**] * **label-alert** [**no-control-word**] [**remote** *remote-ip-address* | **draft6**] * [**pipe** | **uniform**]

ping vc *pw-type pw-id* [*peer-address*] [**-c** *echo-number* | **-m** *time-value* | **-s** *data-bytes* | **-t** *timeout-value* | **-exp** *exp-value* | **-r** *reply-mode* | **-v**] * **normal** [**no-**

control-word] [**remote** *remote-ip-address peer-pw-id*] [**ttl** *ttl-value*] [**pipe** | **uniform**]

Parameters

Parameter	Description	Value
pw-type	Specifies the encapsulation type of a local PW.	Currently, PWs of the following types are supported: **ethernet**, **ip-interworking**, and **vlan**.
pw-id	Specifies the ID of a local PW.	The value is an integer that ranges from 1 to 4294967295.
peer-address	Specifies the peer LSR ID of a local PW. In PWE3 and Martini VLL scenarios, if the VC IDs of the primary and secondary VCs are the same, this parameter must be specified to uniquely identify a PW.	The value is in dotted decimal notation.
-c *echo-number*	Specifies the number of Echo Request messages to be sent. If the network works unstably, you can set this parameter to a larger value to test network quality based on the packet loss ratio.	The value is an integer that ranges from 1 to 4294967295. The default value is 5.
-m *time-value*	Specifies the interval for sending Echo Request messages. Each time after the source sends an Echo Request message by using the **ping vc** command, it waits a period of time (2000 ms by default) before sending the next Echo Request message. You can set the interval for sending Echo Request messages through the parameter *time-value*. If the network works unstably, the value should be greater than or equal to 2000 ms.	The value is an integer that ranges from 1 to 10000, in milliseconds. The default value is 2000.
-s *data-bytes*	Specifies the number of bytes of the sent Echo Request messages.	The value is an integer that ranges from 65 to 8100, in bytes. The default value is 100.

Parameter	Description	Value
-t *timeout-value*	Specifies the timeout period for sending Echo Request messages.	The value is an integer that ranges from 0 to 65535, in milliseconds. The default value is 2000.
-exp *exp-value*	Specifies the EXP value of the sent Echo Request messages. **NOTE** If DSCP priority has been configured by running the **set priority** command, the *exp-value* parameter does not take effect.	The value is an integer that ranges from 0 to 7. The default value is 0.
-r *reply-mode*	Specifies the mode in which the peer returns MPLS Echo Reply messages. ● 1: No MPLS Echo Reply message is returned. ● 2: MPLS Echo Reply messages are encapsulated into IPv4/IPv6 UDP packets. ● 3: MPLS Echo Reply messages are encapsulated into IPv4/IPv6 UDP packets carrying the Router Alert option. ● 4: MPLS Echo Reply messages are returned through the control channel of the application plane.	The value is an integer that ranges from 1 to 4. The default value is 2.
-v	Displays the detailed information.	-
no-control-word	Disables the control word function.	-
control-word	Enables the control word function. The switching node along a multi-segment PW does not transmit ping packets. When the control word function is enabled, you can ping only the termination node of the PW. Before using the control word to ping the PW, you must enable the control word for a PW.	-

Parameter	Description	Value
remote	Specifies information about the PW on the remote PE. Information specified by the remote PE is finally encapsulated into the ping packets. The PW can be searched on the remote PE based on the specified information. By default, information contained in the ping packets is the information about the PW on the local end, which applies to single-segment PWs.	-
peer-pw-id	Specifies the ID of the PW on the peer.	The value is an integer that ranges from 1 to 4294967295. By default, the peer PW ID is the same as the local PW ID.
draft6	Specifies the command version. If this parameter is specified, the ping operation is performed based on "draft-ietf-mpls-lsp-ping-06". By default, the ping operation is performed based on RFC 4379.	-
pipe	Specifies the pipe mode. When a probe packet passes through the MPLS domain, the entire MPLS domain is considered as one hop and the IP TTL of the probe packet is reduced by one on the ingress and egress respectively.	-
uniform	Specifies the uniform mode. The IP TTL of the probe packet is reduced by one each time it passes through one hop in the MPLS domain.	-

Parameter	Description	Value
remote-ip-address	Specifies the remote IP address. By default, the system searches for the IP address of the next hop based on the PW on the local PE. In the case of a multi-segment PW, if the ping operation is performed in control word mode, the IP address of the termination node must be specified. In MPLS router alert mode, the IP address of any switching node or the termination node can be specified. Then, the Echo Request message is sent to the peer and then sent back.	-
label-alert	Specifies the label alert mode. The switching node along a multi-segment PW sends ping packets forcibly. In MPLS router alert mode, you can ping any switching node along the PW.	-
normal	Specifies the normal mode, that is, the TTL detection mode. In this mode, control word and router alert are not encapsulated in to MPLS Echo Request messages, and TTL values are used to detect PW connectivity.	-
ttl *ttl-value*	Specifies the TTL value.	The value is an integer that ranges from 1 to 255. The default value is 64.
sender *sender-address*	Specifies a source address. For end-to-end detection of a multi-segment PW, a source IP address needs to be specified for a public network device that communicates with the remote PE. Generally, the source IP address is the address of the adjacent SPE or UPE.	-

Views

All views

Default Level

0: Visit level

Usage Guidelines

Usage Scenario

If a PW is Up, the **ping vc** command can be used to locate the fault on the PW. For example, a forwarding entry is abnormally lost or incorrect.

The **ping vc** command can be used to check a PW in the following scenarios:

VLL networking

Based on VLL types, the VLL PW ping can be classified into the following types:

- PWE3 VLL PW ping: In a PWE3 VLL networking, a PW ping is initiated to check the connectivity of a PW. A PWE3 VLL PW ping can be performed in control word mode, TTL mode, or label alert mode. In a ping test, a local PE sends an Echo Request message to the peer PE. After receiving the message, the peer PE abstracts and sends FEC information to the L2VPN module to determine whether the message has reached the egress. If so, the peer PE returns an Echo Reply message.
- Kompella VLL PW ping: A VLL PW ping is initiated to check the connectivity of a PW. Different from the PWE3 networking, the Kompella VLL does not need the PW template and supports the control word, TTL, and label alert modes.

VPLS networking

Based on the VPLS types, the VPLS PW ping can be classified into the following types:

- Martini VPLS PW ping: The Martini VPLS PW ping supports only the label alert mode. On a Hierarchical Virtual Private LAN Service (HVPLS) network, the Martini VPLS PW ping can only detect single-segment PWs. If an optional PW ID is configured and specified, the PW with the PW ID is detected. If the PW ID is not specified, the PW with a specified VSI ID is detected.
- Kompella VPLS PW ping: The Kompella VPLS PW ping supports only the label alert mode.

If a PW fault is detected by using the **ping vc** command, the **tracert vc** command can be used to locate the fault. Both the **ping vc** command and the **tracert vc** command can properly check the connectivity of PWs and locate faults.

Prerequisites

The MPLS module has been enabled on the device and works properly.

Precautions

control-word is recommended to detect the entire PW. Even though **label-alert** can be used to check the entire PW, the whole process is the same as the forwarding process only when **control-word** is used.

The execution of the **ping vc** command terminates when either of the following situations occurs:

- The ping packet reaches the egress.
- The TTL value of the ping packet reaches the upper threshold.

When a PE is single-homed to an SPE and two multi-segment PWs are deployed for PW redundancy, end-to-end detection cannot be performed for the secondary

PW if services are transmitted over the primary PW. If services are transmitted over the secondary PW, the primary PW can only be detected segment by segment.

Example

# Run the **ping vc** command in label alert mode on the device to check the connectivity of an Ethernet PW.

```
<HUAWEI> ping vc ethernet 100 -c 10 -m 10 -s 65 -t 100 -v label-alert remote 2.2.2.2
   Reply from 2.2.2.2: bytes=65 Sequence=1 time = 31 ms Return Code 3, Subcode 1
   Reply from 2.2.2.2: bytes=65 Sequence=2 time = 15 ms Return Code 3, Subcode 1
   Reply from 2.2.2.2: bytes=65 Sequence=3 time = 32 ms Return Code 3, Subcode 1
   Reply from 2.2.2.2: bytes=65 Sequence=4 time = 15 ms Return Code 3, Subcode 1
   Reply from 2.2.2.2: bytes=65 Sequence=5 time = 32 ms Return Code 3, Subcode 1
   Reply from 2.2.2.2: bytes=65 Sequence=6 time = 15 ms Return Code 3, Subcode 1
   Reply from 2.2.2.2: bytes=65 Sequence=7 time = 15 ms Return Code 3, Subcode 1
   Reply from 2.2.2.2: bytes=65 Sequence=8 time = 16 ms Return Code 3, Subcode 1
   Reply from 2.2.2.2: bytes=65 Sequence=9 time = 15 ms Return Code 3, Subcode 1
   Reply from 2.2.2.2: bytes=65 Sequence=10 time = 32 ms Return Code 3, Subcode 1

--- FEC: FEC 128 PSEUDOWIRE (NEW). Type = ethernet, ID = 100 ping statistics
   10 packet(s) transmitted
   10 packet(s) received
   0.00% packet loss
   round-trip min/avg/max = 15/21/32 ms
```

10.6.35 pw-template

Function

The **pw-template** command creates a PW template. In the PW template, you can set attributes for a PW, such as the peer, control word, and tunnel policy.

The **undo pw-template** command deletes a PW template.

By default, no PW template is created.

Format

pw-template *pw-template-name*

undo pw-template *pw-template-name*

Parameters

Parameter	Description	Value
pw-template-name	Specifies the PW template name.	The value is a string of 1 to 19 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Importing a PW template simplifies the configuration of PWs with similar attributes.

Prerequisites

L2VPN has been enabled by running the **mpls l2vpn** command.

Precautions

- If a PW template is applied to a PW, the PW template cannot be deleted.
- When a PW template is applied to a PW, the PW uses the PW attributes specified on the interface if the PW attributes specified on the interface are different from those specified in the template.
- When modifying attributes in a PW template, run the **reset pw** command to make the modification take effect. This will cause PW disconnection and reconnection.
- After a PW is bound to a link detection protocol, the remote IP address in the PW template cannot be changed. To change the remote IP address, unbind the PW from the link detection protocol.

Example

# Create a PW template named **pwt1**.

```
<HUAWEI> system-view
[HUAWEI] pw-template pwt1
[HUAWEI-pw-template-pwt1]
```

10.6.36 reset pw

Function

The **reset pw** command re-creates a PW or a PW template.

Format

reset pw { [**peer-address** *peer-address*] *pw-id pw-type* | **pw-template** *pw-template-name* }

Parameters

Parameter	Description	Value
peer-address *peer-address*	Specifies the IPv4 address of the target PE.	The value is in dotted decimal notation.

Parameter	Description	Value
pw-id	Specifies the ID of a VC connected to L2VPN.	The value is an integer that ranges from 1 to 4294967295.
pw-type	Specifies the encapsulation type of a PW.	Currently, PWs of the following types are supported: **ethernet**, **vlan**, and **ip-interworking**.
pw-template	Re-creates all PWs in the PW template.	-
pw-template-name	Specifies the PW template name.	The value is an existing PW template name.

Views

User view

Default Level

2: Configuration level

Usage Guidelines

After changing the parameters in a PW template, you need to run the **reset pw pw-template** command to make the modification take effect. The configuration on the PW template applies to all PWs using this PW template. You can configure the attributes of a PW by using a PW template or commands. The attributes configured by using commands take precedence over those configured by using the template. If you configure PW attributes by using commands, the corresponding attributes in the PW template do not take effect. Therefore, if you run the **reset pw pw-template** and **reset pw** *pw-id* commands, the PW attributes remain unchanged. To change a PW attribute, configure the attribute in the PW template but do not configure attribute by using a command.

Example

# Re-create a PW by specifying the VC ID and VC type.

```
<HUAWEI> reset pw 100 vlan
```

# Re-create all PWs that use the PW template named **pwt1**.

```
<HUAWEI> reset pw pw-template pwt1
```

10.6.37 tnl-policy (PW template view)

Function

The **tnl-policy** command configures a tunnel policy for a PW template.

The **undo tnl-policy** command deletes the tunnel policy configured for a PW template.

By default, no tunnel policy is configured for a PW template.

Format

tnl-policy *policy-name*

undo tnl-policy

Parameters

Parameter	Description	Value
policy-name	Specifies the tunnel policy name of a PW.	The value is a string of 1 to 39 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Views

PW template view

Default Level

2: Configuration level

Usage Guidelines

The **tnl-policy** command specifies a PWE3 tunnel policy based on which a PW selects a tunnel to be associated with.

If no policy is configured, an LSP tunnel is selected and load balancing is not performed.

Example

# Configure a tunnel policy named **policy1** for a PW template named **pwt**.

```
<HUAWEI> system-view
[HUAWEI] pw-template pwt
[HUAWEI-pw-template-pwt] tnl-policy policy1
```

10.6.38 tracert vc

Function

The **tracert vc** command detects the status of a PW or locates a faulty node on a PW in Down state.

Format

tracert vc *pw-type pw-id* [*peer-address*] [**-exp** *exp-value* | **-f** *first-ttl* | **-m** *max-ttl* | **-r** *reply-mode* | **-t** *timeout-value*] * **control-word** [**draft6**] [**full-lsp-path**] [**pipe** | **uniform**]

tracert vc *pw-type pw-id* [*peer-address*] [**-exp** *exp-value* | **-f** *first-ttl* | **-m** *max-ttl* | **-r** *reply-mode* | **-t** *timeout-value*] * **control-word remote** *remote-ip-address* [**ptn-mode** | **full-lsp-path**] [**pipe** | **uniform**]

tracert vc *pw-type pw-id* [*peer-address*] [**-exp** *exp-value* | **-f** *first-ttl* | **-m** *max-ttl* | **-r** *reply-mode* | **-t** *timeout-value*] * **control-word remote** *remote-pw-id* **draft6** [**full-lsp-path**] [**pipe** | **uniform**]

tracert vc *pw-type pw-id* [*peer-address*] [**-exp** *exp-value* | **-f** *first-ttl* | **-m** *max-ttl* | **-r** *reply-mode* | **-t** *timeout-value*] * **label-alert** [**no-control-word**] [**remote** *remote-ip-address*] [**full-lsp-path**] [**draft6**] [**pipe** | **uniform**]

tracert vc *pw-type pw-id* [*peer-address*] [**-exp** *exp-value* | **-f** *first-ttl* | **-m** *max-ttl* | **-r** *reply-mode* | **-t** *timeout-value*] * **normal** [**no-control-word**] [**remote** *remote-ip-address*] [**full-lsp-path**] [**draft6**] [**pipe** | **uniform**]

Parameters

Parameter	Description	Value
pw-type	Specifies the PW type.	Currently, PWs of the following types are supported: **ethernet**, **vlan**, and **ip-interworking**.
pw-id	Specifies the local PW ID.	The value is an integer that ranges from 1 to 4294967295.
peer-address	Specifies a peer LSR ID for the local PW. In a PWE3 or Martini VLL scenario, if the primary and secondary VCs are configured with the same VC ID, this parameter must be specified to determine a unique PW to be monitored.	The value is in dotted decimal notation.
-exp *exp-value*	Specifies the EXP value in the outer label of an MPLS Echo Request packet. The default value is 0. **NOTE** If DSCP priority has been configured by running the **set priority** command, the *exp-value* parameter does not take effect.	The value is an integer that ranges from 0 to 7.

Parameter	Description	Value
-f *first-ttl*	Specifies the initial Time-to-Live (TTL).	The value is an integer that ranges from 1 to 255, and must be smaller than the value of *max-ttl*. The default value is 1.
-m *max-ttl*	Specifies the maximum TTL.	The value is an integer that ranges from 1 to 255, and must be larger than the value of *first-ttl*. The default value is 30.
-r *reply-mode*	Specifies the mode in which the peer returns MPLS Echo Reply packets. ● 1: No MPLS Echo Reply packet is returned. ● 2: The MPLS Echo Reply packet is encapsulated in IPv4/IPv6 UDP packets. ● 3: MPLS Echo Reply packets are encapsulated in IPv4/IPv6 /IPv6 UDP packets carrying the Router Alert option. ● 4: MPLS Echo Reply packets are returned through the control channel of the application plane.	The value is an integer that ranges from 1 to 4.
-t *timeout-value*	Specifies the timeout interval of an MPLS Echo Reply packet.	The value is an integer that ranges from 0 to 65535, in milliseconds. The default value is 5.
control-word	Indicates that the control word is encapsulated in the MPLS Echo Request packet.	-
label-alert	Indicates that the router alert label is encapsulated in the MPLS Echo Request packet.	-

Parameter	Description	Value
no-control-word	Indicates that the control word is not encapsulated in the MPLS Echo Request packet.	-
normal	Indicates the normal mode where the router alert label and control word are not encapsulated in the MPLS Echo Request packet.	-
remote	Specifies information about the PW on the remote PE.	-
remote-ip-address	Specifies the remote IP address. By default, the system searches for the IP address of the next hop based on the PW on the local PE. If **label-alert** is configured, you can specify the IP address of any switching node or the termination node.	-
remote-pw-id	Specifies the ID of the remote PW. By default, the ID of the local PW is used. If the tracert operation is performed in control word mode for a multi-segment PW, the IP address of the termination node must be specified.	-
ptn-mode	Specifies the PTN mode. In a multi-segment PW scenario, this parameter is indicated that trace VC packets are replied. You need to run the **lspv pw reply ptn-mode** command on both the SPE and TPE.	-
full-lsp-path	Displays the responses from all nodes along the LSP that the MPLS Echo Request packets pass through. If this parameter is not specified, only the responses from the PW nodes along the LSP are displayed.	-
pipe	Specifies the pipe mode. When a probe packet passes through the MPLS domain, the entire domain is regarded as one hop and the IP TTL of the probe packet is reduced by one on both the ingress and egress.	-

Parameter	Description	Value
uniform	Specifies the uniform mode. The IP TTL of the probe packet is reduced by one each time it passes through one hop in the MPLS domain.	-
draft6	Specifies the version of the **tracert vc** command. If this parameter is specified, the tracert operation is performed according to "draft-ietf-mpls-lsp-ping-06". By default, the tracert operation is performed according to RFC 4379. **NOTE** Tracert VC based on **draft6** is applied only to VLL over LDP scenarios.	-

Views

All views

Default Level

0: Visit level

Usage Guidelines

Usage Scenario

If a fault occurs on the PW, the **ping vc** command can be used to check the connectivity of the network, and the **tracert vc** command can be used to locate the fault and provide reference for fault diagnosis. If a PW is Up, the **ping vc** command can be used to locate the fault on the PW. For example, a forwarding entry is abnormally lost or incorrect. If a PW is down, the **tracert vc** command must be used to locate the faulty node on the PW.

The **tracert vc** command applies to the following networking scenarios:

- PWE3 VLL PW tracert

  In PWE3 VLL networking, PW tracert can help you obtain information about SPEs and Ps along the path that the message travels from the source to the destination, check the connectivity of the PW, and locate the fault of the PW.

  A PWE3 VLL PW tracert can be performed in control word mode, label alert mode, or TTL mode. The default mode is label alert. The TTL mode and control word mode are mutually exclusive.

  To detect faults on a VLL network with control word enabled, run the **tracert vc** *pw-type pw-id* **control-word** command.

  To encapsulate packets with the router alert label and detect faults on a VLL network, run the **tracert vc** *pw-type pw-id* **label-alert** command.

  If control word is not enabled and packets are not encapsulated with the router alert label, to detect faults on a VLL network, run the **tracert vc** *pw-type pw-id* command.

The TTL value of the PW Tracert Request message is incremented by 1 each time. Each time the transit node (P) receives an Echo Request message after the TTL value of the message expires, it sends the Echo Request message to the LSPV module. Then the transit node returns an Echo Reply message carrying the next hop information.

Prerequisite

- The UDP module of each node works properly; otherwise, the tracert operation will fail.
- The MPLS module has been enabled on each node and works properly.
- The ICMP module of each node works properly; otherwise, " * * * " is displayed.

Procedure

The execution process of the **tracert vc** command is as follows:

1. The source sends an MPLS Echo Request packet with the TTL being 1. After the TTL times out, the first hop sends an MPLS Echo Reply packet to the source.
2. The source sends an MPLS Echo Request packet with the TTL being 2. After the TTL times out, the second hop sends an MPLS Echo Reply packet to the source.
3. The source sends an MPLS Echo Request packet with the TTL being 3. After the TTL times out, the third hop sends an MPLS Echo Reply packet to the source.
4. The preceding steps continue until the MPLS Echo Request packet reaches the destination.

When the device on each hop receives the MPLS Echo Request packet, it will respond with an MPLS Echo Reply packet, indicating that the tracert test ends. In the command output information of the source device, you can view the path that the packet passes through.

Configuration Impact

In control word mode, if a transit node receives an MPLS Echo Request packet whose TTL does not time out, it does not send the packet to the CPU. In this mode, the source obtains only a little PW information and cannot obtain information about the downstream devices of the transit node. This mode is recommended when the traffic volume is heavy.

In router alert mode, a transit node sends the received MPLS Echo Request packets to the CPU. In this mode, the source obtains a lot of PW information; therefore, device performance is affected when the traffic volume is heavy. This mode is recommended when the traffic volume is light.

Information specified by **remote** is encapsulated in MPLS Echo Request packets. The PW can be searched on the remote PE based on the specified information. By default, information contained in the MPLS Echo Request packets is about the PW on the local PE. This applies to single-segment PWs.

Precautions

- When the probe packet reaches the egress or the TTL reaches the upper threshold, the PW tracert is terminated.

- You can press **Ctrl + C** to terminate the execution of the **tracert vc** command.

When a PE is single-homed to an SPE and two multi-segment PWs are deployed for PW redundancy, end-to-end detection cannot be performed for the secondary PW if services are transmitted over the primary PW. If services are transmitted over the secondary PW, the primary PW can only be detected segment by segment.

Example

# Trace a multi-segment PW. The encapsulation type, local PW ID, and remote PW ID of the PW is ethernet, 100, and 200.

```
<HUAWEI> tracert vc ethernet 100 control-word remote 200 draft6 full-lsp-path
 TTL   Replier          Time    Type      Downstream
 0                           Ingress    10.1.1.2/[1025 ]
 1     10.1.1.2         230 ms  Transit   10.2.1.2/[3 ]
 2     10.2.1.2         230 ms  Transit   10.3.1.2/[3 ]
 3     10.3.1.2         100 ms  Transit   10.4.1.2/[3 ]
 4     10.4.1.2         150 ms  Egress
```

Table 10-89 Description of the **tracert vc** command output

Item	Description
TTL	TTL value in an Echo Request packet. It represents the number of hops along the path through which an Echo Request packet passes.
Replier	IP address of the node sending MPLS Echo Reply packets.
Time	Time when the packet is processed.
Type	Node type. The value can be: ● Ingress: indicates an ingress node. ● Transit: indicates a transit node. ● Egress: indicates an egress node.
Downstream	IP address and label of the downstream node.

10.7 VPLS Configuration Commands

10.7.1 Command Support

Only the following switch models support VPLS:

S5731-S, S5731-H, S5731S-H, S5732-H, S6720-EI, S6720S-EI, S6730-S, S6730S-H, and S6730-H

10.7.2 broadcast-suppression cir cbs (VSI view)

Function

The **broadcast-suppression cir cbs** command enables the broadcast traffic suppression function in a VSI.

The **undo broadcast-suppression** command disables the broadcast traffic suppression function in the VSI.

By default, the broadcast traffic suppression function is disabled in a VSI.

Format

broadcast-suppression cir *cir-value* **cbs** *cbs-value*

undo broadcast-suppression

Parameters

Parameter	Description	Value
cir *cir-value*	Specifies the Committed Information Rate (CIR), that is, the allowed rate at which traffic can pass through.	The value is an integer that ranges from 0 to 10000000, in kbit/s.
cbs *cbs-value*	Specifies the Committed Burst Size (CBS), that is, the traffic that can pass instantly, or the depth of the first token bucket.	The value is an integer that ranges from 10000 to 4294967295, in bytes.

Views

VSI view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On a VPLS network, broadcast packets, multicast packets, and unknown unicast packets are transmitted in broadcast mode and copied to neighboring ACs and PWs. If a large number of broadcast packets are sent to the access device on the network, the device has to make a lot of copies of these broadcast packets, which wastes bandwidth and resources, and degrades the performance of the system. You can run the **broadcast-suppression cir cbs** command to suppress the broadcast traffic in the VSI. The rate of broadcast traffic on the VPLS network is limited.

Prerequisites

A VSI has been created using the **vsi** *vsi-name* [**auto** | **static**] command.

Precautions

The **broadcast-suppression cir cbs** command can be configured in a maximum of 100 VSIs.

Example

# Set the CIR to 100 kbit/s and the CBS to 18800 bytes for the broadcast traffic that can pass in **VSI1**.

```
<HUAWEI> system-view
[HUAWEI] vsi VSI1
[HUAWEI-vsi-VSI1] broadcast-suppression cir 100 cbs 18800
```

10.7.3 bfd bind pw vsi

Function

The **bfd bind pw vsi** command configures a BFD session on a non-SPE node to detect a PW.

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

By default, no BFD session is configured to detect the PW.

Format

bfd *cfg-name* **bind pw vsi** *vsi-name* **peer** *peer-address* [**vc-id** *vc-id*] [**remote-peer** *remote-peer-address* **pw-ttl** { **auto-calculate** | *ttl-number* }]

undo bfd *cfg-name*

Parameters

Parameter	Description	Value
cfg-name	Specifies the name of a BFD session.	The value is a string of 1 to 15 case-insensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Parameter	Description	Value
vsi *vsi-name*	Specifies the name of a VSI.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
peer *peer-address*	Specifies the destination IP address of the VPLS PW, which is usually the LSR ID.	The value is in dotted decimal notation.
vc-id *vc-id*	Specifies the ID of a Layer 2 VC.	The value is an integer ranging from 1 to 4294967295.
remote-peer *remote-peer-address*	Specifies the IP address used as the destination address of the PW to be detected by a BFD session, which is usually the LSR ID.	The value is in dotted decimal notation. It cannot be in the format of 127.X.X.X.
pw-ttl	Indicates the BFD session detects the PW in TTL mode.	-
auto-calculate	Indicates that the number of hops along a PW is counted automatically.	-
ttl-number	Specifies the number of hops along the PW to be detected.	The value is an integer ranging from 1 to 255.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

BFD sessions can rapidly detect links on the network. You can run the **bfd bind pw vsi** command to detect a single-hop VPLS PW or a multi-hop PW formed by connecting a VPLS PW to a VLL PW. The **bfd bind pw vsi** command detects the VPLS PW in unicast mode and specifies the VPLS PW to be detected through the parameter **peer** *peer-address*.

- If the configured BFD session is used to detect an end-to-end single-hop VPLS PW, the value of **peer** *peer-address* and the value of **remote-peer** *remote-peer-address* are identical. In this case, you can run the **bfd** *cfg-name* **bindpw vsi** *vsi-name* **peer** *peer-address* command only. The TTL value is 255.
- If the BFD session is used to detect a multi-hop PW formed by connecting a VPLS PW to a VLL PW, you need to specify the destination IP address of the VPLS PW through **peer** *peer-address* and the destination IP address of the multi-hop PW through **remote-peer** *remote-peer-address*.
  - If **auto-calculate** is specified, the system automatically counts the number of hops along the PW to be detected based on **remote-peer** *remote-peer-address*.
  - If **ttl** *ttl-number* is specified, the number of hops along the PW to be detected is manually set.

NOTE

When running the **bfd bind pw vsi** command to detect a multi-hop PW, ensure that the first-hop PW is the VPLS PW, which must be configured on a non-SPE node.

When running the **bfd bind pw vsi** command to detect a single-hop VPLS PW, ensure that the single-hop VPLS PW is configured on a non-SPE node.

If VPLS forwards data through TE tunnels, PW detection using a BFD session is not supported.

Prerequisites

The PW to be detected must exist. The BFD session must be established between the source and destination of the PW.

Before running the **bfd bind pw vsi** command, ensure that the following configuration operations have been performed:

- The BFD function has been enabled globally through the **bfd** command.
- A single-hop VPLS PW or multi-hop PW formed by connecting a VPLS PW to a VLL PW has been created.

Precautions

This command is used to configure a BFD session to detect a VPLS PW only in TTL mode.

Example

# Configure a BFD session on a non-SPE node to detect the VPLS PW in TTL mode.

```
<HUAWEI> system-view
[HUAWEI] bfd
[HUAWEI-bfd] quit
[HUAWEI] bfd vplspw bind pw vsi vsi1 peer 2.2.2.2 vc-id 123 remote-peer 3.3.3.3 pw-ttl auto-calculate
```

10.7.4 bfd for vsi-pw enable

Function

The **bfd for vsi-pw enable** command enables the device to send BFD for VSI-PW packets to the protocol stack.

The **undo bfd for vsi-pw enable** command disables the device from sending BFD for VSI-PW packets to the protocol stack.

By default, the device does not send BFD for VSI-PW packets to the protocol stack, but discards or forwards the packets.

Format

bfd for vsi-pw enable

undo bfd for vsi-pw enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When performing BFD for VSI PW, the device needs to send BFD for VSI-PW packets to the protocol stack. Therefore, the **bfd for vsi-pw enable** command must be run.

Precautions

If you run the **undo bfd for vsi-pw enable** command to disable the device from sending BFD for VSI-PW packets to the protocol stack, the BFD for VSI-PW packets are discarded or forwarded. The **bfd for vsi-pw enable** command and other BFD commands can be run in any sequence.

After the **bfd for vsi-pw enable** command is run in the system view, the BFD for VSI-PW packets are sent to the protocol stack. If this command is not run, the BFD for VSI PW packets are discarded or forwarded, and the BFD for VSI PW function does not take effect.

Example

# Enable the device to send BFD for VSI-PW packets to the protocol stack.

```
<HUAWEI> system-view
[HUAWEI] bfd for vsi-pw enable
```

# Disable the device from sending BFD for VSI-PW packets to the protocol stack.

```
<HUAWEI> system-view
[HUAWEI] undo bfd for vsi-pw enable
```

10.7.5 bgp-ad

Function

The **bgp-ad** command displays the BGP-AD view.

Format

bgp-ad

Parameters

None

Views

VSI view

Default Level

2: Configuration level

Usage Guidelines

To establish the BGP-AD VSI, you need to run the **bgp-ad** command in the VSI view to display the BGP-AD view. In the BGP-AD view, you can configure parameters such as VPLS-ID and VPN-Target.

Example

# Enter the BGP-AD view.

```
<HUAWEI> system-view
[HUAWEI] vsi v100
[HUAWEI-vsi-v100] bgp-ad
[HUAWEI-vsi-v100-bgpad]
```

10.7.6 description (VSI view)

Function

The **description** command configures the description of a Virtual Switch Instance (VSI).

The **undo description** command deletes the description of a VSI.

By default, no description of the VSI is configured.

Format

description *description*

undo description

Parameters

Parameter	Description	Value
description	Specifies the description of a VSI.	The value is a string of 1 to 64 case-sensitive characters with spaces.

Views

VSI view

Default Level

2: Configuration level

Usage Guidelines

The **description** command can be used to identify different VSIs or describe the functions of VSIs.

Example

# Configure the description of the current VSI.

```
<HUAWEI> system-view
[HUAWEI] vsi v100
[HUAWEI-vsi-v100] description vsi for company1
```

10.7.7 display bgp l2vpn-ad routing-table

Function

The **display bgp l2vpn-ad routing-table** command displays BGP L2VPN-AD routes.

Format

display bgp l2vpn-ad [**route-distinguisher** *route-distinguisher*] **routing-table** [**vpls-ad**] [*ipv4-address* | **statistics**]

display bgp l2vpn-ad routing-table peer *ipv4-address* **advertised-routes** [**vpls-ad**] [*ipv4-address* | **statistics**]

display bgp l2vpn-ad routing-table peer *ipv4-address* **received-routes** [**active**] [**statistics**]

display bgp l2vpn-ad routing-table vpws route-distinguisher *route-distinguisher* [**ce-id** *ce-id* [**label-offset** *label-offset*]]

display bgp l2vpn-ad routing-table { **vpws** | **vpls** | **all** } [**statistics**]

display bgp l2vpn-ad routing-table peer *ipv4-address* **advertised-routes vpls-ad** *ipv4-address*

display bgp l2vpn-ad routing-table peer *ipv4-address* **received-routes vpls-ad** [**active**] [**statistics**]

display bgp l2vpn-ad routing-table vpls route-distinguisher *route-distinguisher* [**site-id** *site-id* [**label-offset** *label-offset*]]

display bgp l2vpn-ad routing-table peer *ipv4-address* **received-routes** { **vpws** | **vpls** | **all** } [**statistics**]

display bgp l2vpn-ad routing-table peer *ipv4-address* **advertised-routes vpws** [**statistics** | **route-distinguisher** *route-distinguisher* **ce-id** *ce-id* **label-offset** *label-offset*]

display bgp l2vpn-ad routing-table peer *ipv4-address* **advertised-routes vpls** [**statistics** | **route-distinguisher** *route-distinguisher* **site-id** *site-id* **label-offset** *label-offset*]

display bgp l2vpn-ad routing-table peer *ipv4-address* **advertised-routes all** [**statistics**]

display bgp l2vpn-ad routing-table peer *ipv4-address* **received-routes vpls-ad** *network*

display bgp l2vpn-ad routing-table peer *ipv4-address* **received-routes vpws route-distinguisher** *route-distinguisher* **ce-id** *ce-id* **label-offset** *label-offset*

display bgp l2vpn-ad routing-table peer *ipv4-address* **received-routes vpls route-distinguisher** *route-distinguisher* **site-id** *site-id* **label-offset** *label-offset*

Parameters

Parameter	Description	Value
route-distinguisher *route-distinguisher*	Displays BGP L2VPN-AD routing information of the specified RD.	-
ipv4-address	Specifies the IPv4 network address.	-
statistics	Display the statistics of the BGP L2VPN-AD routes.	-
peer	Displays the routing information for the specified BGP peer.	-
advertised-routes	Displays the routes advertised to the specified peer.	-
received-routes	Displays the routes received from the specified peer.	-
active	Displays the active routes received from the specified peer.	-

Parameter	Description	Value
network	Specifies the IPv4 network address.	-
vpls-ad	Displays VPLS-AD route information.	-
vpws	Displays VPWS route information.	-
vpls	Displays VPLS route information.	-
all	Displays information about all types of routes.	-
ce-id *ce-id*	Specifies the CE ID.	The value is a decimal integer ranging from 0 to 65535.
site-id *site-id*	Specifies the site ID of a VSI.	The value is a decimal integer ranging from 0 to 65535.
label-offset *label-offset*	Specifies the offset of a label.	The value is a decimal integer ranging from 0 to 65535.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can specify different parameters to view the specific routing information.

Example

# Display all the BGP L2VPN-AD routing information.

```
<HUAWEI> display bgp l2vpn-ad routing-table


 Local AS number : 100
 BGP Local router ID is 10.1.150.122
 Status codes: * - valid, > - best, d - damped,
               h - history,  i - internal, s - suppressed, S - Stale
               Origin : i - IGP, e - EGP, ? - incomplete



 Total number of routes from all PE: 2
 Route Distinguisher: 1:1


      Network            NextHop        MED        LocPrf    PrefVal Path/Ogn

 *>   1.1.1.9/32         0.0.0.0                              0      ?
 *>i  3.3.3.9/32         3.3.3.9                   100        0      ?
```

# Display the detailed routing information of a specified route.

```
<HUAWEI> display bgp l2vpn-ad routing-table 3.3.3.9


 BGP local router ID : 10.1.150.122
 Local AS number : 100

 Total routes of Route Distinguisher(1:1): 1
 BGP routing table entry information of 3.3.3.9/32:
 From: 3.3.3.9 (192.2.2.2)
 Route Duration: 00h02m09s
 Relay IP Nexthop: 172.1.1.1
 Relay IP Out-Interface: Vlanif30
 Original nexthop: 3.3.3.9
 Qos information : 0x0
 Ext-Community:RT <100 : 1>, Layer2 Info <1 : 1>
 AS-path Nil, origin incomplete, localpref 100, pref-val 0, valid, internal, bes
t, select, pre 255, IGP cost 1
 Not advertised to any peer yet
```

# Display VPLS route information.

```
<HUAWEI> display bgp l2vpn-ad routing-table vpls

 BGP Local router ID is 10.1.0.3
 Status codes: * - valid, > - best, d - damped,
               h - history,  i - internal, s - suppressed, S - Stale


 Total Number of Routes: 2
      Network(RD/Site-ID/LabelOffset)        NextHop

 *>i  100:1/1/0                              1.1.1.1
 *>   100:2/2/0                              0.0.0.0
```

# Display information about VPLS routes received from 1.1.1.1.

```
<HUAWEI> display bgp l2vpn-ad routing-table peer 1.1.1.1 received-routes vpls

 BGP Local router ID is 10.1.0.3
 Status codes: * - valid, > - best, d - damped,
               h - history,  i - internal, s - suppressed, S - Stale


 Total Number of Routes: 1
      Network(RD/Site-ID/LabelOffset)        NextHop

 *>i  100:1/1/0                              1.1.1.1
```

Table 10-90 Description of the display bgp l2vpn-ad routing-table command output

Item	Description
Network	Network address in the BGP routing table
NextHop	Next Hop address through which the packet has to be sent
MED	Multi-Exit discriminator
LocPrf	Local preference
PrefVal	Value preferred by the protocol
Path/Ogn	AS-Path number and the attributes of Origin
BGP Local router ID	ID of the local BGP device. The ID is in the same format as an IPv4 address.
Local AS number	Local AS number.
Total routes of Route Distinguisher	Total number of L2VPN-AD routes with a specified RD.
BGP routing table entry information of x.x.x.x/x	The following information is about a specified BGP routing entry.
From	IP address of the route originator.
Route Duration	Route duration.
Relay IP Nexthop	Recursive next-hop IP address.
Relay IP Out-Interface	Recursive outbound interface.
Original nexthop	Original next hop.
Qos information	QoS information. ● 0x20000000: indicates that the **apply behavior** command has been run. ● 0x40000001–0x40000FFF: indicates that the **apply qos-local-id** *qos-local-id* command has been run and the *qos-local-id* varies from 1 to 4095. ● 0x80000001–0x80000007: indicates that the **apply ip-precedence** *precedence* command has been run and the *precedence* varies from 1 to 7. ● 0x0: indicates that the preceding QoS configurations are not performed.
Ext-Community	Extended community attribute of BGP.

Item	Description
AS-path	AS_Path attribute. **Nil** indicates that the attribute value is null.
origin	Origin attribute of the BGP route. ● IGP: The routes imported into the BGP routing table by using the **network** command. ● EGP: The routes are obtained by EGP. ● Incomplete: The origin of the routes cannot be determined, for example, the routes imported into the BGP routing table by using the **import-route** command.
localpref	Local preference of the BGP route.
pref-val	Preferred value.
valid	Valid BGP route.
internal	Internal BGP route.
best	The BGP route is the optimal route.
select	The BGP route is a preferred route.
pre 255	The preference of the BGP route is 255.
IGP cost 1	Indicates the IGP cost is 1.
Not advertised to any peer yet	The BGP route has not been advertised to any peer.

# Display detailed information about the specified invalid VPLS-AD routes.

```
<HUAWEI> display bgp l2vpn-ad routing-table 1.1.1.1
 BGP local router ID : 10.1.1.2
 Local AS number : 100

 Total routes of Route Distinguisher(1:1): 1
 BGP routing table entry information of 1.1.1.1/32:
 From: 1.1.1.1 (10.1.1.1)
 Route Duration: 00h00m30s
 Relay IP Nexthop: 10.1.1.1
 Relay IP Out-Interface: GigabitEthernet0/0/0
 Original nexthop: 1.1.1.1
 Qos information : 0x0
 Ext-Community:RT <100 : 1>, Layer2 Info <1 : 1>

 AS-path Nil, origin incomplete, localpref 100, pref-val 0, internal, select, pre 255, invalid for route-policy
not pass
 Not advertised to any peer yet
```

Table 10-91 Description of the display bgp l2vpn-ad routing-table command output

Item	Description
BGP local router ID	ID of the local BGP router. The format is the same as the IPv4 address.
Local AS number	Local AS number.
Total routes of Route Distinguisher(1:1)	The total number of routes with the RD of 1:1.
BGP routing table entry information of 1.1.1.1/32	The following information is about 1.1.1.1/32 routing entries.
From	IP address of the router that sends the route. 10.1.1.1 is the IP address of the source interface of the peer with which the BGP connection is established, and 1.1.1.1 is the Router ID of the peer.
Route Duration	Duration of routes.
Relay IP Nexthop	Recursive next hop.
Relay IP Out-Interface	Recursive outbound interface.
Original nexthop	Original next hop.
Qos information	QoS information. ● 0x20000000: indicates that the **apply behavior** command has been run. ● 0x40000001–0x40000FFF: indicates that the **apply qos-local-id** *qos-local-id* command has been run and the *qos-local-id* varies from 1 to 4095. ● 0x80000001–0x80000007: indicates that the **apply ip-precedence** *precedence* command has been run and the *precedence* varies from 1 to 7. ● 0x0: indicates that the preceding QoS configurations are not performed.
Ext-Community	Extended community attribute.
AS-path Nil	AS_Path attribute, with Nil indicating that the attribute value is null.

Item	Description
origin incomplete	Well-known mandatory property. This property defines the origin of a path and records how a route turns to a BGP route. The property has the following three values: ● IGP: The priority of this value is the highest. The origin property of the routes that are added to the BGP routing table by using the **network (BGP)** command is IGP. ● EGP: The priority of this value is second to that of IGP. The origin property of the routes imported from EGP is EGP. ● Incomplete: The priority of this value is the lowest. The value indicates the origin of a route is unknown. The origin property of the routes that are added to the BGP routing table by using the **import-route (BGP)** command is Incomplete.
localpref	Local priority.
pref-val	Value preferred by the protocol.
internal	The BGP route is an internal route.
select	The BGP route is a preferred route.
pre 255	The priority of the BGP route is 255.
invalid for route-policy not pass	Reason why a route is invalid: ● invalid for route-policy not pass: The route does not match the route-policy. ● invalid for supernet route: The route is a supernet route. ● invalid for IP unreachable: The route fails to recurse to another route. ● invalid for supernet route not advertise: No supernet routes are advertised. ● invalid for supernet label route not advertise: No supernet labeled routes are advertised. ● invalid for next-hop unreachable: The next-hop IP address is unreachable. ● invalid for tunnel unreachable: The route fails to recurse to a tunnel.

Item	Description
Not advertised to any peer yet	The BGP route has not been advertised to any peer yet.

10.7.8 display bgp vpls

Function

The **display bgp vpls** command displays information about VPLS in the BGP routing table.

Format

display bgp vpls { **all** | **route-distinguisher** *route-distinguisher* [**site-id** *site-id* [**label-offset** *label-offset*]] }

Parameters

Parameter	Description	Value
all	Displays all VPLS information in the BGP VPLS address family.	-

Parameter	Description	Value
route-distinguisher *route-distinguisher*	Displays the VSI information about the specified Route Distinguisher (RD). The formats of an RD are as follows: ● 16-bit AS number:32-bit user-defined number: for example, 101:3. An AS number ranges from 0 to 65535, and a user-defined number ranges from 0 to 4294967295. The AS number and user-defined number cannot be both 0. That is, a VPLS ID cannot be 0:0. ● Integral 4-byte AS number:2-byte user-defined number, for example, 65537:3. An AS number ranges from 65536 to 4294967295. A user-defined number ranges from 0 to 65535. The AS number and user-defined number cannot be both 0s. That is, a VPLS ID cannot be 0:0. ● 4-byte AS number in dotted notation:2-byte user-defined number, for example, 0.0:3 or 0.1:0. A 4-byte AS number in dotted notation is in the format of *x.y*, where *x* and *y* are integers that range from 1 to 65535 and from 0 to 65535, respectively. A user-defined number ranges from 0 to 65535. The AS number and user-defined number cannot be both 0s. That is, a VPLS ID cannot be 0.0:0. ● 32-bit IP address:16-bit user-defined number: for example, 192.168.122.15:1. An IPv4 address ranges from 0.0.0.0 to 255.255.255.255, and a user-defined number ranges from 0 to 65535.	-
site-id *site-id*	Displays the VSI of the specified site ID.	The value is an integer that ranges from 0 to 65534.
label-offset *label-offset*	Displays the VSI information about the specified label offset.	The value is an integer that ranges from 0 to 65535.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can specify the parameter values of the command to view required VPLS.

When the output information is excessive, you can run the **display bgp vpls peer** command to view information about the BGP peer in the VPLS, and run the **display bgp vpls group** command to view information about the BGP peer group in the VPLS.

Example

# Display the VPLS with the VSI of the BGP RD as 1.1.1.2:1.

```
<HUAWEI> display bgp vpls route-distinguisher 1.1.1.2:1
BGP Local Router ID : 10.1.1.1, Local AS Number : 100
Status codes : * - active, > - best

--------------------------------------------------------------------------------
Route Distinguisher: 1.1.1.2:1
   SiteID Offset NextHop         Range LabBase TunnelID   FromPeer       MHPref
--------------------------------------------------------------------------------
>  1      0      0.0.0.0         3     35840   0x0        0.0.0.0        0
```

Table 10-92 Description of the display bgp vpls route-distinguisher command output

Item	Description
BGP Local Router ID	ID of the BGP local router. To set the value, run the **router-id** command.
Local AS Number	Local AS number. To set the value, run the **bgp** command.
Status codes	Route status. ● *: active route ● >: best route
Route Distinguisher	RD of the VPN instance. To set the value, run the **route-distinguisher** command.
SiteID	Site ID of the remote VSI. To set the value, run the **site** command.
Offset	Offset of the site ID. The value is 0 or 1 and the default value is 0. To set the value, run the **site** command.
Nexthop	IP address of the next hop.

Item	Description
Range	Range of the number of sites in the VSI. The value is a decimal integer. To set the value, run the **site** command.
LabBase	Start number of the allocated labels.
Tunnel ID	Tunnel ID, which is automatically allocated by the system and is in hexadecimal notation.
FromPeer	IP address of the BGP peer.
MHPref	Multi-homing preference. To set the value, run the **multi-homing-preference** command.

10.7.9 display l2vpn ccc-interface vc-type

Function

The **display l2vpn ccc-interface vc-type** command displays information about the interface used by an L2VPN connection.

Format

display l2vpn ccc-interface vc-type { **all** | *vc-type* } [**down** | **up**]

Parameters

Parameter	Description	Value
all	Displays information about all interfaces of L2VPN connections.	-
vc-type	Specifies the type of the L2VPN connection.	The following types of the L2VPN connection are available: ● ccc: Cross Circuit Connection ● ldp-vc: L2VPN connection in the Martini mode ● static-vc: L2VPN connection in the SVC mode ● bgp-vc: L2VPN connection in the Kompella mode ● vpls-vc: VPLS connection

Parameter	Description	Value
down	Displays information about interfaces of L2VPN connection in the Down state.	-
up	Displays information about interfaces of L2VPN connection in the Up state.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

When locating L2VPN faults, you can use the **display l2vpn ccc-interface vc-type** command to view information about the AC interface of the current L2VPN connection, the total number of AC interfaces of various L2VPN connections, interface status, interface encapsulation type, and L2VPN connection types.

Example

# Display information about all the interfaces of L2VPN.

```
<HUAWEI> display l2vpn ccc-interface vc-type all
Total ccc-interface of LDP VC: 1
up (1), down (0)
Interface              Encap Type           State     VC Type
Vlanif12               vlan              up        ldp-vc
```

Table 10-93 Description of the **display l2vpn ccc-interface vc-type** command output

Item	Description
Total ccc-interface of CCC : 2 up (2), down (0)	Total number of L2VPN connections is 2. Two connections is Up. No connection is Down.
Interface	Interface connected to the L2VPN connection on the switch.
Encap Type	Encapsulation type of the L2VPN connection. The encapsulation type can be VLAN encapsulation or Ethernet encapsulation.
State	Current status of the L2VPN connection. The status can be Up or Down.

Item	Description
VC Type	Type of the L2VPN connection: ● ccc: Cross Circuit Connection ● ldp-vc: L2VPN connection in the Martini mode ● static-vc: L2VPN connection in the SVC mode ● bgp-vc: L2VPN connection in the Kompella mode ● vpls-vc: VPLS connection

10.7.10 display l2vpn vsi-list tunnel-policy

Function

The **display l2vpn vsi-list tunnel-policy** command displays the correlation between tunnel policies and VSIs.

Format

display l2vpn vsi-list tunnel-policy *policy-name*

Parameters

Parameter	Description	Value
policy-name	Specifies the name of a PW tunnel policy.	The value is an existing tunnel policy.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Using the **display l2vpn vsi-list tunnel-policy** *policy-name* command, you can view the names of VSIs that create a PW using the specified tunnel policy.

Example

# Display the name of the tunnel policy used by the VSI.

```
<HUAWEI> display l2vpn vsi-list tunnel-policy p1
Using Tunnel-Policy p1 VSI Instance statistics:
------------------------------------------------------------------------
  vsi v1
  vsi v2
  vsi v3
```

Table 10-94 Description of the display l2vpn vsi-list tunnel-policy command output

Item	Description
Using Tunnel-Policy p1 VSI Instance statistics	Names of all the PW VSIs established by the specified tunnel policy.
vsi	VSI name.

10.7.11 display loop-detect

Function

The **display loop-detect** command displays blocking information about L2VPN loop detection.

Format

display loop-detect

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After L2VPN loop detection is enabled on an interface by running the **loop-detect enable** command, you can run the **display loop-detect** command to check blocking information about L2VPN loop detection. The information helps determine whether loops occur on an L2VPN network, facilitating fault location.

Example

# Display blocking information about L2VPN loop detection on interfaces.

```
<HUAWEI> display loop-detect
----------------------------------------------------------------
Interface                 RecoverTime  Action    Status
-----------------------------------------------------------------
GigabitEthernet0/0/1.1       20        block     NORMAL
GigabitEthernet0/0/2.1       20        block     NORMAL
-----------------------------------------------------------------
```

Table 10-95 Description of the **display loop-detect** command output

Item	Description
Interface	Interface with L2VPN loop detection enabled. To enable L2VPN loop detection on an interface, run the **loop-detect enable** command.
RecoverTime	Period for restoring an interface to normal state. To specify this period, run the **loop-detect recovery-time** command.
Action	Action after an L2VPN loop is detected: ● BLOCK: Block this interface.
Status	Status of an interface with L2VPN loop detection enabled: ● NORMAL: No loop is detected. ● BLOCK: A loop is detected, and the interface is blocked.

10.7.12 display mpls l2vpn resource

Function

The **display mpls l2vpn resource** command displays MPLS L2VPN specifications and usage information.

Format

display mpls l2vpn resource

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

To check MPLS L2VPN specifications and usage information in routine maintenance, run the **display mpls l2vpn resource** command.

Example

# Display MPLS L2VPN specifications and usage information.

```
<HUAWEI> display mpls l2vpn resource

Public Capacity Statistics
 Statistics Item                 Supported Number      Used Number
 L2VPN AC Number                      2000                 2
 L2VPN VC Number                      8000                 2

 VPWS Capacity Statistics
 Statistics Item                 Supported Number      Used Number
 L2VPN Local CCC Number                 512                  0
 L2VPN Remote CCC Number                  1008                 0
 L2VPN SVC Number                     1008                 1
 L2VPN LDP VC Number                    2000                 0
 L2VPN BGP VC Number                    2000                 0
 L2VPN Switch VC Number                 2000                 0

 VPLS Capacity Statistics
 Statistics Item                 Supported Number      Used Number
 L2VPN VSI Number                     1024                 3
 L2VPN BGP VSI Number                   1024                 0
 L2VPN VSI VC Number                   8000                 1
 L2VPN VSI PWG Number                   1024                 0
```

Table 10-96 Description of the **display mpls l2vpn resource** command output

Item	Description
Public Capacity Statistics	MPLS L2VPN capacity statistics
Statistics Item	Statistics item
Supported Number	Maximum number allowed
Used Number	Number already used
L2VPN AC Number	Number of L2VPN AC interfaces, including the maximum number allowed and number already used
L2VPN VC Number	Number of L2VPN VCs, including the maximum number allowed and number already used
VPWS Capacity Statistics	VPWS capacity statistics
L2VPN Local CCC Number	Number of VLLs in local CCC mode, including the maximum number allowed and number already used
L2VPN Remote CCC Number	Number of VLLs in remote CCC mode, including the maximum number allowed and number already used
L2VPN SVC Number	Number of VLLs in SVC mode, including the maximum number allowed and number already used
L2VPN LDP VC Number	Number of LDP VLLs, including the maximum number allowed and number already used

Item	Description
L2VPN BGP VC Number	Number of BGP VLLs, including the maximum number allowed and number already used
L2VPN Switch VC Number	Number of Switch VC, including the maximum number allowed and number already used
VPLS Capacity Statistics	VPLS capacity statistics
L2VPN VSI Number	Number of VSIs, including the maximum number allowed and number already used
L2VPN BGP VSI Number	Number of BGP VSIs, including the maximum number allowed and number used
L2VPN VSI VC Number	Number of VSI VCs, including the maximum number allowed and number already used
L2VPN VSI PWG Number	Number of protection groups for a VSI, including the maximum number allowed and number already used

10.7.13 display mpls label-stack vpls vsi

Function

The **display mpls label-stack vpls vsi** command displays information about label stacks in a VPLS scenario.

Format

display mpls label-stack vpls vsi *vsi-name* **peer** *peer-ip-address* **vc-id** *vc-id*

Parameters

Parameter	Description	Value
vsi-name	Specifies the name of a VSI.	The value is an existing VSI.
peer *peer-ip-address*	Specifies the IP address of a peer.	The value is in dotted decimal notation.
vc-id *vc-id*	Specifies the VPLS PW ID.	The value is an integer ranging from 1 to 4294967295.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

To view PW traffic forwarding information in a Martini VPLS scenario, run the **display mpls label-stack vpls vsi** command.

Example

# Display stack label information in a Martini VPLS scenario with the peer IP address **1.1.1.9** and PW ID **11**.

```
<HUAWEI> display mpls label-stack vpls vsi a1 peer 1.1.1.9 vc-id 11
Label-stack  : 1
Level        : 1
Type         : VPLS
Label        : 1028
Level        : 2
Type         : LDP
Label        : --
OutInterface : Vlanif1024
```

Table 10-97 Description of the **display mpls label-stack vpls vsi** command output

Item	Description
Label-stack	Number of label stacks
Level	Number of label layers
Type	Tunnel type
Label	Outgoing label value
OutInterface	Outbound interface name

10.7.14 display oam-mac list

Function

The **display oam-mac list** command displays the MAC address list for the diagnostic test on the MAC address learning capacity.

Format

display oam-mac list

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The **display oam-mac list** command displays MAC address lists of all the **mac populate** or **mac purge** operations that are available on the device.

NOTE

Before performing diagnostic test of the MAC address learning capacity, you need to apply for a MAC address specialized for the diagnostic test. In this case, the diagnostic test does not impact on the normal forwarding.

At present, only the following MAC addresses are used in the diagnostic test.

- 0018-82a4-3fb1
- 0018-82a4-3fb2
- 0018-82a4-3fb3
- 0018-82a4-3fb4
- 0018-82a4-3fb5
- 0018-82a4-3fb6
- 0018-82a4-3fb7
- 0018-82a4-3fb8
- 0018-82a4-3fb9
- 0018-82a4-3fba

Example

# Display the MAC address list for the diagnostic test of the MAC address learning capacity.

```
<HUAWEI> display oam-mac list
No.  Mac Address
 1  0018-82a4-3fb1
 2  0018-82a4-3fb2
 3  0018-82a4-3fb3
 4  0018-82a4-3fb4
 5  0018-82a4-3fb5
 6  0018-82a4-3fb6
 7  0018-82a4-3fb7
 8  0018-82a4-3fb8
 9  0018-82a4-3fb9
10  0018-82a4-3fba
```

10.7.15 display oam-mac statistics

Function

The **display oam-mac statistics** command displays the statistics about the number of MAC diagnostic packets.

Format

display oam-mac statistics { **populate** | **purge** | **purge-register** | **all** }

Parameters

Parameter	Description	Value
populate	Displays the statistics about the number of populate packets.	-
purge	Displays the statistics about the number of purge packets.	-
purge-register	Displays the statistics about the number of purge register packets.	-
all	Displays the statistics about the number of MAC diagnostic packets of all types.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Using the **display oam-mac statistics** command, you can view the number of MAC diagnostic packets that is counted since the **reset oam-mac statistics** command was run.

Example

# Display the statistics about the number of populate packets that are received by the device.

```
<HUAWEI> display oam-mac statistics populate
Received populate packet: 3
```

# Display the statistics about the number of all MAC diagnostic packets that are received by the device.

```
<HUAWEI> display oam-mac statistics all
 Received populate packet: 3
 Received purge packet: 1
 Received purge register packet: 2
```

Table 10-98 Description of the display oam-mac statistics all command output

Item	Description
Received populate packet	Number of received populate packets.
Received purge packet	Number of received purge packets.
Received purge register packet	Number of received purge register packets.

10.7.16 display traffic-statistics vsi

Function

The **display traffic-statistics vsi** command displays the statistics about the public traffic on all VPLS PWs in a specified VSI.

Format

display traffic-statistics vsi *vsi-name*

Parameters

Parameter	Description	Value
vsi-name	Specifies the name of a specified VSI.	The value is an existing VSI.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

After the VPLS network is configured, you can run the **display traffic-statistics vsi** command to view the statistics about the traffic on all VPLS PWs in a specified VSI.

Precautions

- Currently, this command only displays the statistics about the traffic on the Martini VPLS PWs in the VSI.
- Within five minutes, if a PW goes Down, traffic before the PW is Down cannot be used to compute the traffic rate in the five minutes.

Example

# Display the statistics about the traffic on all VPLS PWs in a specified VSI.

```
<HUAWEI> display traffic-statistics vsi newvsi
vsi-name: newvsi
Peer-address: 10.22.33.20
Negotiation-vc-id: 2
Statistics last cleared: never
Last 300 seconds input rate : 0 bytes/sec, 0 packets/sec
Last 300 seconds output rate: 0 bytes/sec, 0 packets/sec
Input: 0 bytes, 0 packets
Output: 0 bytes, 0 packets
```

Table 10-99 Description of the display traffic-statistics vsi command output

Item	Description
vsi-name	VSI name.
Peer-address	IP address of the remote peer.
Negotiation-vc-id	VC ID of the PW.
Statistics last cleared	Last time when statistics are cleared.
Last 300 seconds input rate	Rate of incoming traffic in the last 300 seconds.
Last 300 seconds output rate	Rate of outgoing traffic in the last 300 seconds.
Input	Number of packets received by the PW from the AC.
Output	Number of packets sent from the PW to the AC.

10.7.17 display traffic-statistics vsi peer

Function

The **display traffic-statistics vsi peer** command displays the statistics about the public traffic on a VPLS PW in a specified VSI.

Format

display traffic-statistics vsi *vsi-name* **peer** *peer-address*

Parameters

Parameter	Description	Value
vsi-name	Specifies the name of a specified VSI.	The value is an existing VSI.
peer-address	Specifies the peer IP address of the PW.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

After the VPLS network is configured, you can run the **display traffic-statistics vsi peer** command to view the statistics about the traffic on the PW.

Precautions

- Currently, this command only displays the statistics about the traffic on the Martini VPLS PWs in the VSI.
- Within five minutes, if a PW goes Down, traffic before the PW is Down cannot be used to compute the traffic rate in the five minutes.

Example

# Display the statistics about the outgoing traffic on the specified VPLS PW.

```
<HUAWEI> display traffic-statistics vsi newvsi peer 10.22.33.20
vsi-name: newvsi
Peer-address: 10.22.33.20
Negotiation-vc-id: 2
Statistics last cleared: never
Last 300 seconds input rate : 0 bytes/sec, 0 packets/sec
Last 300 seconds output rate: 0 bytes/sec, 0 packets/sec
Input: 0 bytes, 0 packets
Output: 0 bytes, 0 packets
```

Table 10-100 Description of the display traffic-statistics vsi peer command output

Item	Description
vsi-name	VSI name.
Peer-address	IP address of the remote peer.
Negotiation-vc-id	VC ID of the PW.
Statistics last cleared	Last time when statistics are cleared.
Last 300 seconds input rate	Rate of incoming traffic in the last 300 seconds.
Last 300 seconds output rate	Rate of outgoing traffic in the last 300 seconds.
Input	Number of packets received by the PW from the AC.
Output	Number of packets sent from the PW to the AC.

10.7.18 display traffic-statistics vsi peer ldp129

Function

The **display traffic-statistics vsi peer ldp129** command displays the statistics about the public traffic on a BGP-AD VPLS PW in a specified VSI.

Format

display traffic-statistics vsi *vsi-name* **peer** *peer-address* **ldp129**

Parameters

Parameter	Description	Value
vsi-name	Specifies the name of a VSI. The specified VSI must be a VSI of the BGP-AD VPLS.	The value is an existing VSI.
peer-address	Specifies the peer IP address of the PW.	-
ldp129	Specifies the statistics about the public traffic in the BGP-AD VPLS that uses LDP 129 signaling.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

After the BGP-AD VPLS configuration is complete, you can run the **display traffic-statistics vsi peer ldp129** command to view the statistics about the traffic on the PW.

Prerequisites

The following operations have been performed before this command is used:

1. The BGP-AD VPLS has been configured.
2. The traffic statistics function has been enabled using the **traffic-statistics enable (VSI-BGPAD view)** command or the **traffic-statistics peer enable (VSI-BGPAD)** command in the VSI-BGPAD view.

Precautions

- The **display traffic-statistics vsi peer ldp129** command only displays the statistics about the traffic on the PW in the BGP-AD VPLS.

- Within five minutes, if a PW goes Down, traffic before the PW is Down cannot be used to compute the traffic rate in the five minutes.

Example

# Display the statistics about the public traffic on the specified PW in the BGP-AD VPLS.

```
<HUAWEI> display traffic-statistics vsi vplsad1 peer 10.22.33.20 ldp129
vsi-name: vplsad1
Peer-address: 10.22.33.20
Statistics last cleared: never
Last 300 seconds input rate : 0 bytes/sec, 0 packets/sec
Last 300 seconds output rate: 0 bytes/sec, 0 packets/sec
Input: 0 bytes, 0 packets
Output: 0 bytes, 0 packets
```

Table 10-101 Description of the display traffic-statistics vsi peer ldp129 command output

Item	Description
vsi-name	VSI name.
Peer-address	IP address of the peer device.
Statistics last cleared	Last time when statistics are cleared.
Last 300 seconds input rate	Rate of incoming traffic in the last 300 seconds.
Last 300 seconds output rate	Rate of outgoing traffic in the last 300 seconds.
Input	Number of packets received by the PW from the AC.
Output	Number of packets sent from the PW to the AC.

10.7.19 display traffic-statistics vsi peer negotiation-vc-id

Function

The **display traffic-statistics vsi peer negotiation-vc-id** command displays the statistics about the public traffic on the Martini VPLS PW in a specified VSI.

Format

display traffic-statistics vsi *vsi-name* **peer** *peer-address* **negotiation-vc-id** *vc-id*

Parameters

Parameter	Description	Value
vsi-name	Specifies the name of a specified VSI.	The value is an existing VSI.
peer-address	Specifies the peer IP address of the PW.	-
vc-id	Specifies the VC ID of the PW.	The value is an integer that ranges from 1 to 4294967295.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

After the Martini VPLS network is configured, you can run the **display traffic-statistics vsi peer negotiation-vc-id** command to view the statistics about the traffic on the PW.

Prerequisites

The following operations have been performed before this command is used:

1. The Martini VPLS has been configured.
2. The traffic statistics function has been enabled using the **traffic-statistics enable (VSI-LDP view)** command or the **traffic-statistics peer enable** command in the VSI-LDP view.

Precautions

- Currently, this command only displays the statistics about the traffic on the Martini VPLS PWs in the VSI.
- Within five minutes, if a PW goes Down, traffic before the PW is Down cannot be used to compute the traffic rate in the five minutes.

Example

# Display the statistics about the traffic on the specified Martini VPLS PW.

```
<HUAWEI> display traffic-statistics vsi newvsi peer 10.22.33.20 negotiation-vc-id 2
vsi-name: newvsi
Peer-address: 10.22.33.20
Negotiation-vc-id: 2
Statistics last cleared: never
Last 300 seconds input rate : 0 bytes/sec, 0 packets/sec
Last 300 seconds output rate: 0 bytes/sec, 0 packets/sec
```

```
Input: 0 bytes, 0 packets
Output: 0 bytes, 0 packets
```

Table 10-102 Description of the display traffic-statistics vsi peer negotiation-vc-id command output

Item	Description
vsi-name	VSI name.
Peer-address	IP address of the remote peer.
Negotiation-vc-id	VC ID of the PW.
Statistics last cleared	Last time when statistics are cleared.
Last 300 seconds input rate	Rate of incoming traffic in the last 300 seconds.
Last 300 seconds output rate	Rate of outgoing traffic in the last 300 seconds.
Input	Number of packets received by the PW from the AC.
Output	Number of packets sent from the PW to the AC.

10.7.20 display traffic-statistics vsi peer remote-site

Function

The **display traffic-statistics vsi peer remote-site** command displays the statistics about the public traffic on the Kompella VPLS PW in a specified VSI.

Format

display traffic-statistics vsi *vsi-name* **peer** *peer-address* **remote-site** *site-id*

Parameters

Parameter	Description	Value
vsi-name	Specifies the name of a specified VSI.	The value is an existing VSI.
peer-address	Specifies the peer IP address of the PW.	-
site-id	Specifies the remote site ID.	The value is an integer that ranges from 0 to 65534.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

After the Kompella VPLS network is configured, you can run the **display traffic-statistics vsi peer remote-site** command to view the statistics about the traffic on the PW.

Prerequisites

The following operations have been performed before this command is used:

1. The Kompella VPLS has been configured.
2. The traffic statistics function has been enabled using the **traffic-statistics peer remote-site enable (Kompella)** command in the VSI-BGP view.

Precautions

- The Kompella VPLS PW is uniquely identified by the user-defined VSI name, the next-hop IP address, and the remote site value.
- Within five minutes, if a PW goes Down, traffic before the PW is Down cannot be used to compute the traffic rate in the five minutes.

Example

# Display the statistics about the traffic on the specified Kompella VPLS PW.

```
<HUAWEI> display traffic-statistics vsi newvsi peer 10.22.33.20 remote-site 2
vsi-name: newvsi
Peer-address: 10.22.33.20
Negotiation-vc-id: 2
Statistics last cleared: never
Last 300 seconds input rate : 0 bytes/sec, 0 packets/sec
Last 300 seconds output rate: 0 bytes/sec, 0 packets/sec
Input: 0 bytes, 0 packets
Output: 0 bytes, 0 packets
```

Table 10-103 Description of the display traffic-statistics vsi peer remote-site command output

Item	Description
vsi-name	VSI name.
Peer-address	IP address of the remote peer.
Remote-site-id	Remote Site ID.
Statistics last cleared	Last time when statistics are cleared.
Last 300 seconds input rate	Rate of incoming traffic in the last 300 seconds.
Last 300 seconds output rate	Rate of outgoing traffic in the last 300 seconds.

Item	Description
Input	Number of packets received by the PW from the AC.
Output	Number of packets sent from the PW to the AC.

10.7.21 display vpls connection

Function

The **display vpls connection** command displays the VPLS connection.

Format

display vpls connection [**ldp** | **bgp** | **bgp-ad** | **vsi** *vsi-name*] [**down** | **up**] [**verbose**]

Parameters

Parameter	Description	Value
ldp	Displays information about LDP signaling connections.	-
bgp	Displays information about BGP signaling connections.	-
bgp-ad	Displays information about BGP AD signaling connections.	-
vsi *vsi-name*	Displays information about connections of the specified VSI.	The value is an existing VSI.
down	Displays information about connections in Down state.	-
up	Displays information about connections in Up state.	-
verbose	Displays detailed information about connections.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

After VPLS services are configured, you can run the **display vpls connection** command with different keywords or parameters to view information about specific VPLS connections.

Prerequisites

One of the following operations has been performed before the **display vpls connection** command is used:

- Configuring Kompella VPLS
- Configuring Martini VPLS
- Configuring BGP AD VPLS

Precautions

If no keyword or parameter is specified, information about all VPLS connections in Up state is displayed.

Example

# Display information about the connections of all VSIs.

```
<HUAWEI> display vpls connection

2 total connections,
connections: 2 up, 0 down, 1 ldp, 1 bgp, 0 bgpad

VSI Name: a2                           Signaling: ldp
VsiID      EncapType               PeerAddr         InLabel   OutLabel  VCState
2          vlan                 3.3.3.9          1026      1025      up
VSI Name: bgp1                           Signaling: bgp
SiteID     RD                      PeerAddr         InLabel   OutLabel  VCState
2          168.1.1.2:1             3.3.3.9          35842     35841     up
```

Table 10-104 Description of the display vpls connection command output

Item	Description
VSI Name	Name of the VSI. To set the value, run the **vsi** command.
Signaling	Signaling mode: ldp, bgp, bgpad or ldp bgpad. To set the value, run the **pwsignal** or **bgp-ad** command.
VsiID	VSI ID. To set the value, run the **vsi-id** command.

Item	Description
EncapType	VPLS encapsulation type of the VSI, namely, the encapsulation type of the packets transmitted over the VC. To set the value, run the **encapsulation** command.
PeerAddr	IP addresses of the peer.
InLabel	VC label distributed locally.
OutLabel	Local outgoing label, namely, the VC label distributed by the peer.
VCState	Status of the VC.
SiteID	Site ID of the remote VSI. To set the value, run the **site** command.
RD	RD used for identifying a VSI on the PE in the VPLS using BGP signaling. To set the value, run the **route-distinguisher** command.

# Display the detailed information about all VSI connections.

```
<HUAWEI> display vpls connection verbose
VSI Name: a2                          Signaling: ldp
  **Remote Vsi ID   : 2
    VC State        : up
    Encapsulation   : vlan
    Group ID        : 0
    MTU             : 1500
    Peer Ip Address : 3.3.3.9
    PW Type         : label
    Local VC Label  : 1026
    Remote VC Label : 1025
    Tunnel Policy   : --
    Tunnel ID       : 0x1
VSI Name: bgp1                          Signaling: bgp
  **Remote Site ID     : 2
    VC State           : up
    RD                 : 168.1.1.2:1
    Encapsulation      : vlan
    MTU                : 1500
    Peer Ip Address    : 3.3.3.9
    PW Type            : label
    Local VC Label     : 35842
    Remote VC Label    : 35841
    Tunnel Policy      : --
    Tunnel ID          : 0x1
    Remote Label Block : 35840/5/0
    Export vpn target  : 100:1
```

Table 10-105 Description of the display vpls connection verbose command output

Item	Description
VSI Name	Name of the VSI. To set the value, run the **vsi** command.
Signaling	Signaling mode: ldp, bgp, bgpad or ldp bgpad.
Remote Vsi ID	Remote VSI ID that is consistent with the local VSI ID.
VC State	Status of the VC, which can be Up or Down.
Encapsulation	VPLS encapsulation type of the VSI, namely, the encapsulation type of the packets transmitted over the VC. The encapsulation type is VLAN or Ethernet. To set the value, run the **encapsulation** command.
Group ID	Group identifier.
MTU	Maximum transmission unit. To set the value, run the **mtu** command.
Peer Ip Address	IP addresses of the peer.
PW Type	Type of the PW.
Local VC Label	Local VC label.
Remote VC Label	Remote VC label.
Tunnel Policy	Tunnel policy that is used by the L2VPN.
Tunnel ID	Tunnel ID.
Remote Label Block	Remote label block.
Export vpn target	Outbound extended community attribute to the target VPN.

# Display the detailed information about connections of a VSI named **bgp1**

```
<HUAWEI> display vpls connection vsi bgp1 verbose
VSI Name: bgp1                          Signaling: bgp
  **Remote Site ID     : 2
    VC State           : up
    RD                 : 168.1.1.2:1
    Encapsulation      : vlan
    MTU                : 1500
    Peer Ip Address    : 3.3.3.9
    PW Type            : label
    Local VC Label     : 35842
    Remote VC Label    : 35841
    Tunnel Policy      : --
    Tunnel ID          : 0x1
    Remote Label Block : 35840/5/0
    Export vpn target  : 100:1
```

Table 10-106 Description of the display vpls connection vsi vsi-name verbose command output

Item	Description
VSI Name	Name of the VSI.
Signaling	Signaling mode: ldp, bgp, bgpad or ldp bgpad.
Remote Site ID	the Site ID of remote peer.
VC State	Status of the VC.
RD	Local router distinguisher.
Encapsulation	VPLS encapsulation type of the VSI, namely, the encapsulation type of the packets transmitted over the VC.
MTU	Maximum transmission unit.
Peer Ip Address	IP addresses of the peer.
PW Type	Type of the PW.
Local VC Label	VC label distributed locally.
Remote VC Label	VC label distributed by the peer.
Tunnel Policy	Tunnel policy.
Tunnel ID	Tunnel ID.
Remote Label Block	Remote label block.
Export vpn target	Outbound extended community attribute to the target VPN.

# Display information about BGP AD VPLS connections with peers.

```
<HUAWEI> display vpls connection bgp-ad

1 total bgpad connections ,
connections: 1 up, 0 down

VSI Name: vplsad1                    Signaling: bgpad
VPLS ID            EncapType      PeerAddr        InLabel   OutLabel  VCState
168.1.1.1:1        vlan           3.3.3.9         1027      1026      up
```

Table 10-107 Description of the display vpls connection bgp-ad command output

Item	Description
VSI Name	Name of the VSI.

Item	Description
Signaling	VPLS signaling mode: ● ldp ● bgp ● bgpad ● ldp bgpad
VPLS ID	Identifier of a BGP AD VPLS domain.
EncapType	VPLS encapsulation type of the VSI, namely, the encapsulation type of the packets transmitted over the VC: ● VLAN ● Ethernet
PeerAddr	IP addresses of the peer.
InLabel	VC label distributed locally.
OutLabel	Local outgoing label, namely, the VC label distributed by the peer.
VCState	Status of the VC. ● up ● down

# Display detailed information about BGP AD connections of the VSIs that are in Up state.

```
<HUAWEI> display vpls connection bgp-ad up verbose
VSI Name: vplsad1                         Signaling: bgpad
  **VPLS ID         : 168.1.1.1:1
    VC State        : up
    Encapsulation   : vlan
    Group ID        : 0
    MTU             : 1500
    Peer Ip Address : 3.3.3.9
    PW Type         : label
    Local VC Label  : 1027
    Remote VC Label : 1026
    Tunnel Policy   : --
```

Table 10-108 Description of the display vpls connection bgp-ad up verbose command output

Item	Description
VSI Name	Name of the VSI.

Item	Description
Signaling	VPLS signaling mode: ● ldp ● bgp ● bgpad ● ldp bgpad
VPLS ID	Identifier of a BGP AD VPLS domain.
Encapsulation	VPLS encapsulation type of the VSI, namely, the encapsulation type of the packets transmitted over the VC: ● VLAN ● Ethernet
Group ID	Group identifier
MTU	Maximum transmission unit.
Peer Ip Address	IP addresses of the peer.
Local VC Label	VC label distributed locally.
Remote VC Label	Local outgoing label, namely, the VC label distributed by the peer.
Tunnel Policy	Name of a tunnel policy used by the VPLS.

10.7.22 display vpls forwarding-info

Function

The **display vpls forwarding-info** command displays forwarding information of all VSIs.

Format

display vpls forwarding-info [**vsi** *vsi-name* [**peer** *peer-address* [**negotiation-vc-id** *vc-id* | **remote-site** *site-id*]] | **state** { **up** | **down** }] [**verbose**]

Parameters

Parameter	Description	Value
vsi *vsi-name*	Displays forwarding information of a specified VSI.	The value is an existing VSI.

Parameter	Description	Value
peer *peer-address*	Specifies the peer IP address of the PW.	The value is in dotted decimal notation.
negotiation-vc-id *vc-id*	Specifies the VC ID of the PW.	The value is an integer that ranges from 1 to 4294967295.
remote-site *site-id*	Specifies the remote site ID.	The value is an integer that ranges from 0 to 65534.
state	Displays the forwarding information about VSIs based on the PW status.	-
up	Displays the forwarding information about the VSIs whose PWs are in Up state.	-
down	Displays the forwarding information about the VSIs whose PWs are in Down state.	-
verbose	Displays detailed forwarding information of the VSI.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

After the VPLS is configured, you can run the **display vpls forwarding-info** command to view the forwarding information of all VSIs.

Prerequisites

One of the following operations has been performed before the **display vpls forwarding-info** command is used:

- Configuring Kompella VPLS
- Configuring Martini VPLS
- Configuring BGP AD VPLS

Precautions

- The **display vpls forwarding-info vsi** *vsi-name* command is used to display forwarding information of a specified VSI (in Martini mode or Kompella mode).
- The **display vpls forwarding-info vsi** *vsi-name* **peer** *peer-address* [**negotiation-vc-id** *vc-id*] command is used to display forwarding information of a specified PW in the Martini VSI.
- The **display vpls forwarding-info vsi** *vsi-name* **peer** *peer-address* **remote-site** *site-id* command is used to display forwarding information about a specified PW in the Kompella VSI.

Example

# Display brief forwarding information of all PWs in all VSIs.

```
<HUAWEI> display vpls forwarding-info
Total Number   : 2,       2  up,  0  down

Vsi-Name                       PeerIP         VcOrSiteId  PwState
a2                          3.3.3.9        2          UP
vplsad1                       3.3.3.9        0          UP
```

# Display brief information about the VSI PWs in Up state.

```
<HUAWEI> display vpls forwarding-info state up
Total Number   : 2,       2  up,  0  down

Vsi-Name                       PeerIP         VcOrSiteId  PwState
a2                          3.3.3.9        2          UP
vplsad1                       3.3.3.9        0          UP
```

Table 10-109 Description of the display vpls forwarding-info command output

Item	Description
Total Number	The number of VSI.
Vsi-Name	Name of the VSI.
PeerIP	Peer IP address of the PW in the VSI.
VcOrSiteId	● VSI ID for the Martini VSI. ● Site ID for the Kompella VSI.
PwState	PW status: ● Up ● Down

# Display detailed forwarding information of all PWs in all VSIs.

```
<HUAWEI> display vpls forwarding-info verbose
Total Number   : 2,       2  up,  0  down

**Vsi-Name      : a2
  Vsi Index     : 0                         PwState      : UP
  Peer IP       : 3.3.3.9                   VcOrSiteId   : 2
  InVcLabel     : 1026                        OutVcLabel   : 1025
  BroadTunnelID : 0x1                           OutInterface : Vlanif1025
```

```
 MainPwToken   : 0x1                    SlavePwToken : 0x0
 NKey          : 0x9                    CKey         : 0xa

**Vsi-Name      : vplsad1
 Vsi Index     : 2                      PwState      : UP
 Peer IP       : 3.3.3.9                VcOrSiteId   : 0
 InVcLabel     : 1036                   OutVcLabel   : 1031
 BroadTunnelID : 0x1                    OutInterface : Vlanif1025
 MainPwToken   : 0x1                    SlavePwToken : 0x0
 NKey          : 0x9                    CKey         : 0x1b
```

# Display the detailed forwarding information about the VSI PWs in Up state.

```
<HUAWEI> display vpls forwarding-info state up verbose
Total Number   : 2,        2  up,  0  down

**Vsi-Name      : a2
 Vsi Index     : 0                      PwState      : UP
 Peer IP       : 3.3.3.9                VcOrSiteId   : 2
 InVcLabel     : 1026                   OutVcLabel   : 1025
 BroadTunnelID : 0x1                    OutInterface : Vlanif1025
 MainPwToken   : 0x1                    SlavePwToken : 0x0
 NKey          : 0x9                    CKey         : 0xa

**Vsi-Name      : vplsad1
 Vsi Index     : 2                      PwState      : UP
 Peer IP       : 3.3.3.9                VcOrSiteId   : 0
 InVcLabel     : 1036                   OutVcLabel   : 1031
 BroadTunnelID : 0x1                    OutInterface : Vlanif1025
 MainPwToken   : 0x1                    SlavePwToken : 0x0
 NKey          : 0x9                    CKey         : 0x1b
```

Table 10-110 Description of the display vpls forwarding-info verbose command output

Item	Description
Total Number	The number of VSI.
Vsi-Name	Name of the VSI.
Vsi Index	VSI index.
PwState	PW status: ● Up ● Down
Peer IP	Peer IP address of the PW in the VSI.
VcOrSiteId	● VSI ID for the Martini VSI. ● Site ID for the Kompella VSI.
InVcLabel	Incoming label of the VC.
OutVcLabel	Outgoing label of the VC.
BroadTunnelID	ID of the tunnel used for broadcast.
OutInterface	Outbound interface.
MainPwToken	Token of the master PW.
SlavePwToken	Token of the slave PW.

Item	Description
NKey	Network key. Each NKey corresponds to one peer + tunnel policy.
CKey	User key. Each CKey corresponds to a PW.

10.7.23 display vpls multicast-ping statistics

Function

The **display vpls multicast-ping statistics** command displays the statistics on the number of sent and received MFIB Ping packets.

Format

display vpls multicast-ping statistics

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Using the **display vpls multicast-ping statistics** command, you can view the statistics on the number of MFIB Ping packets that are received and sent by the device since the last time the **reset vpls multicast-ping statistics** command was run.

Example

# Display the statistics on the number of MFIB Ping packets.

```
<HUAWEI> display vpls multicast-ping statistics
Total sent: 5 packet(s)
Total received: 5 packet(s)
Vpls Mfib-ping echo request sent: 5 packet(s), received: 0 packet(s)
Vpls Mfib-ping echo reply sent: 0 packet(s), received: 5 packet(s)
```

Table 10-111 Description of the display vpls multicast-ping statistics command output

Item	Description
Total sent	Total number of sent packets.
Total received	Total number of received packets.
Vpls Mfib-ping echo request	Number of sent and received VPLS MFIB Ping Echo Request packets.
Vpls Mfib-ping echo reply	Number of sent and received VPLS MFIB Ping Echo Reply packets.

10.7.24 display vpls multicast-trace statistics

Function

The **display vpls multicast-trace statistics** command displays the statistics on the number of sent and received MFIB Trace packets.

Format

display vpls multicast-trace statistics

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display vpls multicast-trace statistics** command to view the number of sent and received MFIB Trace packets since the last time the **reset vpls multicast-trace statistics** command is executed.

Example

# Display the statistics on the number of MFIB Trace packets.

```
<HUAWEI> display vpls multicast-trace statistics
Total sent: 2 packet(s)
Total received: 2 packet(s)
Vpls Mfib-trace echo request sent: 2 packet(s), received: 0 packet(s)
Vpls Mfib-trace echo reply sent: 0 packet(s), received: 2 packet(s)
```

Table 10-112 Description of the display vpls multicast-trace statistics command output

Item	Description
Total sent	Total number of sent packets.
Total received	Total number of received packets.
Vpls Mfib-trace echo request	Number of sent and received VPLS MFIB Trace Echo Request packets.
Vpls Mfib-trace echo reply	Number of sent and received VPLS MFIB Trace Echo Reply packets.

10.7.25 display vpls-ping statistics

Function

The **display vpls-ping statistics** command displays the statistics on the number of sent and received VPLS MAC Ping packets.

Format

display vpls-ping statistics

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Using the **display vpls-ping statistics** command, you can view the statistics on the number of sent and received VPLS MAC Ping packets on the device.

Example

# Display the statistics on the number of VPLS MAC Ping packets.

```
<HUAWEI> display vpls-ping statistics
Vpls-ping statistics:
Total sent: 104797 packet (s)
Total received: 104792 packet (s)
vpls-ping request sent: 13 packet (s), received: 104784 packet (s)
vpls-ping reply sent: 104784 packet (s), received: 8 packet (s)
```

Table 10-113 Description of the display vpls-ping statistics command output

Item	Description
Total sent	Total number of sent VPLS MAC Ping packets.
Total received	Total number of received VPLS MAC Ping packets.
vpls-ping request sent	Number of sent VPLS Ping Request packets.
vpls-ping reply sent	Number of sent VPLS Ping Reply packets.

10.7.26 display vpls-trace statistics

Function

The **display vpls-trace statistics** command displays the statistics on the number of sent and received VPLS MAC Trace packets.

Format

display vpls-trace statistics

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Using the **display vpls-trace statistics** command, you can view the statistics on the number of sent and received VPLS MAC Trace packets on the device.

Example

# Display the statistics on the number of VPLS MAC Trace packets.

```
<HUAWEI> display vpls-trace statistics
Vpls-trace statistics:
Total sent : 4 packet (s)
Total received : 4 packet (s)
vpls-trace request sent: 4 packet (s), received: 0 packet (s)
vpls-trace reply sent: 0 packet (s), received: 4 packet (s)
```

Table 10-114 Description of the display vpls-trace statistics command output

Item	Description
Total sent	Total number of sent VPLS MAC Trace packets.
Total received	Total number of received VPLS MAC Trace packets.
vpls-trace request sent	Number of sent VPLS MAC Trace Request packets.
vpls-trace reply sent	Number of sent VPLS MAC Trace Reply packets.

10.7.27 display vsi

Function

The **display vsi** command displays information about a VSI.

Format

display vsi [**name** *vsi-name*] [**verbose**]

display vsi [**name** *vsi-name*] **peer-info** [**statistics**]

display vsi name *vsi-name* **peer-info** *peer-ip* [**verbose**]

Parameters

Parameter	Description	Value
name *vsi-name*	Displays the name of a specified VSI.	The value is an existing VSI.
verbose	Displays detailed information about the VSI.	-
peer-info	Displays detailed information or statistics about the PW status of peers.	-
statistics	Displays statistics about the PW status of peers.	-
peer-ip	Displays detailed information about the PW status of the peer with a specified IP address.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

When you run the **display vsi** command:

- The **display vsi** command displays information about VSIs. By default, information of all VSIs is displayed.
- The **display vsi peer-info** command displays detailed information about the PW status of peers of all VSIs.
- The **display vsi name** *vsi-name* **peer-info** command displays detailed information about the PW status of peers to a specified VSI.
- The **display vsi name** *vsi-name* **peer-info** *peer-ip* command displays detailed information about the PW status of a specific peer to a specified VSI.
- The **display vsi peer-info statistics** command displays statistics about the PW status of peers of all VSIs.
- The **display vsi name** *vsi-name* **peer-info statistics** command displays statistics about the PW status of a specific peer to a specified VSI.

Example

# Display information about the VSI named **a2**.

```
<HUAWEI> display vsi name a2
Vsi                             Mem    PW   Mac       Encap     Mtu   Vsi
Name                            Disc   Type Learn     Type      Value State
--------------------------------------------------------------------------
a2                              static ldp  unqualify vlan      1500  up
```

# Display information about the hybrid VSI named **vsi1**.

```
<HUAWEI> display vsi name vsi1
Vsi                             Mem    PW   Mac       Encap     Mtu   Vsi
Name                            Disc   Type Learn     Type      Value State
--------------------------------------------------------------------------
vsi1                            --     mixed unqualify vlan     1500  up
```

Table 10-115 Description of the **display vsi** command output

Item	Description
Vsi Name	Name of the VSI. To set the value, run the **vsi** command.
Mem Disc	Member discovery mode: ● static ● auto ● --

Item	Description
PW Type	PW type: ● ldp ● bgp ● bgpad ● mixed
Mac Learn	Mode of learning the MAC address.
Encap Type	Encapsulation type. ● vlan ● ethernet If the encapsulation types on both ends are different, run the **encapsulation** { **ethernet** | **vlan** } command in the VSI view to change the encapsulation type on one end to be the same as that on the other end.
Mtu Value	Maximum transmission unit. If the MTU values on both ends are different, run the **mtu** *mtu-value* command in the VSI view to change the MTU values on one end to be the same as that on the other end.
Vsi State	Status of the VSI: ● up ● down ● *down

# Display detailed information about all VSIs.

```
<HUAWEI> display vsi verbose

 ***VSI Name               : a2
    Administrator VSI      : no
    Isolate Spoken         : disable
    VSI Index              : 0
    PW Signaling           : ldp
    Member Discovery Style : static
    PW MAC Learn Style     : unqualify
    Encapsulation Type     : vlan
    MTU                    : 1500
    Diffserv Mode          : uniform
    Mpls Exp               : --
    DomainId               : 255
    Domain Name            :
    Ignore AcState         : disable
    P2P VSI                : disable
    Create Time            : 0 days, 3 hours, 6 minutes, 43 seconds
    VSI State              : up

    VSI ID                 : 2
   *Peer Router ID         : 10.3.3.9
    Negotiation-vc-id      : 2
    primary or secondary   : primary
    ignore-standby-state   : no
    VC Label               : 1026
    Peer Type              : dynamic
    Session                : up
    Tunnel ID              : 0x1
    Broadcast Tunnel ID    : 0x1
    Broad BackupTunnel ID  : 0x0
    CKey                   : 10
    NKey                   : 9
    Stp Enable             : 0
    PwIndex                : 0
    Control Word           : disable
    BFD for PW             : unavailable

    Interface Name         : Vlanif1024
    State                  : up
    Access Port            : false
    Last Up Time           : 2012/07/06 14:00:15
    Total Up Time          : 0 days, 3 hours, 6 minutes, 20 seconds

  **PW Information:

   *Peer Ip Address        : 10.3.3.9
    PW State               : up
    Local VC Label         : 1026
    Remote VC Label        : 1025
    Remote Control Word    : disable
    PW Type                : label
    Local  VCCV            : alert lsp-ping bfd
    Remote VCCV            : alert lsp-ping bfd
    Tunnel ID              : 0x1
    Broadcast Tunnel ID    : 0x1
    Broad BackupTunnel ID  : 0x0
    Ckey                   : 0xa
    Nkey                   : 0x9
    Main PW Token          : 0x1
    Slave PW Token         : 0x0
    Tnl Type               : LSP
    OutInterface           : Vlanif1025
    Backup OutInterface    :
    Stp Enable             : 0
    PW Last Up Time        : 2012/07/06 14:01:07
    PW Total Up Time       : 0 days, 3 hours, 5 minutes, 28 seconds

 ***VSI Name               : bgp1
    Administrator VSI      : no
    Isolate Spoken         : disable
    VSI Index              : 6
    PW Signaling           : bgp
    Member Discovery Style : auto
    PW MAC Learn Style     : unqualify
    Encapsulation Type     : vlan
    MTU                    : 1500
    Diffserv Mode          : uniform
    Mpls Exp               : --
    DomainId               : 255
    Domain Name            :
    Ignore AcState         : disable
    P2P VSI                : disable
    Create Time            : 2 days, 20 hours, 19 minutes, 16 seconds
    VSI State              : up

    BGP RD                 : 172.16.1.1:1
    SiteID/Range/Offset    : 1/5/0
    Import vpn target      : 100:1
    Export vpn target      : 100:1
    Remote Label Block     : 35840/5/0
    Local Label Block      : 0/35840/5/0
    Interface Name          : Vlanif1022
    State                   : up
    Access Port             : false
    Last Up Time            : 2012/08/06 03:24:45
    Total Up Time           : 0 days, 0 hours, 10 minutes, 11 seconds

  **PW Information:

   *Peer Ip Address         : 10.3.3.9
    PW State                : up
    Local VC Label          : 35843
    Remote VC Label         : 35841
    PW Type                 : label
    Local  VCCV             : alert lsp-ping bfd
    Remote VCCV             : alert lsp-ping bfd
    Tunnel ID               : 0x2e4d
    Broadcast Tunnel ID     : 0x2e4d
    Broad BackupTunnel ID  : 0x0
    Ckey                    : 0x17
    Nkey                    : 0x15
    Main PW Token           : 0x2e4d
    Slave PW Token          : 0x0
    Tnl Type                : LSP
    OutInterface            : Vlanif1025
    Backup OutInterface     :
    Stp Enable              : 0
    PW Last Up Time         : 2012/08/06 03:25:12
    PW Total Up Time        : 0 days, 0 hours, 9 minutes, 44 seconds

 ***VSI Name                : vplsad1
    Administrator VSI       : no
    Isolate Spoken          : disable
    VSI Index               : 2
    PW Signaling            : bgpad
    Member Discovery Style : --
    PW MAC Learn Style      : unqualify
    Encapsulation Type      : vlan
    MTU                     : 1500
    Diffserv Mode           : uniform
    Mpls Exp                : --
    DomainId                : 255
    Domain Name             :
    Ignore AcState          : disable
    P2P VSI                 : disable
    Create Time             : 0 days, 1 hours, 28 minutes, 24 seconds
    VSI State               : up

    VPLS ID                 : 172.16.1.1:1
    RD                      : 172.16.1.1:1
    Import vpn target       : 100:1
    Export vpn target       : 100:1
    VSI ID                  : 1.1.1.9

   *Peer Router ID          : 10.3.3.9
    VPLS ID                 : 172.16.1.1:1
    SAII                    : 1.1.1.9
    TAII                    : 10.3.3.9
    VC Label                : 1027
    Peer Type               : dynamic
    Session                 : up
    Tunnel ID               : 0x1
    Broadcast Tunnel ID     : 0x1
    CKey                    : 12
    NKey                    : 9

    Interface Name          : Vlanif1023
    State                   : up
    Access Port             : false
    Last Up Time            : 2012/07/06 15:38:40
    Total Up Time          : 0 days, 1 hours, 27 minutes, 56 seconds

  **PW Information:

   *Peer Ip Address        : 10.3.3.9
    PW State               : up
    Local VC Label         : 1027
    Remote VC Label        : 1026
    PW Type                : label
    Local  VCCV            : alert lsp-ping bfd
    Remote VCCV            : alert lsp-ping bfd
    Tunnel ID              : 0x1
    Broadcast Tunnel ID    : 0x1
    Broad BackupTunnel ID  : 0x0
    Ckey                   : 0xc
    Nkey                   : 0x9
    Main PW Token          : 0x1
    Slave PW Token         : 0x0
    Tnl Type               : LSP
    OutInterface           : Vlanif1025
    Backup OutInterface    :
    Stp Enable             : 0
    PW Last Up Time        : 2012/07/06 15:38:56
    PW Total Up Time       : 0 days, 1 hours, 27 minutes, 40 seconds
```

Table 10-116 Description of the **display vsi verbose** command output

Item	Description
VSI Name	Name of the VSI.
Administrator VSI	Whether the VSI is an administrator VSI: ● yes ● no
Isolate Spoken	Whether the forwarding isolation function is enabled: ● enable ● disable
VSI Index	Index of the VSI.
PW Signaling	Type of the PW signaling, which can be ldp, bgp, bgpad or ldp bgpad. To set the value, run the **pwsignal** or **bgp-ad** command.
Member Discovery Style	Member discovery mode, which can be auto or static.
PW MAC Learn Style	Mode of MAC address learning of the PW.

Item	Description
Encapsulation Type	VPLS encapsulation type of the VSI: - VLAN - Ethernet If the PW encapsulation types on both ends are different, run the **encapsulation** { **ethernet** | **vlan** } command in the VSI view to change the encapsulation type on one end to be the same as that on the other end.
MTU	Maximum transmission unit. If the MTU values on both ends are different, run the **mtu** *mtu-value* command in the VSI view to change the MTU values on one end to be the same as that on the other end.
Diffserv Mode	VSI QoS mode.
Mpls Exp	EXP priority in MPLS packets.
DomainId	ID of a domain.
Domain Name	Domain name.
Ignore AcState	Whether the **vpls ignore-ac-state** command is used to prevent the status of a VSI from being affected by the status of the Attachment Circuit (AC).
P2P VSI	A P2P VSI identifier, which can be: - enable: indicates that the VSI is a P2P VSI. - disable: indicates that the VSI is not a P2P VSI.
Create Time	Time when the VSI is created.
VSI State	Status of the VSI: - up - down - administratively down
BGP RD	Route distinguisher. The BGP RD is an identifier on the local device for identifying a VSI on the PE in BGP VPLS. This item is displayed only when the VPLS type is Kompella.
SiteID/Range/Offset	Site ID, site range (the number of sites), and initial site ID offset of the VSI on the local device. This item is displayed only when the VPLS type is Kompella.
Import vpn target	Inbound extended community attribute from the target VPN. This item is displayed only when the VPLS type is Kompella.

Item	Description
Export vpn target	Outbound extended community attribute to the target VPN. This item is displayed only when the VPLS type is Kompella.
Remote Label Block	Initial value, label range, and initial site ID offset of the remote label block. This item is displayed only when the VPLS type is Kompella.
Local Label Block	Initial value, label range, and initial site ID offset of the local label block. This item is displayed only when the VPLS type is Kompella.
VSI ID	VSI ID that is displayed only when the Martini VPLS is configured. If the VSI IDs or negotiation IDs on both ends are different, run the **vsi-id** *vsi-id* or **peer (VSI-LDP view)** command in the VSI-LDP view to change the VSI ID or negotiation ID on one end to be the same as that on the other end.
Peer Router ID	ID of the peer device. This item is displayed only when the VPLS type is Martini.
Negotiation-vc-id	VC ID for negotiation.
primary or secondary	Whether the PW is a primary PW or a secondary PW.
ignore-standby-state	Whether the PW ignores the secondary state sent from the peer device. yes: Ignore the secondary state sent from the peer device. no: Do not ignore the secondary state sent from the peer device.
VC Label	Label value of the VC. This item is displayed only when the VPLS type is Martini.
Peer Type	PW type of the peer, which can be Dynamic or Static. This item is displayed only when the VPLS type is Martini.
Session	Status of the session between the local end and its peer. The status can be Up or Down. This item is displayed only when the VPLS type is Martini.
Tunnel ID	Tunnel ID that is displayed only when the Martini VPLS is configured.
Broadcast Tunnel ID	Tunnel ID (for broadcast).
Broad BackupTunnel ID	ID of the selected backup broadcast tunnel.
CKey	Index of the public tunnel for VPN QoS.
NKey	Index of the public tunnel.

Item	Description
Stp Enable	Whether STP for PW is enabled: ● 0: disabled ● 1: enable
PwIndex	PW index.
Control Word	Whether the control word is enabled for the local end on the PW: ● enable: The control word is enabled. ● disable: The control word is disabled.
BFD for PW	Whether BFD is configured: ● unavailable: not configured ● available: configured ● timeout: timeout period after which a BFD session fails to be established
Interface Name	Name of the interface bound to the VSI.
Access Port	Whether the interface supports the access-port attribute: ● true: indicates that the interface supports the access-port attribute. ● false: indicates that the interface does not support the access-port attribute.
State	Status of the AC bound to the VSI. ● up ● down
Last Up Time	Last time when the AC interface goes Up.
Total Up Time	Total time when the AC interface is Up.
PW Information	Information about the PW.
Peer Ip Address	IP addresses of the peer.
PW State	Status of the PW. ● up ● down ● backup
Local VC Label	VC label distributed locally.
Remote VC Label	VC label distributed by the peer.

Item	Description
Remote Control Word	Whether the control word is enabled for the remote end on the PW: ● enable: The control word is enabled. ● disable: The control word is disabled.
PW Type	Type of the PW.
Local VCCV	Type of VCCV supported on the local device.
Remote VCCV	Type of VCCV supported on the remote device.
Tunnel ID	Tunnel ID.
Main PW Token	Token of the master PW.
Slave PW Token	Token of the slave PW.
Tnl Type	Type of a tunnel. ● LSP ● CR-LSP ● GRE ● Other
OutInterface	Outbound interface.
Backup OutInterface	Outbound interface of the selected backup broadcast tunnel.
PW Last Up Time	Last time when the PW goes Up.
PW Total Up Time	Total time when the PW is Up.

# Display detailed information about the BGP VSI named **bgp1**.

```
<HUAWEI> display vsi name bgp1 verbose

 ***VSI Name               : bgp1
    Administrator VSI      : no
    Isolate Spoken         : disable
    VSI Index              : 6
    PW Signaling           : bgp
    Member Discovery Style : auto
    PW MAC Learn Style     : unqualify
    Encapsulation Type     : vlan
    MTU                    : 1500
    Diffserv Mode          : uniform
    Mpls Exp               : --
    DomainId               : 255
    Domain Name            :
    Ignore AcState         : disable
    P2P VSI                : disable
    Create Time            : 2 days, 20 hours, 19 minutes, 16 seconds
    VSI State              : up

    BGP RD                 : 172.16.1.1:1
    SiteID/Range/Offset    : 1/5/0
```

```
  Import vpn target      : 100:1
  Export vpn target      : 100:1
  Remote Label Block     : 35840/5/0
  Local Label Block      : 0/35840/5/0

  Interface Name         : Vlanif1022
  State                  : up
  Access Port            : false
  Last Up Time           : 2012/08/06 03:24:45
  Total Up Time          : 0 days, 0 hours, 10 minutes, 11 seconds

**PW Information:

 *Peer Ip Address        : 10.3.3.9
  PW State               : up
  Local VC Label         : 35843
  Remote VC Label        : 35841
  PW Type                : label
  Local  VCCV            : alert lsp-ping bfd
  Remote VCCV            : alert lsp-ping bfd
  Tunnel ID              : 0x2e4d
  Broadcast Tunnel ID    : 0x2e4d
  Broad BackupTunnel ID  : 0x0
  Ckey                   : 0x17
  Nkey                   : 0x15
  Main PW Token          : 0x2e4d
  Slave PW Token         : 0x0
  Tnl Type               : LSP
  OutInterface           : Vlanif20
  Backup OutInterface    :
  Stp Enable             : 0
  PW Last Up Time        : 2012/08/06 03:25:12
  PW Total Up Time       : 0 days, 0 hours, 9 minutes, 44 seconds
```

Table 10-117 Description of the **display vsi name bgp1 verbose** command output

Item	Description
VSI Name	Name of the VSI.
Administrator VSI	Whether the VSI is an administrator VSI: ● yes: It is an administrator VSI. ● no: It is not an administrator VSI.
Isolate Spoken	Whether the forwarding isolation function is enabled: ● enable ● disable
VSI Index	Index of the VSI.
PW Signaling	Type of the PW signaling, which can be ldp, bgp, bgpad or ldp bgpad.
Member Discovery Style	Member discovery mode, which can be auto or static.
PW MAC Learn Style	Mode of MAC address learning of the PW.

Item	Description
Encapsulation Type	VPLS encapsulation type of the VSI, namely, the encapsulation type of the packets transmitted over the VC: ● VLAN ● Ethernet If the PW encapsulation types on both ends are different, run the **encapsulation** { **ethernet** | **vlan** } command in the VSI view to change the encapsulation type on one end to be the same as that on the other end.
MTU	Maximum transmission unit. If the MTU values on both ends are different, run the **mtu** *mtu-value* command in the VSI view to change the MTU values on one end to be the same as that on the other end.
Diffserv Mode	VSI QoS mode.
Mpls Exp	EXP priority in MPLS packets.
DomainId	ID of a domain.
Domain Name	Domain name.
Ignore AcState	Whether the **vpls ignore-ac-state** command is used to prevent the status of a VSI from being affected by the status of the AC.
Create Time	Time when the VSI is created.
VSI State	Status of the VSI: ● up ● down ● administratively down
BGP RD	Route distinguisher. The BGP RD is an identifier on the local device for identifying a VSI on the PE in BGP VPLS. This item is displayed only when the VPLS type is Kompella.
SiteID/Range/Offset	Site ID, site range (the number of sites), and initial site ID offset of the VSI on the local device. This item is displayed only when the VPLS type is Kompella.
Import vpn target	Inbound extended community attribute from the target VPN.
Export vpn target	Outbound extended community attribute to the target VPN.

Item	Description
Local Label Block	Initial value, label range, and initial site ID offset of the local label block.

# Display information about the BGP AD VSI named **vplsad1**.

```
<HUAWEI> display vsi name vplsad1
Vsi                          Mem    PW   Mac       Encap     Mtu   Vsi
Name                          Disc   Type Learn     Type      Value State
--------------------------------------------------------------------------
vplsad1                      --     bgpad   unqualify vlan      1500  up
```

# Display detailed information about the BGP AD VSI.

```
<HUAWEI> display vsi name vplsad1 verbose

 ***VSI Name               : vplsad1
    Administrator VSI      : no
    Isolate Spoken         : disable
    VSI Index              : 2
    PW Signaling           : bgpad
    Member Discovery Style : --
    PW MAC Learn Style     : unqualify
    Encapsulation Type     : vlan
    MTU                    : 1500
    Diffserv Mode          : uniform
    Mpls Exp               : --
    DomainId               : 255
    Domain Name            :
    Ignore AcState         : disable
    P2P VSI                : disable
    Create Time            : 0 days, 1 hours, 59 minutes, 39 seconds
    VSI State              : up

    VPLS ID                : 172.16.1.1:1
    RD                     : 172.16.1.1:1
    Import vpn target      : 100:1
    Export vpn target      : 100:1
    VSI ID                 : 1.1.1.9

   *Peer Router ID         : 10.3.3.9
    VPLS ID                : 172.16.1.1:1
    SAII                   : 1.1.1.9
    TAII                   : 10.3.3.9
    VC Label               : 1027
    Peer Type              : dynamic
    Session                : up
    Tunnel ID              : 0x1
    Broadcast Tunnel ID    : 0x1
    CKey                   : 12
    NKey                   : 9

    Interface Name         : Vlanif1023
    State                  : up
    Access Port            : false
    Last Up Time           : 2012/07/06 15:38:40
    Total Up Time          : 0 days, 1 hours, 59 minutes, 11 seconds

  **PW Information:

   *Peer Ip Address        : 10.3.3.9
    PW State               : up
    Local VC Label         : 1027
    Remote VC Label        : 1026
    PW Type                : label
    Local  VCCV            : alert lsp-ping bfd
    Remote VCCV            : alert lsp-ping bfd
    Tunnel ID              : 0x1
    Broadcast Tunnel ID    : 0x1
    Broad BackupTunnel ID  : 0x0
    Ckey                   : 0xc
    Nkey                   : 0x9
    Main PW Token          : 0x1
    Slave PW Token         : 0x0
    Tnl Type               : LSP
    OutInterface           : Vlanif1025
    Backup OutInterface    :
    Stp Enable             : 0
    PW Last Up Time        : 2012/07/06 15:38:56
    PW Total Up Time       : 0 days, 1 hours, 58 minutes, 55 seconds
```

Table 10-118 Description of the **display vsi name vplsad1 verbose** command output

Item	Description
PW Signaling	Type of the PW signaling, which can be ldp, bgp, bgpad or ldp bgpad.
Member Discovery Style	Member discovery mode: ● auto: indicates automatic member discovery. When creating a VSI on a Kompella VPLS network, configure **auto** in the **vsi** command. ● static: indicates static member discovery. When creating a VSI on a Martini VPLS network, configure **static** in the **vsi** command. ● --: When creating a VSI on a BGP AD VPLS network, do not configure the member discovery mode in the **vsi** command.
VPLS ID	Identifier for identifying a BGP AD VSI on various PEs.
RD	Route Distinguisher, which is the same as the VPLS ID in the BGP AD VSI.
SAII	Source Attachment Individual Identifier, which is a local IP address used during negotiation on the creation of a PW in the BGP AD VSI.
TAII	Target Attachment Individual Identifier, which is a remote IP address used during negotiation on the creation of a PW in the BGP AD VSI.

# Display detailed information of PW status of peers to all VSIs.

```
<HUAWEI> display vsi peer-info

VSI Name: a2                                    Signaling: ldp
-------------------------------------------------------------------
Peer              Transport  Local      Remote      VC
Addr              VC ID/TAII  VC Label   VC Label    State
-------------------------------------------------------------------
10.3.3.9            2          1026       1025        up
```

# Display detailed information of PW status of a specific peer to a specified VSI.

```
<HUAWEI> display vsi name a2 peer-info 10.3.3.9

VSI Name: a2                              Signaling: ldp
-------------------------------------------------------------------
Peer            Transport  Local      Remote      VC
Addr             VC ID/TAII  VC Label   VC Label    State
-------------------------------------------------------------------
10.3.3.9           2          1026       1025        up
```

Table 10-119 Description of the **display vsi peer-info** command output

Item	Description
Vsi Name	Name of the VSI.
Signaling	Signaling mode, which can be ldp, bgp, bgpad or ldp bgpad.
Peer Addr	IP addresses of the peer.
Transport VC ID/TAII	● VC ID for an LDP PW ● TAII for a BGP-AD PW
Local VC Label	VC label distributed locally.
Remote VC Label	VC label distributed by the peer.
VC State	Status of the PW. ● up ● down

# Display statistics about PW status of peers to all VSIs.

```
<HUAWEI> display vsi peer-info statistics
Total Local Peers: 1          1 Up          0 Down
--------------------------------------------------------
Vsi Name                       Up Peers       Down Peers
--------------------------------------------------------
a2                            1             0
```

# Display statistics about PW status of peers to a specified VSI.

```
<HUAWEI> display vsi name a2 peer-info statistics
Vsi Name                       Up Peers       Down Peers
--------------------------------------------------------
a2                            1             0
```

Table 10-120 Description of the **display vsi peer-info statistics** command output

Item	Description
Total Local Peers	Total number of remote peers to the local end, that is, total number of PWs.
Up	Total number of PWs in Up state.
Down	Total number of PWs in Down state.

Item	Description
Vsi Name	Name of the VSI.
Up Peers	Total number of PWs in Up state in a specified VSI.
Down Peers	Total number of PWs in Down state in a specified VSI.

10.7.28 display vsi bgp-ad

Function

The **display vsi bgp-ad** command displays the VPN targets of the local and remote devices in a BGP AD VPLS domain.

Format

display vsi bgp-ad { **export-vt** | **import-vt** | **remote-export-vt** }

Parameters

Parameter	Description	Value
export-vt	Displays local export VPN targets, namely, the export VPN targets of all local BGP AD VSIs.	-
import-vt	Displays local import VPN targets, namely, the import VPN targets of all local BGP AD VSIs.	-
remote-export-vt	Displays remote export VPN targets, namely, VPN targets received from BGP AD peers.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

When you configure or debug BGP AD VPLS, you can run the **display vsi bgp-ad** command to check the correctness of VPN targets that are locally configured or sent from peers.

Prerequisites

BGP AD VPLS member information has been configured on the local or remote end.

Precautions

When you run the **display vsi bgp-ad** command:

- To view import VPN targets that are configured locally, specify **import-vt** in the command.
- To view export VPN targets that are configured locally, specify **export-vt** in the command.
- To view export VPN targets that are sent from peers, specify **remote-export-vt** in the command.

Example

# Display local import VPN targets in a BGP AD VPLS domain.

```
<HUAWEI> display vsi bgp-ad import-vt
import vpn target list:
  100:1           192.168.12.4:100    312:250
  192.168.120.220:53364  100:100          5.5.5.5:13
  312:250
```

# Display local export VPN targets in a BGP AD VPLS domain.

```
<HUAWEI> display vsi bgp-ad export-vt
export vpn target list:
  100:1           192.168.12.4:100    312:250
  192.168.120.220:53364  100:100          5.5.5.5:13
  312:250
```

# Display remote export VPN targets in a BGP AD VPLS domain.

```
<HUAWEI> display vsi bgp-ad remote-export-vt
remote export vpn target list:
  100:1           192.168.12.4:100    312:250
  192.168.120.220:53364  100:100          5.5.5.5:13
  312:250
```

Table 10-121 Description of the display vsi command output

Item	Description
import vpn target list	List of import VPN targets configured locally.
export vpn target list	List of export VPN targets configured locally.
remote export vpn target list	List of export VPN targets sent from remote BGP AD PEs.

10.7.29 display vsi bgp-ad remote

Function

The **display vsi bgp-ad remote** command displays information about a specified remote peer of a PE in a BGP AD VPLS domain.

Format

display vsi bgp-ad remote vpls-id *vpls-id*

Parameters

Parameter	Description	Value
vpls-id *vpls-id*	Specifies the VPLS ID of a remote peer.	A VPLS ID is in one of the following formats: ● 16-bit AS number: a 32-bit user-defined number, for example, 1:3. The AS number ranges from 0 to 65535. The user-defined number ranges from 0 to 4294967295. The AS number and the user-defined number cannot both be 0. That is, a VPN target cannot be 0:0. ● 32-bit IP address: a 16-bit user-defined number, for example, 192.168.122.15:1. The IP address ranges from 0.0.0.0 to 255.255.255.255. The user-defined number ranges from 0 to 65535. ● Integral 4-byte AS number:2-byte user-defined number, for example, 65537:3. An AS number ranges from 65536 to 4294967295. A user-defined number ranges from 0 to 65535. The AS number and user-defined number cannot be both 0s. That is, a VPN target cannot be 0:0. ● 4-byte AS number in dotted notation:2-byte user-defined number, for example, 0.0:3 or 0.1:0. A 4-byte AS number in dotted notation is in the format of *x.y*, where *x* and *y* are integers that range from 0 to 65535. A user-defined number ranges from 0 to 65535. The AS number and user-defined number cannot be both 0s. That is, a VPN target cannot be 0.0:0.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

When you configure or debug BGP AD VPLS, the **display vsi bgp-ad remote** command can be used to display information about a remote peer in a BGP AD VSI such as the VPLS ID, VSI ID, and ERT configured on that peer.

Example

# Display information about a BGP AD peer with the VPLS ID of 10.1.1.1:1.

```
<HUAWEI> display vsi bgp-ad remote vpls-id 10.1.1.1:1
BGP AD Network Layer Reachability Information
----------------------------------------------
 *Peer            :3.3.3.9
  VPLS ID          :10.1.1.1:1
  VSI ID          :3.3.3.9
  VSI index        :2
  Export vpn target:100:1
----------------------------------------------
```

Table 10-122 Description of the display vsi bgp-ad remote command output

Item	Description
Peer	Peer IP address.
VPLS ID	VPLS ID configured on the remote peer. To set the value, run the **vpls-id** command.
VSI ID	VSI ID configured on the remote peer. To set the value, run the **vsi-id** command.
VSI index	Local VSI index matching BGP AD network layer reachability information sent by the remote peer.
Export vpn target	List of export VPN targets sent from the remote peer.

10.7.30 display vsi mac-withdraw loop-detect

Function

The **display vsi mac-withdraw loop-detect** command displays information about MAC withdraw loop detection.

Format

display vsi [**name** *vsi-name*] **mac-withdraw loop-detect**

Parameters

Parameter	Description	Value
name *vsi-name*	Specifies the name of a VSI.	The value is an existing VSI.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After you enable MAC withdraw loop detection, run the **display vsi mac-withdraw loop-detect** command to view information about MAC withdraw loop detection. If you specify **name** *vsi-name*, the command output shows information about MAC withdraw loop detection in a specified VSI. If you do not specify **name** *vsi-name*, the command output shows information about MAC withdraw loop detection in all VSIs.

Example

# Display information about MAC withdraw loop detection in all VSIs.

```
<HUAWEI> display vsi mac-withdraw loop-detect
Total number of vsi detect loop is 2.
Support max hop 255.

Vsi name        : VSI1
Last loop type  : detect loop
Send peer       : 10.5.5.5
Receive peer    : 10.2.2.2
Last loop time  : 2012/10/26 11:35:59

Vsi name        : VSI2
Last loop type  : exceed max hop
Send peer       : 10.5.5.5
Receive peer    : 10.3.3.3
Last loop time  : 2012/10/26 11:35:59
```

# Display information about MAC withdraw loop detection in VSI1.

```
<HUAWEI> display vsi name VSI1 mac-withdraw loop-detect
Vsi name        : VSI1
Last loop type  : detect loop
Send peer       : 10.5.5.5
Receive peer    : 10.2.2.2
Last loop time  : 2012/10/26 11:35:59
```

Table 10-123 Description of the **display vsi mac-withdraw loop-detect** command output

Item	Description
Total number of vsi detect loop	Number of MAC Withdraw message loops.
Support max hop 255	Indicates that the maximum number of hops supported by MAC Withdraw loop detection is 255.
Vsi name	Name of the VSI in which a MAC Withdraw message loop occurred.

Item	Description
Last loop type	Type of the MAC Withdraw message loop. The values are as follows: ● **detect loop**: The PE detects that a MAC Withdraw message loop occurs. ● **exceed max hop**: The number of hops for forwarding MAC Withdraw messages exceeds the maximum number of hops.
Send peer	Peer to which MAC Withdraw messages are sent.
Receive peer	Peer from which MAC Withdraw messages are received.
Last loop time	Time when the MAC Withdraw message loop occurs.

10.7.31 display vsi protect-group

Function

The **display vsi protect-group** command displays information about the PW protection group of a specified VSI.

Format

display vsi name *vsi-name* **protect-group** [*group-name* [**verbose** | **history**]]

Parameters

Parameter	Description	Value
name *vsi-name*	Specifies the VSI name.	The value is an existing VSI name.
group-name	Specifies the name of a PW protection group.	The value is an existing PW protection group.
verbose	Displays detailed information.	-
history	Displays historical switchover information about PWs in a PW protection group.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

After a PW protection group is configured, you can run the **display vsi protect-group** command to view summary or detailed information about the PW protection group of a specified VSI and check whether PW configurations have taken effect. When maintaining a PW protection group, you can track the running status of the group by viewing historical switchover information about PWs in the group.

Prerequisites

A PW protection group has been created and the primary and secondary PWs have jointed the group.

Example

# Display summary information about the PW protection group of VSI vsi1.

```
<HUAWEI> display vsi name vsi1 protect-group

Vsi name: vsi1
Protect group num: 1

Protect-group: vsi1
-------------------------------------------------------------------------------
PeerIp:VcId                Pref   Active
-------------------------------------------------------------------------------
3.3.3.3:10                 2      Active
3.3.3.9:10                 4      Inactive
```

Table 10-124 Description of the **display vsi protect-group** command output

Item	Description
Vsi name	VSI name.
Protect group num	Number of a PW protection group.
Protect-group	Name of a PW protection group.
PeerIp:VcId	Peer IP address of a PW:VC ID. This pair uniquely identifies a PW.
Pref	PW priority specified by running the **peer preference** command in the protect-group view.

Item	Description
Active	Forwarding status of a PW: ● Active: The PW can send service packets. ● Inactive: The PW cannot send service packets, but can send OAM packets if the PW is Up.

# Display detailed information about the PW protection group group1 of VSI vsi1.

```
<HUAWEI> display vsi name vsi1 protect-group group1 verbose

Vsi name           : vsi1
Protect group      : group1
Protect mode       : PW redundancy master
Reroute policy     : delay 30s
Last change time   : 2012/11/27 11:11:55
Last change action : 3.3.3.9:10 to 3.3.3.3:10
Last change reason : config changed
Holdoff remain time: --
Reroute remain time: --

Members            :
 PeerIp:VcId               Pri/Sec   Active

 3.3.3.3:10                Primary   Active
 3.3.3.9:10                Secondary Inactive
```

Table 10-125 Description of the **display vsi protect-group** command output

Item	Description
Protect mode	PW redundancy mode of a PW protection group: PW redundancy master: The PW redundancy mode is master/slave.
Reroute policy	Revertive switching policy of a PW protection group. The default revertive switching delay is 30s. In master/ slave mode, you can modify the revertive switching policy by running the **reroute** command in the protect-group view.
Last change time	Last PW switching time.
Last change action	Last PW switching action. A PW is uniquely identified by peerIP:VcID.

Item	Description
Last change reason	Reason for last PW switching: ● manual force switch: The PW switching is triggered by the **protect-switch force** command. ● manual clear switch: The PW switching is triggered by the **protect-switch clear** command. ● config changed: The PW switching is triggered by configuration changes such as PW addition, PW deletion, or PW priority changes. ● fault detected: The PW switching is triggered by failures detected by BFD or VCCV. ● PW down: The PW switching occurs because the active PW goes Down. ● PW up: The PW switching occurs because the active PW goes Up again.
Holdoff remain time	Remaining time before a switching is performed. **NOTE** If the value is **--**, no switching delay is configured.
Reroute remain time	Remaining time before a revertive switching is performed. **NOTE** If the value is **--**, no revertive switching delay is configured.
Members	Displays members in a PW protection group.
Pri/Sec	Primary/secondary status of a PW: ● Primary: The PW is a primary PW. ● Secondary: The PW is a secondary PW.

# Display historical switchover information about PWs in PW protection group group1 of VSI vsi1.

```
<HUAWEI> display vsi name vsi1 protect-group group1 history

Vsi name      : vsi1
Protect group : group1

Date/Time     : 2012/11/27 11:05:40
Action        : 3.3.3.9:10 to 3.3.3.3:10
Reason        : manual clear switch

Date/Time     : 2012/11/27 11:06:29
Action        : 3.3.3.3:10 to 3.3.3.9:10
Reason        : manual force switch

Date/Time     : 2012/11/27 11:06:48
Action        : 3.3.3.9:10 to 3.3.3.3:10
Reason        : PW down

Date/Time     : 2012/11/27 11:11:31
Action        : 3.3.3.3:10 to 3.3.3.9:10
Reason        : PW up
```

```
Date/Time     : 2012/11/27 11:11:55
Action        : 3.3.3.9:10 to 3.3.3.3:10
Reason        : config changed
```

Table 10-126 Description of the **display vsi protect-group history** command output

Item	Description
Date/Time	PW switching time. For example, 2011-08-09 16:31:32 indicates that PW switching occurred on 16:31:32 of August 9, 2011.
Action	PW switching action. A PW is uniquely identified by peerIP:VcID.
Reason	Reason for PW switching: ● manual force switch: The PW switching is triggered by the **protect-switch force** command. ● manual clear switch: The PW switching is triggered by the **protect-switch clear** command. ● config changed: The PW switching is triggered by configuration changes such as PW addition, PW deletion, or PW priority changes. ● fault detected: The PW switching is triggered by failures detected by BFD or VCCV. ● PW down: The PW switching occurs because the active PW goes Down. ● PW up: The PW switching occurs because the active PW goes Up again.

10.7.32 display vsi pw out-interface

Function

The **display vsi pw out-interface** command displays information about the outgoing interface of a VSI PW.

Format

display vsi pw out-interface [**vsi** *vsi-name*]

Parameters

Parameter	Description	Value
vsi *vsi-name*	Specifies the name of a VSI.	The value is an existing VSI.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

You can run the **display vsi pw out-interface** command to view information about the actual outgoing interface of the PW.

Precautions

This command applies to the Martini VPLS PW and BGP-AD VPLS PW.

Example

# Display information about the outgoing interface of the VSI PW.

```
<HUAWEI> display vsi pw out-interface
Total: 2
-------------------------------------------------------------------------------
Vsi Name                       peer          vcid       interface
-------------------------------------------------------------------------------
a2                          3.3.3.9         2          Vlanif1025

vplsad1                       3.3.3.9         --         Vlanif1025
```

Table 10-127 Description of the display vsi pw out-interface command output

Item	Description
Vsi Name	VSI name.
peer	VSI peer.
vcid	VC ID.
interface	Outgoing interface of a VSI PW.

10.7.33 display vsi remote

Function

The **display vsi remote** command displays information about a remote VSI.

Format

display vsi remote ldp [**router-id** *ip-address*] [**pw-id** *pw-id*]

display vsi remote bgp [**nexthop** *nexthop-address* [**export-vpn-target** *vpn-target*] | **route-distinguisher** *route-distinguisher*]

display vsi remote ldp129 [**vpls-id** *vpls-id* [**router-id** *ip-address*]]

display vsi remote fec129 [**vpls-id** *vpls-id* [**router-id** *ip-address*]] [**verbose**]

display vsi remote ldp verbose

Parameters

Parameter	Description	Value
ldp	Displays information about remote VSIs using LDP signaling.	-
bgp	Displays information about remote VSIs using BGP signaling.	-
ldp129	Displays information about remote VSIs using LDP 129 signaling.	-
fec129	Displays information about remote VSIs using FEC 129 signaling.	-
vpls-id *vpls-id*	Specifies the ID of a VPLS domain to which multiple VSIs on PEs belong.	The *vpls-id* value has four formats. For details, see **Table 10-128**.
router-id *ip-address*	Displays the information about the remote VSIs of the specified peer. *ip-address* specifies an IPv4 address of the peer.	The value is in dotted decimal notation. If you set the **router id** parameter to 255.255.255.255, the remote VSIs of all peers are displayed.
pw-id *pw-id*	Displays the information about the remote VSIs of the specified PW. *pw-id* specifies the ID of a VC, which uniquely identifies a VC.	The value is an integer that ranges from 1 to 4294967295.
nexthop *nexthop-address*	Displays the label block sent by the remote end according to the next hop address of the label block.	The value is in dotted decimal notation.

Parameter	Description	Value
export-vpn-target *vpn-target*	Displays the label block sent by the remote end according to the next hop address of the label block and the route attributes in the outgoing direction.	The value is a string that ranges from 3 to 21.
route-distinguisher *route-distinguisher*	Displays the label block sent by the remote end according to the RD.	RD is short for route distinguisher. The *route-distinguisher* value has four formats. For details, see **Table 10-128**.
verbose	Display detailed information about the remote VSIs.	-

Table 10-128 Values of *vpls-id* and *route-distinguisher*

vpls-id and *route-distinguisher* Value Format	Value	Example
16-bit AS number:32-bit user-defined number	An AS number ranges from 0 to 65535, and a user-defined number ranges from 0 to 4294967295. The AS number and user-defined number cannot be both 0. That is, a VPLS ID or RD cannot be 0:0.	101:3
Integral 4-byte AS number:2-byte user-defined number	An AS number ranges from 65536 to 4294967295. A user-defined number ranges from 0 to 65535. The AS number and user-defined number cannot be both 0s. That is, a VPLS ID or RD cannot be 0:0.	65537:3
4-byte AS number in dotted notation:2-byte user-defined number. A 4-byte AS number in dotted notation is in the format of *x.y*	The *x* and *y* are integers that range from 1 to 65535 and from 0 to 65535, respectively. A user-defined number ranges from 0 to 65535. The AS number and user-defined number cannot be both 0s. That is, a VPLS ID or RD cannot be 0.0:0.	0.0:3 or 0.1:0
32-bit IP address:16-bit user-defined number	An IPv4 address ranges from 0.0.0.0 to 255.255.255.255, and a user-defined number ranges from 0 to 65535.	192.168.122.15:1

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

To view information about remote VSIs, configure one of the following parameters in the **display vsi remote** command:

- Run the **display vsi remote ldp** command on a Martini VPLS network.
- Run the **display vsi remote bgp** command on a Kompella VPLS network.
- Run the **display vsi remote ldp129** or **display vsi remote fec129** command on a BGP AD VPLS network.

Example

# Display information about the remote VSIs using LDP signaling.

```
<HUAWEI> display vsi remote ldp
Vsi       Peer            VC      Group   Encap      MTU    Vsi    State
ID        RouterID          Label   ID      Type       Value  Index  Code
2         10.3.3.9        1025     0       vlan       1500   0      FORWARD
```

Table 10-129 Description of the display vsi remote ldp command output

Item	Description
Vsi ID	ID of the VSI.
Peer RouterID	Peer IP address.
VC Label	VC label.
Group ID	Group ID.
Encap Type	PW encapsulation type: ● vlan ● ethernet
MTU Value	MTU value.
Vsi Index	Index of the VSI.

Item	Description
State Code	Remote state code: ● FORWARD: indicates that forwarding is supported. ● NO FORWARD: indicates that forwarding is not supported. ● STANDBY: indicates the secondary PW. ● AC FAULT: indicates that the peer AC interface is faulty. ● PSN FAULT: indicates that a fault occurs on the public network between the local end and peer end. ● -: indicates that the interworking mode negotiated between two devices is Martini.

# Display information about the remote VSIs using BGP signaling.

```
<HUAWEI> display vsi remote bgp
   Total Number       : 1
 **BGP RD             : 10.1.1.2:1
   Ref Number         : 1
   NextHop            : 10.3.3.9
   EncapType          : vlan
   MTU                : 1500
   Export vpn target  : 100:1
   SiteID             : 2
   Remote Label Block : 100001/5/0
```

Table 10-130 Description of the display vsi remote bgp command output

Item	Description
Total Number	Number of the remote VSIs using BGP signaling.
BGP RD	RD of the local VSI.
Ref Number	Serial number of the remote VSI.
NextHop	Next hop address.
EncapType	Encapsulation type: ● vlan ● ethernet
MTU	Maximum transmission unit.
Export vpn target	RT in the outgoing direction.
SiteID	Site ID of the remote VSI.
Remote Label Block	Remote label block.

# Display information about the remote VSIs using LDP 129 signaling.

```
<HUAWEI> display vsi remote fec129
Codes: C(Control word), A(Alert), T(TTL), P(LSP-Ping), B(BFD)
      S(Support), N(No support)
--------------------------------------------------------------------------------
VPLS        Peer      VC        Source    Encap          MTU   VSI   VCCV
ID          RouterID  Label     AII       Type           Value Index |C|A|T|P|B|
--------------------------------------------------------------------------------
10.1.1.1:1  10.3.3.9  1026      10.3.3.9  vlan           1500  2     |N|S|N|S|N|
```

Table 10-131 Description of the display vsi remotefec129 command output

Item	Description
VPLS ID	VPLS ID of the VSI.
VCCV	Supported VCCV detection types.

# Display detailed information about remote VSIs using LDP signaling.

```
<HUAWEI> display vsi remote ldp verbose
Total remote VSI : 1

VSI ID              : 2
VSI Index           : 0
VC Type             : vlan
VC Label            : 1025
Peer Address        : 10.3.3.9
Group ID            : 0
MTU                 : 1500
Status Code         : FORWARD
Match Local VC      : MATCH
Control Word        : disable
```

Table 10-132 Description of the display vsi remote ldp verbose command output

Item	Description
Total remote VSI	Total number of remote VSIs.
VSI ID	ID of a remote VSI.
VSI Index	Index of a remote VSI.
VC Type	Remote VC encapsulation type.
VC Label	Remote VC label.
Peer Address	Remote peer address.
Group ID	Remote group ID. The default value is 0.
MTU	MTU of a remote VC.

Item	Description
Status Code	Status of a remote VC: ● FORWARD: The remote VC is in the forwarding state. ● STANDBY: The remote VC is in the standby state. ● AC FAULT: The remote AC interface is faulty. ● PSN FAULT: The remote VC is faulty. ● NO FORWARD: The remote VC cannot forward packets owing to other reasons.
Match Local VC	Whether a VC matching the remote VC ID exists on the local end: ● MATCH: A VC matching the remote VC ID exists on the local end. ● NOT-MATCH: No VC matching the remote VC ID exists on the local end.
Control Word	Whether the control word is enabled: ● enable: The control word is enabled. ● disable: The control word is disabled.

10.7.34 display vsi services

Function

The **display vsi services** command displays information about the AC interface associated with the VSI.

Format

display vsi services { **all** | *vsi-name* | **interface** *interface-type interface-number* | **vlan** *vlan-id* }

Parameters

Parameter	Description	Value
all	Displays the information about AC interfaces associated with all VSIs.	-
vsi-name	Displays the information about AC interfaces associated with the specified VSI.	The value is an existing VSI.

Parameter	Description	Value
interface *interface-type interface-number*	Specifies the type and number of the AC interface associated with the VSI. ● *interface-type* specifies the type of the interface. ● *interface-number* specifies the number of the interface.	-
vlan *vlan-id*	Displays information about the specified VLAN AC interface associated with the VSI.	The value is an integer that ranges from 1 to 4094.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The **display vsi services** command displays status of the AC interface associated with the VSI, and can be used for fault diagnosis.

Example

# Display information about the AC interfaces associated with all VSIs.

```
<HUAWEI> display vsi services all
Total: 2
Code: AS(Admin Status), PS(Physical Status)
------------------------------------------------------------------------------
Interface                      Vsi Name                     AS    PS
------------------------------------------------------------------------------
GigabitEthernet0/0/1              1                           up    up
Vlanif1024                      a2                          up    up
------------------------------------------------------------------------------
```

# Display information about the AC interface associated with the VSI named **a2**.

```
<HUAWEI> display vsi services a2
Total: 1
Code: AS(Admin Status), PS(Physical Status)
------------------------------------------------------------------------------
Interface                      Vsi Name                     AS    PS
------------------------------------------------------------------------------
Vlanif1024                      a2                          up    up
------------------------------------------------------------------------------
```

# Display information about the GE0/0/1 interface associated with the VSI.

```
<HUAWEI> display vsi services interface gigabitethernet0/0/1
Total: 1
Code: AS(Admin Status), PS(Physical Status)
------------------------------------------------------------------------------
Interface                      Vsi Name                     AS    PS
------------------------------------------------------------------------------
```

```
GigabitEthernet0/0/1              1                          down  up
--------------------------------------------------------------------------------
```

# Display information about the AC interface in VLAN 1024 associated with the VSI.

```
<HUAWEI> display vsi services vlan 1024
Total: 1
Code: AS(Admin Status), PS(Physical Status)
--------------------------------------------------------------------------------
Interface                       Vsi Name                     AS    PS
--------------------------------------------------------------------------------
Vlanif1024                        a2                         up    up
--------------------------------------------------------------------------------
```

Table 10-133 Description of the display vsi services command output

Item	Description
Interface	Name of the interface.
Vsi Name	Name of the VSI that is bound to the interface.
AS	Status of the VSI that is bound to the interface: ● up: indicates that the VSI is in Up state. ● down: indicates that the VSI is in Down state. ● *down: indicates that the VSI status is AdminDown.
PS	Physical status of the interface: ● up: indicates that the physical status of the interface is Up. ● down: indicates that the physical status of the interface is Down.

10.7.35 display vsi statistics

Function

The **display vsi statistics** command displays VSI statistics, including the PW and AC status.

Format

display vsi name *vsi-name* **statistics**

Parameters

Parameter	Description	Value
name *vsi-name*	Specifies the name of a VSI.	The value is an existing VSI.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

To check the statistics of a specified VSI, including its PW and AC status, run the **display vsi statistics** command.

Example

# Display the statistics of a VSI named **vsi1**.

```
<HUAWEI> display vsi name vsi1 statistics

 VSI Name               : vsi1
 VSI State              : up
 PW                     : 1 up, 0 down, 1 backup
 BFD for PW             : 0 up, 0 down
 AC                     : 1 up, 0 down, 0 AC OAM down
 Ignore AcState         : disable
```

Table 10-134 Description of the **display vsi statistics** command output

Item	Description
VSI Name	VSI name
VSI State	VSI status
PW	Number of PWs in each state
BFD for PW	Number of PWs (tracked by BFD) in each state
AC	Number of ACs in each state
Ignore AcState	Whether the function to ignore AC status is enabled

10.7.36 encapsulation (VSI view)

Function

The **encapsulation** command configures the encapsulation type of the interface in the VSI view.

The **undo encapsulation** command restores the encapsulation type of the interface to the default setting.

By default, the encapsulation type is VLAN.

Format

encapsulation { **ethernet** | **vlan** }

undo encapsulation ethernet

Parameters

Parameter	Description	Value
ethernet	Indicates that the encapsulation type is Ethernet.	-
vlan	Indicates the VLAN encapsulation format that meets the 802.1Q standard.	-

Views

VSI view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When you configure the VPLS function, run the **encapsulation** command to configure the encapsulation type of the interface.

Prerequisites

The following operations must have been performed before this command is used:

- The **pwsignal bgp** command and the **route-distinguisher** *route-distinguisher* command have been executed for Kompella VPLS.
- The **pwsignal ldp** command and the **vsi-id** *vsi-id* command have been executed for Martini VPLS.
- The **bgp-ad** command and the **vpls-id** *vpls-id* command have been executed for BGP AD VPLS.

Example

# Configure the encapsulation type of the current VSI as Ethernet.

```
<HUAWEI> system-view
[HUAWEI] vsi a2 static
[HUAWEI-vsi-a2] pwsignal ldp
[HUAWEI-vsi-a2-ldp] vsi-id 101
[HUAWEI-vsi-a2-ldp] quit
[HUAWEI-vsi-a2] encapsulation ethernet
```

10.7.37 encapsulation rfc4761-compatible

Function

The **encapsulation rfc4761-compatible** command enables a device to comply with RFC 4761 to encapsulate Kompella VPLS packets.

The **undo encapsulation rfc4761-compatible** command restores the default encapsulation type of Kompella VPLS packets.

By default, Kompella VPLS packets use the Huawei proprietary encapsulation type. Huawei defines 4 for VLAN encapsulation and 5 for Ethernet encapsulation for Kompella VPLS.

Format

encapsulation rfc4761-compatible

undo encapsulation rfc4761-compatible

Parameters

None

Views

VSI-BGP view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

RFC 4761 defines that the encapsulation type of Kompella VPLS packets is 19. Huawei defines 4 for VLAN encapsulation and 5 for Ethernet encapsulation for Kompella VPLS. Therefore, the encapsulation type of Kompella VPLS packets needs to be modified when Huawei devices communicate with non-Huawei devices.

When the device sends Kompella VPLS packets, run the **encapsulation rfc4761-compatible** command to enable the device to modify the encapsulation type of Kompella VPLS packets from Type 4 or 5 to Type 19. When the device receives Kompella VPLS packets, the device modifies the encapsulation type of Kompella VPLS packets from Type 19 to Type 4 or 5 automatically without running any command.

NOTE

When the device works as a PE, the encapsulation type is determined by the CE access mode. If the CE accesses the PE in VLAN mode, the PE encapsulates packets sent by the CE in Type 4. If the CE accesses the PE in Ethernet mode, the PE encapsulates packets sent by the CE in Type 5. VLAN and Ethernet modes are described as follows:

- VLAN: Ethernet frames transmitted between the CE and PE are attached with a VLAN tag. The tag is a service delimiter required by an ISP to differentiate clients. It is also called P-tag.
- Ethernet: Ethernet frames transmitted between the CE and PE do not have a service delimiter. If the header of Ethernet frames carries a VLAN tag, this tag is the inner VLAN tag of user packets, and is of no use to the PE. It is also called U-tag.

Precautions

The **encapsulation rfc4761-compatible** command is only used for Huawei and non-Huawei devices to communicate with each other.

Example

# Enable the device to comply with RFC 4761 to encapsulate Kompella VPLS packets.

```
<HUAWEI> system-view
[HUAWEI] vsi bgp1
[HUAWEI-vsi-bgp1] pwsignal bgp
[HUAWEI-vsi-bgp1-bgp] encapsulation rfc4761-compatible
```

10.7.38 flow-label (VSI-LDP view)

Function

The **flow-label** command enables flow label-based load balancing for a VSI.

The **undo flow-label** command disables flow label-based load balancing of a VSI.

By default, flow label-based load balancing for a VSI is disabled.

NOTE

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

Format

flow-label { **both** | **send** | **receive** } [**static**]

undo flow-label [{ **both** | **send** | **receive** } [**static**]]

Parameters

Parameter	Description	Value
both	Enables flow label-based load balancing for outgoing traffic and incoming traffic.	-

Parameter	Description	Value
send	Enables flow label-based load balancing for outgoing traffic.	-
receive	Enables flow label-based load balancing for incoming traffic.	-
static	Statically configures flow label-based load balancing. For dynamic PWs, if **static** is not configured, the flow label-based load balancing capability of the local end is negotiated by the remote end. For static PWs, the flow label-based load balancing capability is statically configured, irrespective of whether **static** is configured.	-

Views

VSI-LDP view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When multiple links exist between P devices on a PW, to improve L2VPN traffic forwarding efficiency and ease the forwarding burden on P devices, run the **flow-label** command to configure flow label-based load balancing. After flow label-based load balancing is enabled on a PE, the PE adds different flow labels for different L2VPN data flows to distinguish the data flows. After a P device receives a data packet carrying a flow label, it selects a forwarding path based on the flow label in the data packet. This processing implements load balancing.

To enable flow label-based load balancing for all PWs in a VSI, run the **flow-label** command in the VSI-LDP view.

Prerequisites

MPLS L2VPN has been enabled.

Precautions

Flow label-based load balancing can be enabled only when any of the following conditions is true:

- The **receive** parameter is configured on the local PE, and the **send** parameter is configured on the remote PE.
- The **send** parameter is configured on the local PE, and the **receive** parameter is configured on the remote PE.
- Both the **send** and **receive** parameters are configured on the local and remote PEs.

If the static flow label-based load balancing configuration does not match on both ends, the device discards packets carrying a flow label, causing packet loss.

Example

# Enable flow label-based load balancing for Martini VPLS.

```
<HUAWEI> system-view
[HUAWEI] vsi 1 static
[HUAWEI-vsi-1] pwsignal ldp
[HUAWEI-vsi-1-ldp] flow-label both
```

10.7.39 flow-label (VSI-LDP-PW view)

Function

The **flow-label** command enables flow label-based load balancing for an L2VPN PW.

The **undo flow-label** command disables flow label-based load balancing of an L2VPN PW.

The **flow-label disable** command disables flow label-based load balancing of an L2VPN PW.

The **undo flow-label disable** command restores flow label-based load balancing of an L2VPN PW.

By default, if flow label-based load balancing is enabled for a VSI, the PWs in this VSI also have flow label-based load balancing enabled; if flow label-based load balancing is disabled for a VSI, the PWs in this VSI also have flow label-based load balancing disabled.

NOTE

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

Format

flow-label { **both** | **send** | **receive** } [**static**]

undo flow-label [{ **both** | **send** | **receive** } [**static**]]

flow-label disable

undo flow-label disable

Parameters

Parameter	Description	Value
both	Enables flow label-based load balancing for outgoing traffic and incoming traffic.	-
send	Enables flow label-based load balancing for outgoing traffic.	-
receive	Enables flow label-based load balancing for incoming traffic.	-

Parameter	Description	Value
static	Statically configures flow label-based load balancing. For dynamic PWs, if **static** is not configured, the flow label-based load balancing capability of the local end is negotiated by the remote end. For static PWs, the flow label-based load balancing capability is statically configured, irrespective of whether **static** is configured.	-

Views

VSI-LDP-PW view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On an L2VPN carrying service traffic, when multiple links exist between Ps, flow label-based load balancing can be configured to improve traffic forwarding efficiency and reduce the forwarding pressure on the Ps. After flow label-based load balancing is enabled on a PE, the PE adds different flow labels for different L2VPN data flows to distinguish the data flows. After a P device receives a data packet carrying a flow label, it selects a forwarding path based on the flow label in the data packet. This processing implements load balancing.

To enable flow label-based load balancing for VLL PWs or PWE3 PWs, run the **flow-label** command in the PW template view, and specify the configured PW template when creating VLL PWs or PWE3 PWs.

- If flow label-based load balancing is configured for both a VSI and a PW in this VSI, the configuration of the PW takes precedence.
- If the **undo flow-label** command is run in the VSI-LDP-PW view, only the flow label-based load balancing capability that has been configured using the **flow-label** command in the VSI-LDP-PW view is disabled.
- If the **flow-label** command has been run for a VSI but not for a PW, you can run the **flow-label disable** command in the VSI-LDP-PW view to disable flow label-based load balancing of the PW. If the PW needs the flow label-based load balancing capability again, you can run the **undo flow-label disable** command to restore flow label-based load balancing.

Prerequisites

MPLS L2VPN has been enabled.

Precautions

Flow label-based load balancing can be enabled only when any of the following conditions is true:

- The **receive** parameter is configured on the local PE, and the **send** parameter is configured on the remote PE.

- The **send** parameter is configured on the local PE, and the **receive** parameter is configured on the remote PE.
- Both the **send** and **receive** parameters are configured on the local and remote PEs.

If the static flow label-based load balancing configuration does not match on both ends, the device discards packets carrying a flow label, causing packet loss.

Example

# Enable flow label-based load balancing for a PW.

```
<HUAWEI> system-view
[HUAWEI] vsi 1 static
[HUAWEI-vsi-1] pwsignal ldp
[HUAWEI-vsi-1-ldp] pw p1
[HUAWEI-vsi-1-ldp-pw-p1] flow-label both
```

# Disable flow label-based load balancing for the PW **pw1**.

```
<HUAWEI> system-view
[HUAWEI] vsi 1 static
[HUAWEI-vsi-1] pwsignal ldp
[HUAWEI-vsi-1-ldp] flow-label send
[HUAWEI-vsi-1-ldp] peer 1.1.1.1
[HUAWEI-vsi-1-ldp] peer 1.1.1.1 pw pw1
[HUAWEI-vsi-1-ldp-pw-pw1] flow-label disable
```

10.7.40 holdoff (protect-group view)

Function

The **holdoff** command configures a switching delay for a PW protection group with the master/slave PW redundancy mode.

The **undo holdoff** command deletes the switching delay for a PW protection group with the master/slave PW redundancy mode.

By default, no switching delay is configured for a PW protection group with the master/slave PW redundancy mode. In this situation, if a fault occurs on the primary PW, traffic immediately switches from the primary PW to the secondary PW.

Format

holdoff *holdoff-time*

undo holdoff

Parameters

Parameter	Description	Value
holdoff-time	Specifies the switching delay.	The value is an integer ranging from 1 to 180, in seconds.

Views

protect-group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

By default, if a working path fails, traffic immediately switches to the protection path. If the working path flaps or an error occurs in the detection mechanism, traffic frequently switches between the working and protection paths. If you want to avoid this problem in a PW protection group with the master/slave PW redundancy mode, run the **holdoff** command to configure a switching delay. If the working path recovers before the specified switching delay expires, traffic does not switch to the protection path. If the working path remains faulty after the specified switching delay expires, traffic switches to the protection path.

Prerequisites

The PW redundancy mode of the PW protection group is master/slave.

Precautions

If the **holdoff** command is run multiple times, the latest configuration overrides the previous ones.

After you configure a switching delay, traffic forwarded during the delay period will be interrupted if the primary PW fails to recover before the delay period expires.

A PW protection group with the independent PW redundancy mode does not support delayed switching.

NOTE

On a VPLS network that uses BFD for fault detection, traffic immediately switches from the primary PW to the secondary PW after BFD detects a fault on the primary PW, no matter whether delayed switching is configured. It is recommended that you determine whether to use BFD or delayed switching based on your actual network requirements.

Example

# Configure a switching delay of 60s for a PW protection group.

```
<HUAWEI> system-view
[HUAWEI] vsi vsi1
[HUAWEI-vsi-vsi1] pwsignal ldp
[HUAWEI-vsi-vsi1-ldp] protect-group group1
[HUAWEI-vsi-vsi1-ldp-protect-group-group1] protect-mode pw-redundancy master
[HUAWEI-vsi-vsi1-ldp-protect-group-group1] holdoff 60
```

10.7.41 hub-mode enable

Function

The **hub-mode enable** command sets the VSI attribute of an AC interface to hub.

The **undo hub-mode enable** command sets the VSI attribute of an AC interface to spoke.

By default, the VSI attribute of an AC interface is hub.

NOTE

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

Format

hub-mode enable

undo hub-mode enable

Parameters

None

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the **isolate spoken** command is run in the VSI view, forwarding isolation is enabled on AC interfaces in a VSI, and all AC interfaces in this VSI have their VSI attribute set to spoke. If one AC interface wants to communicate with other AC interfaces in the same VSI, run the **hub-mode enable** command on this AC interface to set its VSI attribute to hub.

Prerequisites

Interfaces have been bound to a VSI instance by running the **l2 binding** command.

Example

# Set the VSI attribute of VLANIF100 to hub.

```
<HUAWEI> system-view
[HUAWEI] mpls l2vpn
[HUAWEI-l2vpn] quit
```

```
[HUAWEI] vsi v100 static
[HUAWEI-vsi-v100] pwsignal ldp
[HUAWEI-vsi-v100-ldp] vsi-id 100
[HUAWEI-vsi-v100-ldp] quit
[HUAWEI-vsi-v100] isolate spoken
[HUAWEI-vsi-v100] quit
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] l2 binding vsi v100
[HUAWEI-Vlanif100] hub-mode enable
```

# Set the VSI attribute of GE0/0/1 to hub.

```
<HUAWEI> system-view
[HUAWEI] mpls l2vpn
[HUAWEI-l2vpn] quit
[HUAWEI] vsi v101 auto
[HUAWEI-vsi-v101] pwsignal bgp
[HUAWEI-vsi-v101-bgp] route-distinguisher 100:1
[HUAWEI-vsi-v101-bgp] quit
[HUAWEI-vsi-v101] isolate spoken
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] l2 binding vsi v101
[HUAWEI-GigabitEthernet0/0/1] hub-mode enable
```

10.7.42 ignore-ac-state

Function

The **ignore-ac-state** command enables a VSI to retain in Up state regardless of the Attachment Circuit (AC) state.

The **undo ignore-ac-state** command restores the default setting.

By default, the VSI state changes with the AC state.

Format

ignore-ac-state

undo ignore-ac-state

Parameters

None

Views

VSI view

Default Level

2: Configuration level

Usage Guidelines

To verify whether a VSI can work normally on the new network before a VPLS network migration, run the **ignore-ac-state** command in the VSI view on the new device. This command enables the VSI to retain in Up state on the new device before the AC-side device is connected to the new device. When the AC interface is Down and the PW is Up, the VSI is Up. When the AC interface is Up and the PW is Down, the VSI is still Up.

Example

# Enable a VSI to retain in Up state regardless of the AC state.

```
<HUAWEI> system-view
[HUAWEI] vsi vsi1
[HUAWEI-vsi-vsi1] pwsignal ldp
[HUAWEI-vsi-vsi1-ldp] vsi-id 2
[HUAWEI-vsi-vsi1-ldp] quit
[HUAWEI-vsi-vsi1] ignore-ac-state
```

10.7.43 ignore-mtu-match (VSI view)

Function

The **ignore-mtu-match** command enables the device to ignore the MTU matching check and re-encapsulate the sent VPLS packets.

The **undo ignore-mtu-match** command disables the device from ignoring the MTU matching check and re-encapsulating the sent VPLS packets.

By default, the device does not ignore the MTU matching check or re-encapsulate sent VPLS packets.

Format

ignore-mtu-match

undo ignore-mtu-match

Parameters

None

Views

VSI view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In the communication in Kompella mode with devices of other vendors, you can use the **ignore-mtu-match** command to ignore the MTU check for VSIs if the devices of other vendors do not support the check. By default, the PE device checks whether MTUs of the VSIs on both ends are matched. If the MTUs of the VSIs on two ends are different, the VC cannot go Up.

As defined by the latest RFC, the encapsulation type of PW in the Kompella VPLS is 19. Huawei devices support only the Ethernet encapsulation and VLAN encapsulation. In the communication in Kompella mode with devices of other vendors, you can use the **ignore-mtu-match** command if the devices of other vendors require to receive a VPLS packet with the encapsulation type as 19. After the **ignore-mtu-match command** is run, the sent VPLS packet adopts encapsulation type 19.

Prerequisites

The following operations have been performed before this command is used:

1. BGP has been configured as the PW signaling protocol using the **pwsignal bgp** command.
2. The RD of the VSI has been configured using the **route-distinguisher** *route-distinguisher* command.

Precautions

- This command is valid only for the VPLS in Kompella mode and does not take effect in the VPLS in Martini mode. In the Martini VPLS, the MTU values of the VSIs on two ends must be the same.
- Huawei devices can interwork with devices of other vendors only when the **ignore-mtu-match** command is used together with the **vpls bgp encapsulation** command.

Example

# Disable the MTU matching check of a VSI named **bgp1** and use encapsulation type 19 for the sent VPLS packet so that a Huawei device is connected to devices of other vendors.

```
<HUAWEI> system-view
[HUAWEI] vsi bgp1 auto
[HUAWEI-vsi-bgp1] pwsignal bgp
[HUAWEI-vsi-bgp1-bgp] route-distinguisher 100:1
[HUAWEI-vsi-bgp1-bgp] quit
[HUAWEI-vsi-bgp1] ignore-mtu-match
```

10.7.44 ignore-stp-loopcheck

Function

The **ignore-stp-loopcheck** command disables STP loop detection function of PW, that is, the PW that cannot be blocked by STP.

The **undo ignore-stp-loopcheck** command restores the default configuration.

By default, STP loop detection is enabled for the PW.

Format

ignore-stp-loopcheck

undo ignore-stp-loopcheck

Parameters

None

Views

VSI-LDP-PW view

Default Level

2: Configuration level

Usage Guidelines

After STP loop detection is enabled, a PW may be blocked when an STP loop is detected. If you do not want a PW to be blocked upon an STP loop, you can run this command to disable STP loop detection.

Example

# Disable STP loop detection function of the PW named pw1.

```
<HUAWEI> system-view
[HUAWEI] vsi aa static
[HUAWEI-vsi-aa] pwsignal ldp
[HUAWEI-vsi-aa-ldp] vsi-id 1
[HUAWEI-vsi-aa-ldp] peer 1.1.1.1
[HUAWEI-vsi-aa-ldp] peer 1.1.1.1 pw pw1
[HUAWEI-vsi-aa-ldp-pw-pw1] ignore-stp-loopcheck
```

10.7.45 ingress-lsp protect-mode

Function

The **ingress-lsp protect-mode** command configures the protection mode for BGP ingress LSPs.

The **undo ingress-lsp protect-mode** command restores the default setting.

By default, no protection mode is configured for BGP ingress LSPs.

Format

ingress-lsp protect-mode bgp-frr

undo ingress-lsp protect-mode

Parameters

Parameter	Description	Value
bgp-frr	Configures the protection mode for BGP ingress LSPs to BGP Auto FRR.	-

Views

BGP view, BGP-IPv4 unicast address family view

Default Level

2: Configuration level

Usage Guidelines

To protect the links between the PE and its dual-homed ASBRs and the ASBRs themselves in the same AS, you can configure the protection mode of BGP Auto FRR.

Before configuring the protection mode of BGP Auto FRR, enable the BGP Auto FRR function.

It is recommended that the selection of labeled BGP IPv4 routes be based on the **bestroute nexthop-resolved tunnel** command.

Example

# Configure the protection mode of BGP Auto FRR for BGP ingress LSPs.

```
<HUAWEI> system-view
[HUAWEI] bgp 100
[HUAWEI-bgp] ipv4-family unicast
[HUAWEI-bgp-af-ipv4] ingress-lsp protect-mode bgp-frr
```

10.7.46 interface-parameter-type vccv (VSI-LDP-PW view)

Function

The **interface-parameter-type vccv** command restores the default setting.

The **undo interface-parameter-type vccv** command deletes the VCCV byte right after the interface parameter in the Mapping packet.

By default, a mapping packet carries the VCCV byte.

Format

interface-parameter-type vccv

undo interface-parameter-type vccv

Parameters

None

Views

VSI-LDP-PW view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If the switch communicates with the devices of VRP V300R001 and all branching versions, and the LDP VPLS is configured, run the **undo interface-parameter-type vccv** command.

Prerequisites

The following operations have been performed before this command is used:

1. LDP has been configured as the PW signaling protocol using the **pwsignal ldp** command.
2. The VSI ID has been configured using the **vsi-id** *vsi-id* command.
3. The peer of the VSI has been configured using the **peer** *peer-address* command.
4. The PW has been configured using the **peer** *peer-address* [**negotiation-vc-id** *vc-id*] **pw** *pw-name* command.

Example

# When configuring the VPLS in LDP mode, delete the VCCV byte from the Mapping packet.

```
<HUAWEI1> system-view
[HUAWEI] vsi vsi1 static
[HUAWEI-vsi-vsi1] pwsignal ldp
[HUAWEI-vsi-vsi1-ldp] vsi-id 100
[HUAWEI-vsi-vsi1-ldp] peer 2.2.2.2
[HUAWEI-vsi-vsi1-ldp] peer 2.2.2.2 pw pw1
[HUAWEI-vsi-vsi1-ldp-pw-pw1] undo interface-parameter-type vccv
```

10.7.47 interface-status-change mac-withdraw enable

Function

The **interface-status-change mac-withdraw enable** command enables the PEs to send LDP MAC Withdraw messages to all peers when the status of the AC interface bound to the VSI changes.

The **undo interface-status-change mac-withdraw enable** command disables the PEs from sending LDP MAC Withdraw messages to all peers when the status of the AC interface bound to the VSI changes.

By default, a PE does not send LDP MAC Withdraw messages when the status of the AC interface bound to the VSI changes.

Format

interface-status-change mac-withdraw enable

undo interface-status-change mac-withdraw enable

Parameters

None

Views

VSI-LDP view, VSI view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On enterprise networks, you can configure this command on the PE to enable the PE to update the MAC address entry when the AC link is in Down state. In this way, the PE connected to the SPE sends LDP MAC Withdraw messages to all peers when the status of the SPE-side interface changes.

Precautions

If the local end sends MAC-Withdraw messages, the remote VSI clears local MAC addresses and learns new MAC addresses.

After you run the **interface-status-change mac-withdraw enable** command, the PE sends LDP MAC-Withdraw messages to all peers if the status of the interface bound to the VSI changes:

- From Down to Up.
- From Up to Down.

The **interface-status-change mac-withdraw enable** takes effect only when the **mac-withdraw enable** is configured.

Example

# Enable the PE to send LDP MAC Withdraw messages to all peers when the status of the AC interface bound to the VSI changes.

```
<HUAWEI> system-view
[HUAWEI] vsi v1 static
[HUAWEI-vsi-v1] pwsignal ldp
[HUAWEI-vsi-v1-ldp] interface-status-change mac-withdraw enable
```

10.7.48 isolate spoken

Function

The **isolate spoken** command enables forwarding isolation between AC interfaces in a VSI.

The **undo isolate spoken** command disables forwarding isolation between AC interfaces in a VSI.

By default, forwarding isolation between AC interfaces in a VSI is disabled.

NOTE

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

Format

isolate spoken

undo isolate spoken

Parameters

None

Views

VSI view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If multiple users are bound to the same VSI, you can use the **isolate spoken** command to enable forwarding isolation between AC interfaces. After this command is run, the VSI attribute of all AC interfaces in the VSI is spoke, preventing the users from communicating with each other.

Prerequisites

- For Martini VPLS, the **pwsignal ldp** and **vsi-id** *vsi-id* commands have been run.
- For Kompella VPLS, the **pwsignal bgp** and **route-distinguisher** *route-distinguisher* commands have been run.
- For BGP AD VPLS, the **bgp-ad** and **vpls-id** *vpls-id* commands have been run.

Example

# Enable forwarding isolation between AC interfaces in a VSI in Martini VPLS.

```
<HUAWEI> system-view
[HUAWEI] mpls l2vpn
[HUAWEI-l2vpn] quit
[HUAWEI] vsi v100 static
[HUAWEI-vsi-v100] pwsignal ldp
[HUAWEI-vsi-v100-ldp] vsi-id 100
[HUAWEI-vsi-v100-ldp] quit
[HUAWEI-vsi-v100] isolate spoken
```

# Enable forwarding isolation between AC interfaces in a VSI in Kompella VPLS.

```
<HUAWEI> system-view
[HUAWEI] mpls l2vpn
[HUAWEI-l2vpn] quit
```

```
[HUAWEI] vsi v101 auto
[HUAWEI-vsi-v101] pwsignal bgp
[HUAWEI-vsi-v101-bgp] route-distinguisher 100:1
[HUAWEI-vsi-v101-bgp] quit
[HUAWEI-vsi-v101] isolate spoken
```

# Enable forwarding isolation between AC interfaces in a VSI in BGP AD VPLS.

```
<HUAWEI> system-view
[HUAWEI] mpls l2vpn
[HUAWEI-l2vpn] quit
[HUAWEI] vsi v102
[HUAWEI-vsi-v102] bgp-ad
[HUAWEI-vsi-v102-bgpad] vpls-id 100:2
[HUAWEI-vsi-v102-bgpad] quit
[HUAWEI-vsi-v102] isolate spoken
```

10.7.49 l2 binding

Function

The **l2 binding** command binds an interface to a VSI.

The **undo l2 binding** command unbinds an interface to a VSI.

By default, the interface is not bound to any VSI.

Format

l2 binding vsi *vsi-name*

undo l2 binding vsi *vsi-name*

Parameters

Parameter	Description	Value
vsi *vsi-name*	Specifies the name of the VSI to be bound with an interface.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In the VPLS, run the **l2 binding** command on the PE to bind the interface that is connected to the CE to the corresponding VSI.

Precautions

When an interface is bound to a VSI, the MTU can be configured in the interface view but does not take effect. The MTU configured in the VSI is used for PW MTU negotiation.

In the VPLS application, different CEs are transparently connected to each other in the same network segment of a LAN through VSIs, and the IP addresses of the CEs must be different.

NOTE

- If an interface is used as a VPLS AC-side interface and a multicast inbound interface at the same time, multicast data cannot be forwarded normally on this interface. (S5731-H, S5731-S, S5731S-S, S5731S-H, S5732-H, S6730S-H, S6730-S, S6730S-S, and S6730-H do not have this restriction.)
- If a sub-interface is bound to a VSI, you can delete the sub-interface only after unbinding it from the VSI.
- To use a 40GE, 100GE, XGE, 25GE, MultiGE, GE, or Eth-Trunk interface of the switch as an AC-side interface, run the **undo portswitch** command to change the interface to a Layer 3 interface before running the **l2 binding** command.
- Before running the **l2 binding** command on a sub-interface, add the main interface to a VLAN.
- The **l2 binding** command and the **ip address** command cannot be configured on the CE-side interface of the PE at the same time.
- If a main interface is bound to a VSI instance, the sub-interfaces of the main interface cannot be bound to the VSI instance. Similarly, if the sub-interface of a main interface is bound to a VSI instance, the main interface cannot be bound to the VSI instance.

Example

# Bind a VLANIF interface to the VSI.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 10
[HUAWEI-Vlanif10] l2 binding vsi company2
```

# Bind a GigabitEthernet interface to a VSI.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] l2 binding vsi company2
```

10.7.50 l2vpn-ad-family

Function

The **l2vpn-ad-family** command displays the BGP L2VPN-AD address family view.

The **undo l2vpn-ad-family** command deletes all configurations in the BGP L2VPN-AD address family view.

Format

l2vpn-ad-family

undo l2vpn-ad-family

Parameters

None

Views

BGP view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The BGP AD VPLS shares a TCP connection with the common BGP. Most BGP AD VPLS configurations are the same as the common BGP configurations. To exchange information about BGP AD VPLS members, enable peers to exchange information about VPLS members in the BGP L2VPN-AD address family view. Run the **l2vpn-ad-family** command to enter the BGP L2VPN-AD address family view.

Prerequisites

Generally, BGP peers need to be configured in the BGP view to implement the configuration of basic BGP functions.

Example

# Enter the BGP L2VPN-AD address family view.

```
<HUAWEI> system-view
[HUAWEI] bgp 100
[HUAWEI-bgp] l2vpn-ad-family
[HUAWEI-bgp-af-l2vpn-ad]
```

10.7.51 loop-detect enable

Function

The **loop-detect enable** command enables L2VPN loop detection on an interface.

The **undo loop-detect enable** command disables L2VPN loop detection on the interface.

By default, L2VPN loop detection is disabled on the interface.

Format

loop-detect enable

undo loop-detect enable

Parameters

None

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Redundant links are used on an Ethernet switching network to provide link backup and enhance network reliability. The use of redundant links, however, may produce loops, causing broadcast storms and unstable MAC address entries. This degrades communication quality or even interrupts communication. On a traditional Layer 2 network, the Spanning Tree Protocol (STP) is usually used to prevent loops.

VPLS is an L2VPN technology providing LAN-like services over the MPLS network. It allows sites in diverse locations to connect the MPLS network and communicate with each other, which frees Ethernet LAN deployment from restrictions imposed by physical locations. As a Layer 2 Ethernet technology, VPLS has the following disadvantages:

- If the customer network leases multiple lines, loops may occur due to incorrect customer configuration or in other unexpected cases, leading to broadcast storms.
- If the customer network traverses a third-party network, loops may occur due to incorrect third-party network configuration or in other unexpected cases, leading to broadcast storms.

STP needs to be deployed on CEs, having high dependency on the customer network. The complex and changing features of the customer network increase the maintenance difficulty of the carrier.

To prevent loops on an L2VPN network, you can run the **loop-detect enable** command on an AC interface of a PE to configure L2VPN loop detection on the AC interface. After this function is enabled, when detecting a loop on the L2VPN network, the PE will automatically block an interface on the loop, report an alarm, and eliminate the loop.

Prerequisites

The interface has been bound to a VSI instance using the **l2 binding** command on the interface.

NOTE

- The interface must be an AC interface bound to a specified VSI. For details about the binding between an AC interface and a VSI, see **Binding VSIs to AC Interfaces**.

Example

# Enable L2VPN loop detection on GigabitEthernet0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
```

```
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] l2 binding vsi company2
[HUAWEI-GigabitEthernet0/0/1] loop-detect enable
```

10.7.52 loop-detect detection pe-vid ce-vid

Function

The **loop-detect detection pe-vid ce-vid** command specifies a VLAN range to which a QinQ termination sub-interface sends L2VPN loop detection packets.

The **undo loop-detect detection pe-vid ce-vid** command deletes the VLAN range to which the QinQ termination sub-interface sends L2VPN loop detection packets.

By default, the QinQ termination sub-interface does not send L2VPN loop detection packets.

Format

loop-detect detection pe-vid *pe-vid* **ce-vid** *low-vid* [**to** *high-vid*]

undo loop-detect detection pe-vid *pe-vid* **ce-vid** *low-vid* [**to** *high-vid*]

Parameters

Parameter	Description	Value
pe-vid *pe-vid*	Specifies the outer VLAN ID in L2VPN loop detection packets sent by the QinQ termination sub-interface.	The value is an integer in the range of 2 to 4094.
ce-vid *low-vid*	Specifies the start inner VLAN ID in L2VPN loop detection packets sent by the QinQ termination sub-interface.	The value is an integer in the range of 1 to 4094.
high-vid	Specifies the end inner VLAN ID in L2VPN loop detection packets sent by the QinQ termination sub-interface.	The value is an integer in the range of 1 to 4094. The value of *high-vid* must be greater than that of *low-vid*.

Views

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

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After you run the **loop-detect enable** command to enable L2VPN loop detection on an interface, the QinQ termination sub-interface does not send L2VPN loop detection packets by default. You need to run the **loop-detect detection pe-vid ce-vid** command to configure the VLAN range to which the QinQ termination sub-interface sends L2VPN loop detection packets. After the VLAN range is configured, the device sends L2VPN loop detection packets to the specified VLANs. If a loop is detected in a VLAN, the sub-interface will stop sending L2VPN loop detection packets to all these VLANs.

Prerequisites

L2VPN loop detection has been enabled on the interface using the **loop-detect enable** command.

Example

# Configure the QinQ termination sub-interface GigabitEthernet0/0/1.1 to send L2VPN loop detection packets to VLANs 2 to 10.

```
<HUAWEI> system-view
[HUAWEI] vcmp role silent
[HUAWEI] interface gigabitethernet
[HUAWEI-GigabitEthernet0/0/1] port link-type hybrid
[HUAWEI-GigabitEthernet0/0/1] quit
[HUAWEI] interface gigabitethernet 0/0/1.1
[HUAWEI-GigabitEthernet0/0/1.1] qinq termination pe-vid 300 ce-vid 2 to 20
[HUAWEI-GigabitEthernet0/0/1.1] l2 binding vsi company2
[HUAWEI-GigabitEthernet0/0/1.1] loop-detect enable
[HUAWEI-GigabitEthernet0/0/1.1] loop-detect detection pe-vid 300 ce-vid 2 to 10
```

10.7.53 loop-detect detection vid

Function

The **loop-detect detection vid** command specifies a VLAN range to which a Dot1q termination sub-interface sends L2VPN loop detection packets.

The **undo loop-detect detection vid** command deletes the VLAN range to which the Dot1q termination sub-interface sends L2VPN loop detection packets.

By default, the Dot1q termination sub-interface does not send L2VPN loop detection packets.

Format

loop-detect detection vid *low-vid* [**to** *high-vid*]

undo loop-detect detection vid *low-vid* [**to** *high-vid*]

Parameters

Parameter	Description	Value
low-vid	Specifies the start VLAN ID in L2VPN loop detection packets sent by the Dot1q termination sub-interface.	The value is an integer in the range of 2 to 4094.
high-vid	Specifies the end VLAN ID in L2VPN loop detection packets sent by the Dot1q termination sub-interface.	The value is an integer in the range of 2 to 4094. The value of *high-vid* must be greater than that of *low-vid*.

Views

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

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After L2VPN loop detection is enabled on an interface using the **loop-detect enable** command, the Dot1q termination sub-interface does not send L2VPN loop detection packets by default. You need to run the **loop-detect detection vid** command to configure the VLAN range to which the Dot1q termination sub-interface sends L2VPN loop detection packets. After the VLAN range is configured, the device sends L2VPN loop detection packets to the specified VLANs. If a loop is detected in a VLAN, the sub-interface will stop sending L2VPN loop detection packets to all these VLANs.

Prerequisites

L2VPN loop detection has been enabled on the interface using the **loop-detect enable** command.

Example

# Configure the Dot1q termination sub-interface GigabitEthernet0/0/1.1 to send L2VPN loop detection packets to VLANs 3 to 10.

```
<HUAWEI> system-view
[HUAWEI] vcmp role silent
[HUAWEI] interface gigabitethernet
[HUAWEI-GigabitEthernet0/0/1] port link-type hybrid
[HUAWEI-GigabitEthernet0/0/1] quit
[HUAWEI] interface gigabitethernet 0/0/1.1
[HUAWEI-GigabitEthernet0/0/1.1] dot1q termination vid 2 to 10
[HUAWEI-GigabitEthernet0/0/1.1] l2 binding vsi company2
```

```
[HUAWEI-GigabitEthernet0/0/1.1] loop-detect enable
[HUAWEI-GigabitEthernet0/0/1.1] loop-detect detection vid 3 to 10
```

10.7.54 loop-detect recovery-time

Function

The **loop-detect recovery-time** command specifies a period for restoring an interface to normal state.

The **undo loop-detect recovery-time** command restores the default period for restoring an interface to normal state.

By default, an AC interface restores a blocked interface every 15 seconds.

Format

loop-detect recovery-time *recovery-time*

undo loop-detect recovery-time

Parameters

Parameter	Description	Value
recovery-time *recovery-time*	Specifies a period for an AC interface to restore a blocked interface.	The value is an integer in the range of 15 to 255, in seconds. By default, the value is 15 seconds.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After an AC interface enabled with L2VPN loop detection detects a loop, a period can be specified for the AC interface to restore a blocked interface. That is, if a blocked interface does not receive any L2VPN loop detection packet within the period specified by *recovery-time*, it will be restored to normal state.

If a device is on multiple loops, interfaces on the device may alternate between blocked and normal states during the initial detection stage. To prevent interface status flapping, you are advised to set *recovery-time* to a larger value.

Prerequisites

L2VPN loop detection has been enabled on the interface using the **loop-detect enable** command.

Example

# Configure the Dot1q termination sub-interface GigabitEthernet0/0/1.1 to restore a blocked interface every 20 seconds.

```
<HUAWEI> system-view
[HUAWEI] vcmp role silent
[HUAWEI] interface gigabitethernet
[HUAWEI-GigabitEthernet0/0/1] port link-type hybrid
[HUAWEI-GigabitEthernet0/0/1] quit
[HUAWEI] interface gigabitethernet 0/0/1.1
[HUAWEI-GigabitEthernet0/0/1.1] dot1q termination vid 1 to 10
[HUAWEI-GigabitEthernet0/0/1.1] l2 binding vsi company2
[HUAWEI-GigabitEthernet0/0/1.1] loop-detect enable
[HUAWEI-GigabitEthernet0/0/1.1] loop-detect recovery-time 20
```

10.7.55 local-mac remove all-but-mine

Function

The **local-mac remove all-but-mine** command enables a local provider edge (PE) device to delete user MAC address entries, except those entries associated with the PW that sends MAC Withdraw messages with the TLV type of 0x404.

The **undo local-mac remove all-but-mine** command restores the default configuration.

A PE removes all MAC addresses by default after receiving MAC Withdraw messages with the TLV type of 0x404.

Format

local-mac remove all-but-mine

undo local-mac remove all-but-mine

Parameters

None

Views

VSI view

Default Level

2: Configuration level

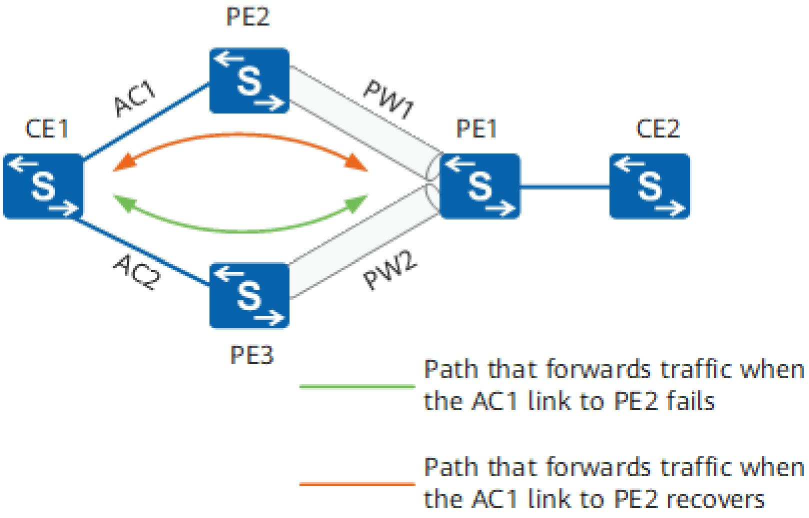
Usage Guidelines

Usage Scenario

A customer edge (CE) device is dual-homed to two PEs over pseudo wires (PWs) on a virtual private LAN service (VPLS) network. If a PE finds that an AC fault is removed, the PE sends MAC Withdraw messages with the TLV type of 0x404 to instruct a remote PE to update MAC address entries and perform a traffic switchover. For example, CE1 is connected to CE2 over primary PW1 and secondary PW2 on the network shown in **Figure 10-1**. After a fault in AC1 or PE2 is removed, PE2 sends to PE1 MAC Withdraw messages with the TLV type of 0x404 over PW1. After PE1 receives the messages, PE1 removes MAC addresses but retains those associated with PW1. The procedure complies with RFC. User traffic can then switch from PW2 to PW1.

To allow communication between a Huawei device and a non-Huawei device in compliance with RFC, run the **local-mac remove all-but-mine** command. This command is run only on PE1 shown in **Figure 10-1**.

Figure 10-1 CE dual-homing to a VPLS network


PE2
AC1
PW1
CE1
PE1
CE2
AC2
PW2
PE3
Path that forwards traffic when the AC1 link to PE2 fails
Path that forwards traffic when the AC1 link to PE2 recovers

Precautions

This command takes effect on a PE that receives MAC Withdraw messages only with the TLV type of 0x404.

Example

# Enable a PE to remove all MAC address entries but retain MAC address entries associated with a PW over which the PE receives MAC Withdraw messages with the TLV type of 0x404.

```
<HUAWEI> system-view
[HUAWEI] vsi vsi1
[HUAWEI-vsi-vsi1] local-mac remove all-but-mine
```

10.7.56 mac-address static vlanif

Function

The **mac-address static vlanif** command configures a static MAC address entry. The outgoing interface of this entry is added to the specified VLAN corresponding to the VLANIF interface. The VLANIF interface is bound to a VSI.

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

By default, the system does not configure any static MAC address entry.

Format

mac-address static *mac-address interface-type interface-number* **vlanif** *interface-number* **vsi** *vsi-name*

undo mac-address static *mac-address interface-type interface-number* **vlanif** *interface-number* **vsi** *vsi-name*

Parameters

Parameter	Description	Value
static	Indicates the static entry that is not aged. When a frame of a specific MAC address is received, the frame is forwarded through the outgoing interface directly. After being configured and saved, the entries are still stored in the table even if the system is reset.	-
mac-address	Specifies the unicast MAC address in the format of H-H-H.	An H is a hexadecimal number of 1 to 4 bits, such as 00e0 and fc01. If you enter less than four digits, 0s are padded before the input digits. For example, if e0 is entered, 00e0 is displayed. The MAC address cannot be a broadcast MAC address (FFFF-FFFF-FFFF) or a multicast MAC address (the eighth bit is 1).
interface-type interface-number	Specifies the type and number of an interface. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number.	-
vlanif *interface-number*	Specifies the number of the VLANIF interface bound to a VSI.	-

Parameter	Description	Value
vsi *vsi-name*	Specifies the name of a specified VSI.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The VPLS provides reachability through MAC address learning. Each PE maintains a MAC address table.

The device learns source MAC addresses and then creates the MAC address table. However, the device cannot identify whether the packets are from authorized users or hackers, which brings security threats. If a hacker sets the source MAC address of attack packets to the MAC address of an authorized user and connects to another interface of the device, the device learns an incorrect MAC address entry. The packets that should be forwarded to the authorized user are forwarded to the hacker.

To improve interface security, the network administrator can manually create MAC address entries to bind MAC addresses of authorized users to specified interfaces using the **mac-address static vlanif** command. This prevents hackers from intercepting data of authorized users.

Prerequisites

The network administrator is familiar with the MAC addresses of the devices on the network that need to use static MAC address entries for communications; otherwise, the configuration will interrupt authorized users' communications.

In the **mac-address static vlanif** command, the interface must be a Layer 2 interface that has been added to the VLAN corresponding to the VLANIF interface. The VLANIF interface must be bound to the VSI configured in the command.

Precautions

After being created, the static MAC address entries will not be aged. When receiving a frame of a specific MAC address, the device forwards the frame through the outgoing interface directly. After being configured and saved, the MAC address entries are still stored in the table even if the system is reset.

A physical interface that is associated with a VSI can be bound to several VLANs. The VSI that is bound to a VLANIF interface can be associated with several physical interfaces. Therefore, you need to specify a physical interface and a VLANIF interface when configuring static MAC address entries for VSIs bound to the VLANIF interface.

Manually created MAC address entries take precedence over automatically created MAC address entries. Static MAC address entries and blackhole MAC address entries take precedence over dynamic MAC address entries.

If the user service changes, specify a new VSI bound to the interface. In this way, data of the user is not forwarded through the previously configured static MAC address entries. You need to configure new MAC address entries on the device or enable the device to learn dynamic MAC address entries to forward the data.

Example

# Bind VLANIF10 to the VSI named **abc**, and add a MAC address entry with the MAC address being 00e0-fc12-3456 to the VSI. When a frame that belongs to VLAN 10 and has the destination MAC address 00e0-fc12-3456 is received, it is forwarded through the outgoing interface GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] vsi abc static
[HUAWEI-vsi-abc] pwsignal ldp
[HUAWEI-vsi-abc-ldp] vsi-id 1
[HUAWEI-vsi-abc-ldp] quit
[HUAWEI-vsi-abc] quit
[HUAWEI] vlan 10
[HUAWEI-vlan10] quit
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] port link-type access
[HUAWEI-GigabitEthernet0/0/1] port default vlan 10
[HUAWEI-GigabitEthernet0/0/1] quit
[HUAWEI] interface vlanif 10
[HUAWEI-Vlanif10] l2 binding vsi abc
[HUAWEI-Vlanif10] quit
[HUAWEI] mac-address static 00e0-fc12-3456 gigabitethernet 0/0/1 vlanif 10 vsi abc
```

10.7.57 mac-address static vsi

Function

The **mac-address static vsi** command configures a static MAC address entry. The outgoing interface in this entry is bound to a specified VSI.

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

By default, the system does not configure any static MAC address entry.

Format

mac-address static *mac-address interface-type interface-number* **vsi** *vsi-name*

undo mac-address static *mac-address interface-type interface-number* **vsi** *vsi-name*

undo mac-address static vsi *vsi-name*

Parameters

Parameter	Description	Value
static	Indicates the static entry that is not aged. When a frame of a specific MAC address is received, the frame is forwarded through the outgoing interface directly. After being configured and saved, the entries are still stored in the table even if the system is reset.	-
mac-address	Specifies the unicast MAC address in the format of H-H-H.	An H is a hexadecimal number of 1 to 4 bits, such as 00e0 and fc01. If you enter less than four digits, 0s are padded before the input digits. For example, if e0 is entered, 00e0 is displayed. The MAC address cannot be a broadcast MAC address (FFFF-FFFF-FFFF) or a multicast MAC address (the eighth bit is 1).
interface-type interface-number	Specifies the type and number of an interface. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number.	The interface can be a GE interface, a GE sub-interface, an XGE interface, an XGE sub-interface, a 25GE interface, a 25GE sub-interface, a 40GE interface, a 40GE sub-interface, a 100GE interface, a 100GE sub-interface, an Eth-Trunk interface, or an Eth-Trunk sub-interface. The interface in this command is a Layer 3 interface bound to a VSI.
vsi *vsi-name*	Specifies the name of a specified VSI.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The VPLS provides reachability through MAC address learning. Each PE maintains a MAC address table.

The device learns source MAC addresses and then creates the MAC address table. However, the device cannot identify whether the packets are from authorized users or hackers, which brings security threats. If a hacker sets the source MAC address of attack packets to the MAC address of an authorized user and connects to another interface of the device, the device learns an incorrect MAC address entry. The packets that should be forwarded to the authorized user are forwarded to the hacker.

To improve interface security, the network administrator can manually create MAC address entries to bind MAC addresses of authorized users to specified interfaces using the **mac-address static vlanif** command. This prevents hackers from intercepting data of authorized users.

Prerequisites

The network administrator is familiar with the MAC addresses of the devices on the network that need to use static MAC address entries for communications; otherwise, the configuration will interrupt authorized users' communications.

In the **mac-address static vsi** command, the interface must be a Layer 3 interface bound to a VSI.

Precautions

After being created, the static MAC address entries will not be aged. When receiving a frame of a specific MAC address, the device forwards the frame through the outgoing interface directly. After being configured and saved, the MAC address entries are still stored in the table even if the system is reset.

Manually created MAC address entries take precedence over automatically created MAC address entries. Static MAC address entries and blackhole MAC address entries take precedence over dynamic MAC address entries.

If the user service changes, specify a new VSI bound to the interface. In this way, data of the user is not forwarded through the previously configured static MAC address entries. You need to configure new MAC address entries on the device or enable the device to learn dynamic MAC address entries to forward the data.

Example

# Add a static MAC address entry to the VSI named **abc**. When the destination MAC address of a received frame is 00e0-fc33-4455, the frame is forwarded in the VSI named **abc**.

```
<HUAWEI> system-view
[HUAWEI] vsi abc static
[HUAWEI-vsi-abc] pwsignal ldp
[HUAWEI-vsi-abc-ldp] vsi-id 1
[HUAWEI-vsi-abc-ldp] quit
[HUAWEI-vsi-abc] quit
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
```

```
[HUAWEI-GigabitEthernet0/0/1] l2 binding vsi abc
[HUAWEI-GigabitEthernet0/0/1] quit
[HUAWEI] mac-address static 00e0-fc33-4455 gigabitethernet 0/0/1 vsi abc
```

10.7.58 mac-diagnose enable

Function

The **mac-diagnose enable** command enables diagnostic test on the MAC address learning capacity.

The **mac-diagnose disable** command disables diagnostic test on the MAC address learning capacity.

The **undo mac-diagnose enable** command disables diagnostic test on the MAC address learning capacity.

By default, diagnostic test on the MAC address learning capacity is enabled.

Format

mac-diagnose enable

mac-diagnose disable

undo mac-diagnose enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To rectify a Layer 2 communication fault on the device, run the **mac-diagnose enable** command to enable diagnostic test on the MAC address learning capacity.

Precautions

Using the **mac-diagnose enable** command, you can enable diagnostic test on the MAC address learning capacity. The **mac-populate** and **mac-purge** operations can be performed only when diagnostic test on the MAC address learning capacity is enabled. Otherwise, the **mac-populate** and **mac-purge** operations cannot be performed. In addition, information and statistics on populated OAM MAC address are cleared.

Example

# Enable diagnostic test on the MAC address learning capacity.

```
<HUAWEI> system-view
[HUAWEI] mac-diagnose enable
```

# Disable diagnostic test on the MAC address learning capacity.

```
<HUAWEI> system-view
[HUAWEI] mac-diagnose disable
```

10.7.59 mac-learning

Function

The **mac-learning enable** command enables MAC address learning for a VSI.

The **mac-learning disable** command disables MAC address learning of a VSI.

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

By default, MAC address learning is enabled for a VSI.

Format

mac-learning { **enable** | **disable** }

undo mac-learning disable

Parameters

Parameter	Description	Value
enable	Enables a VSI to learn MAC addresses.	-
disable	Disables a VSI to learn MAC addresses.	-

Views

VSI view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To disable MAC address learning in a VSI on a VPLS network, run the **mac-learning disable** command. The VPLS network then functions similarly to a VPWS network. For example, if there are only two PEs with each connecting to one CE, disabling MAC address learning in a VSI on a PE reduces the PE's pressure.

Configuration Impact

After the **mac-learning disable** command is run for a VSI, the VSI can no longer automatically learn MAC addresses, causing packets to be broadcast on the network. Therefore, exercise caution when running this command.

Example

# Disable MAC address learning of the current VSI.

```
<HUAWEI> system-view
[HUAWEI] vsi company1
[HUAWEI-vsi-company1] mac-learning disable
```

10.7.60 mac-limit (VSI view)

Function

The **mac-limit** command configures the MAC address limit rules on a VSI.

The **undo mac-limit** command restores the default setting.

By default, none of the MAC address limit rule is configured on a VSI.

NOTE

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

Format

mac-limit { **action** { **discard** | **forward** } | **alarm** { **disable** | **enable** } | **maximum** *max-number* } *

undo mac-limit

Parameters

Parameter	Description	Value
action	Indicates the action performed on packets when the number of MAC entries reaches the limit. By default, the system discards the packets.	-
discard	Indicates that after the number of MAC entries reaches the limit, the system discards the packet whose destination MAC address does not map to any entry in the MAC address table.	-
forward	Indicates that after the number of MAC entries reaches the limit, the system broadcasts a packet whose destination MAC address does not map to any entry in the MAC address table, but does not learn the destination MAC address of the packet.	-

Parameter	Description	Value
alarm	Indicates whether an alarm is generated when the number of MAC address entries reaches the limit.	-
disable	Indicates that no alarm is generated when the number of MAC address entries reaches the limit.	-
enable	Indicates that an alarm is generated in syslog mode when the number of MAC address entries reaches the limit. By default, an alarm is sent to the NM station.	-
maximum *max-number*	Specifies the maximum number of MAC address entries that the current VSI can learn. **NOTE** Set **maximum** *max-number* before you set **action** or **alarm**.	The value is an integer that ranges from 0 to 4096.

Views

VSI view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To prevent attacks, you can run the **mac-limit** command to limit the maximum number of MAC addresses that the current VSI can learn.

Precautions

If the VSI has learned some MAC addresses, run the **undo mac-address dynamic** command to clear the learned MAC addresses. Otherwise, the **mac-limit** command cannot limit the MAC address learning accurately.

When the **mac-limit** command is executed for the first time, you can configure **action** and **alarm** only after **maximum** *max-number* is configured. If the **mac-limit** command is not executed for the first time, there is no special requirement on the configuration sequence.

Example

# Set the maximum number of MAC addresses that can be learned to 100 on the VSI PW.

```
<HUAWEI> system-view
[HUAWEI] vsi 1
[HUAWEI-vsi-1] mac-limit maximum 100
```

10.7.61 mac-populate

Function

The **mac-populate** command populates an OAM MAC address to initiate a diagnostic test on the MAC address learning capacity.

Format

mac-populate vsi *vsi-name* **mac** *mac-address* [**packet-num** *num* | **flood**] *

Parameters

Parameter	Description	Value
vsi *vsi-name*	Specifies the name of the VSI on which the operation is performed.	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.
mac *mac-address*	Specifies the MAC address for the diagnostic test, expressed in the format of H-H-H.	The value is in H-H-H format. The values are as follows: ● 0018-82a4-3fb1 ● 0018-82a4-3fb2 ● 0018-82a4-3fb3 ● 0018-82a4-3fb4 ● 0018-82a4-3fb5 ● 0018-82a4-3fb6 ● 0018-82a4-3fb7 ● 0018-82a4-3fb8 ● 0018-82a4-3fb9 ● 0018-82a4-3fba
packet-num *num*	Specifies the number of packets to be sent.	The value is a decimal integer that ranges from 1 to 5. The default value is 3.
flood	Indicates that the OAM MAC address is flooded throughout the VSI.	-

Views

All views

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To rectify a Layer 2 communication fault on the device, you can run the **mac-populate** command to populate an OAM MAC address into the device to initiate a diagnostic test.

Prerequisites

The diagnostic test on the MAC address learning capacity has been enabled using the **mac-diagnose enable** command.

Precautions

The **mac-populate** command does not support BGP AD VPLS.

Using the **mac-populate** command, you can populate an OAM MAC address into the device.

- If the **mac-populate** command does not contain **flood**, an OAM MAC address is only populated into the local device.
- If the **mac-populate** command contains **flood**, an OAM MAC is flooded throughout the VSI and then populated into the peer and local devices.

NOTE

The OAM MAC address populated into the local and peer devices can control the forwarding. Under the guidance of the OAM MAC address, the peer device forwards the received packets corresponding to the OAM MAC address to the local device.

The default aging time of OAM MAC addresses is 150 seconds.

Example

# Populate an OAM MAC address into the VSI named **vsi1**, flood the OAM MAC address over the domain, and set the number of packets to be sent to 3.

```
<HUAWEI> mac-populate vsi vsi1 mac 0018-82a4-3fb1 flood packet-num 3
```

10.7.62 mac-purge

Function

The **mac-purge** command purges an OAM MAC address from the forwarding table.

Format

mac-purge vsi *vsi-name* **mac** *mac-address* [**packet-num** *num* | **register** | **flood**] *

Parameters

Parameter	Description	Value
vsi *vsi-name*	Specifies the name of the VSI on which the operation is performed.	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.
mac *mac-address*	Specifies the MAC address for the diagnostic test, expressed in the format of H-H-H.	The value is in H-H-H format. The values are as follows: ● 0018-82a4-3fb1 ● 0018-82a4-3fb2 ● 0018-82a4-3fb3 ● 0018-82a4-3fb4 ● 0018-82a4-3fb5 ● 0018-82a4-3fb6 ● 0018-82a4-3fb7 ● 0018-82a4-3fb8 ● 0018-82a4-3fb9 ● 0018-82a4-3fba
packet-num *num*	Specifies the number of packets to be sent.	The value is a decimal integer that ranges from 1 to 5. The default value is 3.
register	Specifies the MAC address reserved for the OAM test. **NOTE** If the preceding command contains **register**, an OAM MAC address is populated into the local device or the peer device to make the device discard received packets corresponding to the OAM MAC address.	-
flood	Indicates that the OAM MAC address is flooded throughout the VSI.	-

Views

All views

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To rectify a Layer 2 communication fault on the device, you can run the **mac-purge** command to clear OAM MAC addresses populated into the device.

Prerequisites

The diagnostic test on the MAC address learning capacity has been enabled using the **mac-diagnose enable** command.

Precautions

- If *vsi-name* in the **mac-purge** command for purging an OAM MAC address is not identical with *vsi-name* in the **mac-purge** command that is previously used in populating the OAM MAC address, the OAM MAC address cannot be cleared.
- A maximum of 100 OAM MAC addresses of **populate** and **register+populate** types can be populated into a device.
- The **mac-purge** command does not support BGP AD VPLS.

Using the **mac-purge** command, you can purge the populated OAM MAC address that is specialized for the test or register an OAM MAC address to a device to make the device discard the received packets corresponding to the OAM MAC address.

Test objects vary according to parameters.

- If the **mac-purge** command contains **flood**, an OAM MAC address is flooded throughout the VSI and then purged from all devices in the VSI and the local device into which the OAM MAC address has been populated. If the preceding command does not contain **flood**, the OAM MAC address is purged only from the local device.
- If the **mac-purge** command contains **register**, an OAM MAC address is registered on the device to make the device discard the packet corresponding to the OAM MAC address after receiving them.

Example

# Purge the OAM MAC address from the VSI named **vsi1**, flood the OAM MAC address over the domain, and set the number of packets to be sent to 3.

```
<HUAWEI> mac-purge vsi vsi1 mac 0018-82a4-3fb1 flood packet-num 3
```

10.7.63 mac-withdraw enable

Function

The **mac-withdraw enable** command enables a VSI to delete the local MAC address and inform all the remote peers of the deletion.

The **undo mac-withdraw enable** command disables a VSI to delete the local MAC address and inform all the remote peers of the deletion.

By default, the MAC-withdraw function is disabled.

Format

mac-withdraw enable

undo mac-withdraw enable

Parameters

None

Views

VSI-LDP view, VSI view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On enterprise networks, if the remote end specifies the local end as the UPE, the remote AC interface does not inform the local end to cancel the label after the AC interface is faulty. In this case, the local end is unaware of an AC fault or a UPE fault. The VSI remains Up and does not delete the corresponding MAC address entries in time. As a result, the remote end cannot receive data streams sent by the local end. After the **mac-withdraw enable** command is executed, the VSI deletes the local MAC address and informs all the remote peers of the deletion when an AC fault or a UPE fault occurs and the VSI remains Up. This solves the preceding problem.

Precautions

When an AC fault or a UPE fault occurs and the VSI remains Up, the UPE device needs to switch the VPLS traffic to another LSP if the UPE device accesses the SPE device in dual-homed mode. The SPE device then only needs to inform the other SPEs corresponding to the VSI to delete the MAC entries learnt from this VSI. After traffic switchover, the SPEs re-learn MAC entries from each other.

This command must be configured on SPEs.

The **mac-withdraw enable** command must be used together with the **interface-status-change mac-withdraw enable** command.

Example

# Configure a VSI named v100 to delete the local MAC addresses and inform all the remote peers of the deletion when an AC fault or a UPE fault occurs and the VSI remains Up.

```
<HUAWEI> system-view
[HUAWEI] vsi v100 static
[HUAWEI-vsi-v100] pwsignal ldp
[HUAWEI-vsi-v100-ldp] mac-withdraw enable
```

10.7.64 mac-withdraw propagate enable

Function

The **mac-withdraw propagate enable** command enables a PE to forward a received MAC Withdraw message to peers.

The **undo mac-withdraw propagate enable** command disables a PE from forwarding a received MAC Withdraw message to peers.

By default, a PE does not forward a received MAC Withdraw message.

Format

mac-withdraw propagate enable

undo mac-withdraw propagate enable

Parameters

None

Views

VSI view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On an LDP or BGP AD VPLS network, after a local PE receives a MAC Withdraw message, the local PE needs to forward the MAC Withdraw message to its peers. Otherwise, its peers cannot detect network topology changes or learn new MAC addresses in a timely manner. As a result, traffic loss caused by invalid MAC addresses will occur. The **mac-withdraw propagate enable** command enables a PE to forward a received MAC Withdraw message to peers.

Precautions

After you run the **mac-withdraw propagate enable** command on a PE, the PE forwards a received MAC Withdraw message to its peers according to the split horizon principle:

- The MAC Withdraw message received from a UPE will be forwarded to NPEs and other UPEs.
- The MAC Withdraw message received from an NPE will be forwarded to UPEs, but will not be forwarded to other NPEs.

Example

# Configure vsi100 on a PE to forward a received MAC Withdraw message to peers.

```
<HUAWEI> system-view
[HUAWEI] vsi vsi100
[HUAWEI-vsi-vsi100] mac-withdraw propagate enable
```

10.7.65 mpls l2vpn default vlan

Function

The **mpls l2vpn default vlan** command configures the default VLAN for a main interface.

The **undo mpls l2vpn default vlan** command deletes the default VLAN of a main interface.

Format

mpls l2vpn default vlan *vlan-id*

undo mpls l2vpn default vlan

Parameters

Parameter	Description	Value
vlan-id	Specifies the default VLAN ID of a main interface.	The value is an integer that ranges from 1 to 4094.

Views

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

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the following conditions are met, you can run the **mpls l2vpn default vlan** command to specify the default VLAN on a main interface:

- The VSI using VLAN encapsulation is configured on the two PEs.
- The remote PE accepts only the tagged packets.

- The local PE is connected to a computer by using a GE interface, XGE interface, 25GE interface, MultiGE interface, 40GE interface, 100GE interface, or Eth-Trunk interface as the AC interface.

  In this scenario, the computer sends and receives only untagged packets. After the default VLAN is specified on the main interface, the local PE performs the following operations:

  – The local PE adds VLAN tags to the packets sent by the computer. The VLAN tags are encapsulated in the user packets, and are transparently transmitted to the remote PE.

  – The local PE removes the VLAN tags from the packets sent by the remote PE, and forwards the packets to the computer.

Precautions

Before binding the main interface to the VSI, you need to run the **mpls l2vpn default vlan** command to specify the default VLAN of the main interface.

If the remote PE can replace the VLAN tags in the packets with the VLAN tag of the AC-side outgoing interface when terminating the PW, the default VLAN on the main interface of the local PE can be set to any VLAN ID. Otherwise, the default VLAN of the main interface must be the same as the VLAN of the AC-side outgoing interface on the remote PE.

To use an XGE interface, a GE interface, a 25GE interface, a MultiGE interface, a 40GE interface, a 100GE interface, or an Eth-Trunk interface of the device as the AC interface of the PE, run the **undo portswitch** command to change a Layer 2 interface to a Layer 3 interface.

Example

# Configure the default VLAN of primary interface.

```
[HUAWEI] interface gigabitethernet 0/0/2
[HUAWEI-GigabitEthernet0/0/2] undo portswitch
[HUAWEI-GigabitEthernet0/0/2] mpls l2vpn default vlan 100
```

10.7.66 mpls l2vpn ip-parse enable

Function

The **mpls l2vpn ip-parse enable** command enables the IP packet parsing function of the MPLS L2VPN module.

The **undo mpls l2vpn ip-parse enable** command disables the IP packet parsing function of the MPLS L2VPN module.

By default, the IP packet parsing function of the MPLS L2VPN module is enabled.

Format

mpls l2vpn ip-parse enable

undo mpls l2vpn ip-parse enable

NOTE

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

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In a Layer 2 VPN scenario, if a traffic policy is configured in the inbound direction of an AC-side interface on a device, L2VPN traffic forwarded from a PE may incorrectly match the traffic policy. As a result, traffic fails to be forwarded. To ensure normal traffic forwarding, run the **undo mpls l2vpn ip-parse enable** command to disable the IP packet parsing function of the MPLS L2VPN module.

Precautions

If the enhanced load balancing mode is configured for an Eth-Trunk, it is recommended that the IP packet parsing function of the MPLS L2VPN module be enabled.

Example

# Disable the IP packet parsing function of the MPLS L2VPN module.

```
<HUAWEI> system-view
[HUAWEI] undo mpls l2vpn ip-parse enable
```

10.7.67 mpls l2vpn mac-withdraw disable

Function

The **mpls l2vpn mac-withdraw disable** command disables the VLL from sending MAC Withdraw messages on a VPLS network with primary and secondary VLLs.

The **undo mpls l2vpn mac-withdraw disable** command restores the default setting.

By default, the VLL is enabled to send MAC Withdraw messages on a VPLS network with primary and secondary VLLs.

Format

mpls l2vpn mac-withdraw disable

undo mpls l2vpn mac-withdraw disable

Parameters

None

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In a VPLS scenario with primary and secondary VLLs, the primary and secondary VLLs send MAC Withdraw messages to the VPLS-enabled RSG each time a primary/secondary PW switchover is performed. After receiving the MAC Withdraw messages, the VPLS-enabled RSG clears all learned MAC addresses. Then packets will be transmitted in broadcast mode. To prevent packets from being broadcast, run the **mpls l2vpn mac-withdraw disable** command to disable the VLL in Ethernet or VLAN encapsulation mode from sending MAC-Withdraws messages during a primary/secondary PW switchover.

Precautions

This command takes effect only in a VPLS scenario with primary and secondary VLLs. In other scenarios, do not run the **mpls l2vpn mac-withdraw disable** command; otherwise, services will be interrupted.

Example

# Disable the VLL in Ethernet or VLAN encapsulation mode from sending MAC Withdraw messages during a primary/secondary PW switchover.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 10
[HUAWEI-Vlanif10] mpls l2vc 2.2.2.2 100
[HUAWEI-Vlanif10] mpls l2vc 4.4.4.4 200 secondary
[HUAWEI-Vlanif10] mpls l2vpn mac-withdraw disable
```

10.7.68 mpls l2vpn vlan-stacking

Function

The **mpls l2vpn vlan-stacking** command configures the stacked VLAN ID for a main interface.

The **undo mpls l2vpn vlan-stacking** command deletes the stacked VLAN ID from a main interface.

By default, the system does not add a VLAN ID to a packet passing through the main interface.

Format

mpls l2vpn vlan-stacking stack-vlan *vlan-id*

undo mpls l2vpn vlan-stacking stack-vlan

Parameters

Parameter	Description	Value
stack-vlan *vlan-id*	Indicates the outer VLAN ID.	The value is an integer that ranges from 1 to 4094.

Views

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

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the following conditions are met, run the **mpls l2vpn vlan-stacking stack-vlan** command to specify a VLAN for a main interface:

- The VLL or VSI using VLAN encapsulation is configured on the two PEs.
- The remote PE accepts packets with one more VLAN tag.
- The local PE is connected to a computer by using a GE interface, XGE interface, 25GE interface, MultiGE interface, 40GE interface, 100GE interface, or Eth-Trunk interface as the AC interface.

  In this scenario, the computer sends and receives all packets. After a VLAN is specified for the main interface, the local PE performs the following operations:

  - The local PE adds VLAN tags to the packets sent by the computer. The VLAN tags are encapsulated in the user packets, and are transparently transmitted to the remote PE.
  - The local PE removes the outer VLAN tags from the packets sent by the remote PE, and forwards the packets to the computer.

Precautions

Before binding the main interface to the VLL or VSI, run the **mpls l2vpn vlan-stacking stack-vlan** command to specify a VLAN for the main interface.

To use an XGE interface, a GE interface, a 25GE interface, a MultiGE interface, a 40GE interface, a 100GE interface, or an Eth-Trunk interface of the device as the AC interface of the PE, run the **undo portswitch** command to change a Layer 2 interface to a Layer 3 interface.

Example

# Configure MPLS VLL on the main interface and add VLAN tag 80 to incoming packets.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/13
[HUAWEI-GigabitEthernet0/0/13] undo portswitch
[HUAWEI-GigabitEthernet0/0/13] mpls l2vpn vlan-stacking stack-vlan 80
[HUAWEI-GigabitEthernet0/0/13] mpls l2vc 10.0.0.17 20 tagged
```

10.7.69 mpls l2vpn vsi-pw limit threshold-alarm

Function

The **mpls l2vpn vsi-pw limit threshold-alarm** command configures the upper and lower alarm thresholds for VPLS VCs.

The **undo mpls l2vpn vsi-pw limit threshold-alarm** command restores the default settings.

By default, the upper and lower alarm thresholds are 80% and 70% respectively.

Format

mpls l2vpn vsi-pw limit threshold-alarm upper-limit *upper-limit-value* **lower-limit** *lower-limit-value*

undo mpls l2vpn vsi-pw limit threshold-alarm [**upper-limit** *upper-limit-value* **lower-limit** *lower-limit-value*]

Parameters

Parameter	Description	Value
upper-limit *upper-limit-value*	Specifies the upper alarm threshold.	The value is an integer ranging from 1 to 100.
lower-limit *lower-limit-value*	Specifies the lower alarm threshold.	The value is an integer ranging from 1 to 100. *lower-limit-value* must be smaller than *upper-limit-value*.

Views

MPLS-L2VPN view

Default Level

2: Configuration Level

Usage Guidelines

A device supports only a limited number of VPLS VCs. If a device has too many VPLS VCs, the device performance deteriorates. The **mpls l2vpn vsi-pw limit**

threshold-alarm command allows you to flexibly adjust the upper and lower alarm thresholds for VPLS VCs to control VPLS VC usage.

Note that:

- *upper-limit-value* specifies the upper alarm threshold for VPLS VCs. If the proportion of VPLS VCs created to the maximum VPLS VCs allowed reaches this threshold, a VPLS VC threshold-crossing alarm is reported.
- *lower-limit-value* specifies the lower alarm threshold for VPLS VCs. If the proportion of VPLS VCs created to the maximum VPLS VCs allowed falls below this threshold, a VPLS VC threshold-crossing clear alarm is reported.

Example

# Configure the upper and lower alarm thresholds for VPLS VCs as 90% and 70% respectively.

```
<HUAWEI> system-view
[HUAWEI] mpls l2vpn
[HUAWEI-l2vpn] mpls l2vpn vsi-pw limit threshold-alarm upper-limit 90 lower-limit 70
```

10.7.70 mtu (VSI view)

Function

The **mtu** command sets the MTU of a VSI.

The **undo mtu** command restores the default value.

The default MTU of a VSI is 1500.

Format

mtu *mtu-value*

undo mtu

Parameters

Parameter	Description	Value
mtu-value	Specifies the MTU of a VSI.	The value is an integer that ranges from 328 to 65535.

Views

VSI view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If the MTUs of the same VSI on two PEs are different, the two PEs cannot exchange information or establish a connection. In this case, you can run the **mtu** command to set the MTU of a VSI so that VSIs created on different PEs for the same VPLS have the same MTU.

Prerequisites

The following operations have been performed before this command is used:

- The **pwsignal bgp** command and the **route-distinguisher (VSI-BGP view)** *route-distinguisher* command have been executed for Kompella VPLS.
- The **pwsignal ldp** command and the **vsi-id** *vsi-id* command have been executed for Martini VPLS.
- The **bgp-ad** command and the **vpls-id** *vpls-id* command have been executed for BGP AD VPLS.

Precautions

When configuring MTUs, note that the MTUs of the VSIs created for the same VPLS on different PEs must be the same.

Devices of some manufacturers cannot perform the MTU matching check on the VSI. When the switch interworks with a non-Huawei device in Kompella mode, you need to perform either of the following configurations to ensure that VCs are Up:

- Set the MTU of the VSI on the PE to be consistent with the MTU of the non-Huawei device.
- Run the **mtu-negotiate disable** command to ignore the check on MTU matching.

Example

# Set the MTU of the VSI named **company1**.

```
<HUAWEI> system-view
[HUAWEI] vsi company1 static
[HUAWEI-vsi-company1] pwsignal ldp
[HUAWEI-vsi-company1-ldp] vsi-id 100
[HUAWEI-vsi-company1-ldp] quit
[HUAWEI-vsi-company1] mtu 1600
```

10.7.71 mtu-negotiate disable

Function

The **mtu-negotiate disable** command disables a PE from checking whether the MTUs for the local and remote VSIs match.

The **undo mtu-negotiate disable** command enables a PE to check whether the MTUs for the local and remote VSIs match.

By default, a PE is enabled to check whether the MTUs for the local and remote VSIs match.

Format

mtu-negotiate disable

undo mtu-negotiate disable

Parameters

None

Views

VSI-BGP view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When two PEs that are Huawei and non-Huawei devices use Kompella VPLS to communicate, and their MTUs are different, the VC cannot Up. To resolve this problem, run the **mtu-negotiate disable** command to disable the local PE from checking whether the MTUs for the local and remote VSIs match. Alternatively, run the **mtu** command to change the MTU of the local VSI to be the same as that of the remote VSI.

Precautions

The **mtu-negotiate disable** command and its undo form are valid only for Kompella VPLS.

Example

# Disable the device from checking whether the MTUs named **bgp1** for the local and remote VSIs match.

```
<HUAWEI> system-view
[HUAWEI] vsi bgp1
[HUAWEI-vsi-bgp1] pwsignal bgp
[HUAWEI-vsi-bgp1-bgp] mtu-negotiate disable
```

10.7.72 multi-homing-preference

Function

The **multi-homing-preference** command configures the multi-homed priority for a VSI.

The **undo multi-homing-preference** command deletes multi-homed priority for a VSI.

By default, the multi-homed priority for a VSI is 0, which is the lowest priority.

Format

multi-homing-preference *preference-value*

undo multi-homing-preference

Parameters

Parameter	Description	Value
preference-value	Specifies the multi-homed priority of a VSI.	The value is an integer that ranges from 1 to 65535. A large value indicates a high priority.

Views

VSI view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In CE dual-homed scenarios, run the **multi-homing-preference** command to specify a primary PE and a backup PE.

Prerequisites

The following operations have been performed before this command is used:

1. A VSI has been created and the automatic member discovery mechanism has been configured using the **vsi** *vsi-name* **auto** command.
2. BGP has been configured as the PW signaling protocol using the **pwsignal bgp** command.
3. The RD has been configured for the VSI using the **route-distinguisher** *route-distinguisher* command.

Precautions

Currently, only Kompella VPLS supports the multi-homed priority for a VSI. In addition, only the dual-homed CE is supported.

If you run the **multi-homing-preference** command for a Kompella VPLS, the configured preference takes effect only after the **bestroute l2vpn-preference vpls** command is run in the BGP-L2VPN-AD address family view.

At present, only one label block can be configured on the VSIs of the two dual-homed PEs. If you want to increase the range, run the **undo site** command to delete the existing site, and then specify a larger range. Only one AC can be configured for the VSIs of the dual-homed PEs.

If the VSIs of two PEs that the dual-homed CE accesses are Up, the PE with higher priority serves as the primary PE, while the PE with lower priority serves as the backup PE. The primary PE is responsible for forwarding the traffic of the CE, while the backup PE is responsible only for checking whether the VSI of the primary PE is Up. After the backup PE is selected, the VSI status of the backup PE turns Down.

If the VSI status of the primary PE turns Down, the primary PE broadcasts Unreach packets. After the backup PE receives the Unreach packets, the backup PE judges that the primary PE is faulty. The backup PE then sends Reach packets to set up a PW with other PEs. The backup PE becomes a primary PE.

If the dual-homed priorities of the two PEs in dual-homed mode are the same, after a session is set up between the PEs, the PEs detect collision. At this time, the VSI of the PE with smaller router ID is Up, while the VSI of the PE with larger router ID is Down.

If a session is set up between PE1 with the priority being "a" and PE2 with the priority being "b", and a is larger than b, the VSI of PE1 is Up and that of PE2 is Down. At this time:

- If the priority of PE1 is changed to "b" (the modification is permitted because PE1 does not have information about remote VCs on PE2), the VSI of PE1 remains Up, while the VSI of PE2 remains Down.
- If the priority of PE2 is changed to "a", the modification is rejected and alarm information is displayed.

After the session turns Down, the PW of the PE with lower priority turns Up. The PW between the two PEs turns Up.

Example

# Configure the multi-homed priority of the VSI named **company1** to 100.

```
<HUAWEI> system-view
[HUAWEI] vsi company1 auto
[HUAWEI-vsi-company1] pwsignal bgp
[HUAWEI-vsi-company1-bgp] route-distinguisher 100:1
[HUAWEI-vsi-company1-bgp] quit
[HUAWEI-vsi-company1] multi-homing-preference 100
```

10.7.73 multicast-suppression cir cbs (VSI view)

Function

The **multicast-suppression cir cbs** command enables the multicast suppression function on the VSI.

The **undo multicast-suppression** command disables the multicast suppression function on the VSI.

By default, the multicast traffic function is disabled on a VSI.

Format

multicast-suppression cir *cir-value* **cbs** *cbs-value*

undo multicast-suppression

Parameters

Parameter	Description	Value
cir *cir-value*	Specifies the CIR, that is, the allowed rate at which traffic can pass through.	The value is an integer that ranges from 0 to 10000000, in kbit/s.
cbs *cbs-value*	Specifies the CBS, that is, the traffic that can pass instantly, or the depth of the first token bucket.	The value is an integer that ranges from 10000 to 4294967295, in bytes.

Views

VSI view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On a VPLS network, the broadcast, multicast, and unknown unicast packets are transmitted in broadcast mode. If large quantities of multicast packets are on the VPLS network, the device has to make a lot of copies of these multicast packets, which wastes bandwidth and resources, and degrades the performance of the system. You can run the **multicast-suppression cir cbs** command to suppress the multicast traffic in the VSI. The rate of multicast traffic on the VPLS network is limited.

Prerequisites

A VSI has been created using the **vsi** *vsi-name* [**auto** | **static**] command.

Example

# Set the CIR to 100 kbit/s and the CBS to 18800 bytes for the multicast traffic that can pass in VSI1.

```
<HUAWEI> system-view
[HUAWEI] vsi VSI1
[HUAWEI-vsi-VSI1] multicast-suppression cir 100 cbs 18800
```

10.7.74 npe-upe mac-withdraw enable

Function

The **npe-upe mac-withdraw enable** command enables an SPE to forward the LDP MAC Withdraw messages received from other SPEs to UPEs.

The **undo npe-upe mac-withdraw enable** command disables an SPE from forwarding the LDP MAC Withdraw messages received from other SPEs to UPEs.

By default, an SPE does not forward the LDP MAC Withdraw messages received from other SPEs to UPEs.

Format

npe-upe mac-withdraw enable

undo npe-upe mac-withdraw enable

Parameters

None

Views

VSI-LDP view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On enterprise networks, you need to run the **npe-upe mac-withdraw enable** command to enable an SPE to forward the LDP MAC Withdraw messages received from other SPEs to UPEs.

Prerequisites

LDP has been configured as the PW signaling protocol using the **pwsignal ldp** command.

Precautions

The **npe-upe mac-withdraw enable** command is used on SPEs.

- An SPE refers to the network end peer of the local VSI in HVPLS. You can run the **peer** *peer-address* [**negotiation-vc-id** *vc-id*] [**tnl-policy** *policy-name*] command to specify an SPE.
- A UPE refers to the user end peer of the local VSI in HVPLS. You can run the **peer** *peer-address* [**negotiation-vc-id** *vc-id*] [**tnl-policy** *policy-name*] **upe** command to specify a UPE.
- If the local device is not configured with HVPLS, the **npe-upe mac-withdraw enable** command is not required.

Example

# Enable the SPE to forward the LDP MAC Withdraw messages received from other SPEs the UPE.

```
<HUAWEI> system-view
[HUAWEI] vsi v1 static
```

```
[HUAWEI-vsi-v1] pwsignal ldp
[HUAWEI-vsi-v1-ldp] npe-upe mac-withdraw enable
```

10.7.75 peer (VSI-LDP view)

Function

The **peer** command configures a peer for a VSI.

The **undo peer** command deletes the peer of a VSI.

By default, no peer is configured for a VSI.

Format

peer *peer-address* [**negotiation-vc-id** *vc-id*] [**tnl-policy** *policy-name*] [**upe**] [**ignore-standby-state**]

undo peer *peer-address* [**negotiation-vc-id** *vc-id*]

Parameters

Parameter	Description	Value
peer-address	Specifies the IPv4 address of the peer. Generally, it is specified as the loopback address of the peer.	The value is in dotted decimal notation.
negotiation-vc-id *vc-id*	Specifies the ID of a VC, which uniquely identifies the VC. Generally, this parameter is specified when the two ends with different VSI IDs need to interconnect.	*vc-id* cannot be the same as the IDs of other local VSIs. The negotiated VC IDs to the same peer must be different. The value is an integer ranging from 1 to 4294967295.
tnl-policy *policy-name*	Specifies the tunnel policy name of the peer.	The value is a string of 1 to 39 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
upe	Identifies whether the peer is a client PE, which applies to Hierarchical Virtual Private LAN Service (HVPLS).	-

Parameter	Description	Value
ignore-standby-state	Configures the created PW to ignore the secondary state sent from the peer device.	-

Views

VSI-LDP view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When you configure Martini VPLS, you need to run the **peer** command to configure a peer for the VSI.

Prerequisites

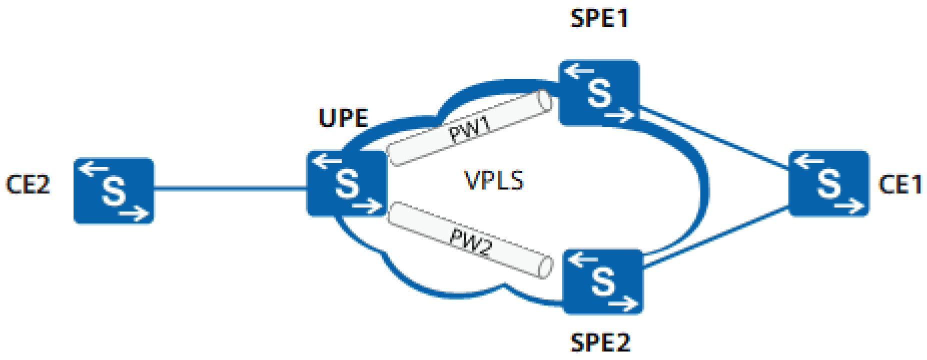
The VSI ID has been configured before you run this command.

- To configure a Spoke PW on the HVPLS network, you can configure **upe** in the **peer** command. If the specified peer is a UPE, the peer is on the user side, which does not comply with split horizon. If **upe** is not configured, a hub PW is configured, meaning that a VSI peer is specified and the peer is not specified as a UPE. Split horizon applies to hub PWs. Traffic from spoke PWs can be forwarded to spoke PWs and hub PWs, but traffic from hub PWs can only be forwarded to spoke PWs and not to hub PWs.

  NOTE

  Split horizon: The data packets received from the PW on the public network are not forwarded to other PWs, but only forwarded to the private network. On a VPLS network, full mesh and split horizon are used to avoid loops. HVPLS partitions the network, and the devices of different levels forward data to each other without complying with the split horizon scheme.
- To configure a VLL to access a VPLS network, you can adopt one of the following configurations to create a PW:
  - Configure the VSI ID on the VPLS network to be the same as the VC ID of the VLL peer.
  - Configure the value of **negotiation-vc-id** *vc-id* to be the same as the VC ID of the VLL peer.
- The **ignore-standby-state** parameter can be configured for PWs dual-homing a CE to PEs on a PW redundancy network. This setting enables the secondary PW to ignore the Backup state and remain in the Up state, preventing packet loss that occurs during a primary/secondary PW switchover. **Figure 10-2** shows PW redundancy networking with CEs asymmetrically accessing PEs.

Figure 10-2 VPLS PW redundancy networking



If the primary PW1 works properly, it transmits traffic over the path CE1–>SPE1–>UPE–>CE2. If PW1 fails, either of the following situations occurs based on the **ignore-standby-state** setting:

- If **ignore-standby-state** is configured on SPE2, PW2 remains in the Up state. After PW1 fails, SPE2 can forward CE1 traffic over the path CE1–>SPE2–>UPE–>CE2.
- If **ignore-standby-state** is not configured on SPE2, PW2 is in the Backup state before switching to the Up state. After PW1 fails and CE1 sends traffic to SPE2, SPE2 fails to forward traffic to UPE because PW2 does not become Up, causing traffic loss. After PW2 switches to the Up state, SPE2 can forward CE1 traffic over the path CE1–>SPE2–>UPE–>CE2, without traffic loss.

Precautions

After you run the **undo peer** command, all PW configurations created by the peer are deleted.

If the value of **negotiation-vc-id** *vc-id* is different from the value of *vsi-id* configured using the **vsi-id** command, you must configure **negotiation-vc-id** *vc-id* when running the **undo peer** command to delete the VSI peer. Otherwise, the system prompts that the VSI peer cannot be deleted.

Example

# Configure the peer for the current VSI.

```
<HUAWEI> system-view
[HUAWEI] vsi company1 static
[HUAWEI-vsi-company1] pwsignal ldp
[HUAWEI-vsi-company1-ldp] vsi-id 1
[HUAWEI-vsi-company1-ldp] peer 10.3.3.3 negotiation-vc-id 10 upe
```

# Delete the peer of a VSI.

```
<HUAWEI> system-view
[HUAWEI] vsi company1 static
[HUAWEI-vsi-company1] pwsignal ldp
[HUAWEI-vsi-company1-ldp] vsi-id 1
[HUAWEI-vsi-company1-ldp] peer 10.3.3.3 negotiation-vc-id 10 upe
[HUAWEI-vsi-company1-ldp] undo peer 10.3.3.3 negotiation-vc-id 10
```

10.7.76 peer preference (protect-group view)

Function

The **peer preference** command adds a specified PW to a PW protection group and specifies the priority of the PW.

The **undo peer preference** command deletes a specified PW from a PW protection group.

By default, no PW is added to a PW protection group.

Format

peer *peer-address* [**negotiation-vc-id** *vc-id*] **preference** *preference-value*

undo peer *peer-address* [**negotiation-vc-id** *vc-id*]

Parameters

Parameter	Description	Value
peer-address	Specifies the IPv4 address of the VSI peer. Generally, the loopback address of the peer is used.	-
negotiation-vc-id *vc-id*	Specifies the parameter negotiated with the peer. By default, the VSI ID is used. Generally, this parameter is used in VPLS accessing VLL scenarios in which the VSI IDs of the two ends are inconsistent and the two ends are required to communicate.	The value is an integer that ranges from 1 to 4294967295.
preference-value	Specifies the priority of a peer when the peer joins a PW protection group. The smaller the value, the higher the priority. Among the two peers added to a PW protection group, the one with the higher priority serves as the primary.	The value is an integer ranging from 1 to 32.

Views

protect-group view

Default Level

2. Configuration level

Usage Guidelines

Usage Scenario

After creating a PW protection group and specifying the PW redundancy mode, you can add specified PWs to the group for them to work in backup mode.

Prerequisites

A PW protection group has been created and the PW redundancy mode has been specified.

Precautions

Add PWs to a PW protection group in the descending order of PW priorities. Do not add the PW with a lower priority to the PW protection group first.

If you add the PW with a lower priority to the PW protection group first, a PW switchover will occur after you add the other PW to the PW protection group.

Example

# Add a specified PW to a PW protection group and set the priority of the PW to 1.

```
<HUAWEI> system-view
[HUAWEI] vsi vsi1
[HUAWEI-vsi-vsi1] pwsignal ldp
[HUAWEI-vsi-vsi1-ldp] peer 2.2.2.2
[HUAWEI-vsi-vsi1-ldp] protect-group group1
[HUAWEI-vsi-vsi1-ldp-protect-group-group1] peer 2.2.2.2 preference 1
```

10.7.77 peer pw

Function

The **peer pw** creates a PW and displays the PW view.

The **undo peer pw** deletes the created PW.

By default, no PW is created.

Format

peer *peer-address* [**negotiation-vc-id** *vc-id*] **pw** *pw-name*

undo peer *peer-address* [**negotiation-vc-id** *vc-id*] **pw**

Parameters

Parameter	Description	Value
peer *peer-address*	Specifies the IPv4 address of the peer. Generally, it is specified as the loopback address of the peer.	-

Parameter	Description	Value
negotiation-vc-id *vc-id*	Specifies the ID of a VC, which uniquely identifies the VC. Generally, this parameter is specified when the two ends with different VSI IDs need to interconnect.	*vc-id* cannot be the same as the IDs of other local VSIs. The negotiated VC IDs to the same peer must be different. The value is an integer ranging from 1 to 4294967295.
pw *pw-name*	Specifies the name of a PW. The PW name is used to distinguish the PW from other PWs, and must be unique in the same VSI. Nevertheless, the PW name can be used in other VSIs.	The value is a string of 1 to 15 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Views

VSI-LDP view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In Martini VPLS, you need to run the **peer pw** command to configure a PW after specifying a peer.

Prerequisites

The IP address of the peer has been specified using the **peer** *peer-address* command.

Precautions

If the value of **negotiation-vc-id** *vc-id* is different from the value of *vsi-id* configured using the **vsi-id** command, you must configure **negotiation-vc-id** *vc-id* when running the **undo peer pw** command to delete the PW. Otherwise, the PW cannot be deleted.

Example

# Create the PW view.

```
<HUAWEI> system-view
[HUAWEI] vsi aa static
[HUAWEI-vsi-aa] pwsignal ldp
[HUAWEI-vsi-aa-ldp] vsi-id 1
[HUAWEI-vsi-aa-ldp] peer 10.1.1.1
[HUAWEI-vsi-aa-ldp] peer 10.1.1.1 pw pw1
[HUAWEI-vsi-aa-ldp-pw-pw1]
```

# Delete the PW.

```
<HUAWEI> system-view
[HUAWEI] vsi aa static
[HUAWEI-vsi-aa] pwsignal ldp
[HUAWEI-vsi-aa-ldp] vsi-id 1
[HUAWEI-vsi-aa-ldp] peer 10.1.1.1
[HUAWEI-vsi-aa-ldp] peer 10.1.1.1 pw pw1
[HUAWEI-vsi-aa-ldp-pw-pw1] quit
[HUAWEI-vsi-aa-ldp] undo peer 10.1.1.1 pw
```

10.7.78 peer signaling

Function

The **peer signaling** command configures the signaling mode for a specified peer or peer group.

The **undo peer signaling** command restores the default signaling mode of a specified peer or peer group.

By default, after the **peer enable** command is run in the L2VPN AD address family view, the BGP AD signaling is enabled for all peers or peer groups.

Format

peer { *peer-address* | *group-name* } **signaling** { **vpws** | **vpls** | **vpls-ad disable** }

undo peer { *peer-address* | *group-name* } **signaling** { **vpws** | **vpls** | **vpls-ad disable** }

Parameters

Parameter	Description	Value
peer-address	Specifies an IPv4 address of a peer. The loopback address of the peer is usually used as its IPv4 address.	-
group-name	Specifies the name of a peer group.	The name is a string of 1 to 47 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
vpws	Configures the signaling mode of a specified peer or peer group as VPWS.	-
vpls	Configures the signaling mode of a specified peer or peer group as VPLS.	-
vpls-ad disable	Disables BGP AD signaling for a specified peer or peer group.	-

Views

L2VPN AD address family view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In Kompella VLL, Kompella VPLS, and BGP AD VPLS scenarios, configure the signaling mode for peers or peer groups in the L2VPN AD address family view so that peers can advertise routes to each other. The parameters used in different scenarios are described as follows:

- In the Kompella VLL scenario, configure **vpws** in the **peer signaling** command.
- In the Kompella VPLS scenario, configure **vpls** in the **peer signaling** command.
- In the BGP AD VPLS scenario, the BGP AD signaling is enabled for all peers or peer groups in the L2VPN AD address family view by default. Therefore, you need to run the **peer** { *peer-address* | *group-name* } **signaling vpls-ad disable** command to disable BGP AD signaling for a specified peer or peer group in Kompella VLL and Kompella VPLS scenarios.

Prerequisites

The **peer enable** command has been run to create a peer or peer group.

Precautions

For the same peer, the **peer enable** and **peer** { *peer-address* | *group-name* } **signaling** { **vpws** | **vpls** | **vpls-ad disable** } commands run in the L2VPN AD address family view are mutually exclusive with the **peer enable** command run in the VPLS address family view.

For the same peer, the **peer** { *peer-address* | *group-name* } **signaling vpws** command run in the L2VPN AD view is mutually exclusive with the **peer enable** command run in the L2VPN address family view.

The signaling mode configured for a peer is preferred over that configured for the peer group to which the peer belongs.

When a signaling mode is configured for a peer group but not configured for a peer that belongs to the peer group, the peer uses the signaling mode configured for its peer group.

Example

# Configure the signaling mode for peer 1.1.1.1 in the L2VPN AD address family view when Kompella VPLS is enabled.

```
<HUAWEI> system-view
[HUAWEI] bgp 100
[HUAWEI-bgp] l2vpn-ad-family
```

```
[HUAWEI-bgp-l2vpn-ad] peer 1.1.1.1 enable
[HUAWEI-bgp-l2vpn-ad] peer 1.1.1.1 signaling vpls
[HUAWEI-bgp-l2vpn-ad] peer 1.1.1.1 signaling vpls-ad disable
```

10.7.79 peer static-npe

Function

The **peer static-npe** command configures the static NPE peer of the VSI in the Hierarchical Virtual Private LAN Service (HVPLS).

The **undo peer static-npe** command deletes the static NPE peer of the VSI in the HVPLS.

By default, the HVPLS has no static NPE peer of the VSI.

Format

peer *peer-address* [**negotiation-vc-id** *vc-id*] [**tnl-policy** *policy-name*] **static-npe trans** *transmit-label* **recv** *receive-label*

undo peer *peer-address* [**negotiation-vc-id** *vc-id*]

Parameters

Parameter	Description	Value
peer-address	Specifies the IPv4 address of the static NPE peer. It is generally specified as the loopback address of the peer.	-
negotiation-vc-id *vc-id*	Indicates the unique ID of a VC. Generally, this parameter is used when the VSI IDs of two ends are inconsistent and the two ends are required to communicate.	*vc-id* cannot be the same as the IDs of other local VSIs. The negotiated VC IDs to the same peer must be different. The value is an integer ranging from 1 to 4294967295.
tnl-policy *policy-name*	Specifies the tunnel-policy name of the static NPE peer.	The value is a string of 1 to 39 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
static-npe	Indicates whether the peer of the static VSI is the PE at the network side.	-

Parameter	Description	Value
trans *transmit-label*	Indicates the outer label that is manually configured and sent from the local device to its peer. It is the outgoing label of the static Layer 2 VC.	The value is an integer ranging from 0 to 1048575.
recv *receive-label*	Indicates the outer label that is manually configured and sent from the peer to the local device. It is the incoming label of the static Layer 2 VC.	The value is an integer that ranges from 16 to 1023.

Views

VSI-LDP view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On the HVPLS network, you can run the **peer static-npe** command on the local device to configure a static NPE peer.

Prerequisites

The VSI ID has been configured using the **vsi-id** *vsi-id* command.

Precautions

If you specify **negotiation-vc-id** *vc-id* when you configure the peer of the VSI, and the specified *vc-id* and that in the configured **vsi-id** command are inconsistent, to delete the peer of the VSI, you must use the **undo peer** command with **negotiation-vc-id** *vc-id*. Otherwise, the peer cannot be deleted.

Example

# Configure the static NPE peer of the current VSI. Configure the received and sent outer labels are 100.

```
<HUAWEI> system-view
[HUAWEI] vsi company1
[HUAWEI-vsi-company1] pwsignal ldp
[HUAWEI-vsi-company1-ldp] vsi-id 1
[HUAWEI-vsi-company1-ldp] peer 3.3.3.3 static-npe trans 100 recv 100
```

10.7.80 peer static-upe

Function

The **peer static-upe** command configures the static UPE peer of the VSI in the HVPLS.

The **undo peer static-upe** command deletes the static UPE peer of the VSI in the HVPLS.

By default, the HVPLS has no static UPE peer of the VSI.

Format

peer *peer-address* [**negotiation-vc-id** *vc-id*] [**tnl-policy** *policy-name*] **static-upe trans** *transmit-label* **recv** *receive-label*

undo peer *peer-address* [**negotiation-vc-id** *vc-id*]

Parameters

Parameter	Description	Value
peer-address	Specifies the IPv4 address of the UPE peer. Generally, it is specified as the loopback address of the peer.	-
negotiation-vc-id *vc-id*	Specifies the ID of a VC, which uniquely identifies the VC. Generally, this parameter is specified when the two ends with different VSI IDs need to interconnect.	*vc-id* cannot be the same as the IDs of other local VSIs. The negotiated VC IDs to the same peer must be different. The value is an integer ranging from 1 to 4294967295.
tnl-policy *policy-name*	Specifies the tunnel-policy name of the static UPE peer.	The value is a string of 1 to 39 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
static-upe	Indicates whether the static UPE is a client PE device. This parameter applies to HVPLS.	-
trans *transmit-label*	Specifies the outer label that sent from the local device to its peer.	It is the outgoing label of the static Layer 2 VC. The value is an integer that ranges from 0 to 1048575.

Parameter	Description	Value
recv *receive-label*	Specifies the outer label manually configured and sent from the peer to the local device. It is the incoming label of the static Layer 2 VC.	The value is an integer that ranges from 16 to 1023.

Views

VSI-LDP view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On the HVPLS network, you can run the **peer static-upe** command on the local device to configure a static UPE peer.

Prerequisites

The VSI ID has been configured using the **vsi-id** *vsi-id* command.

Precautions

If **negotiation-vc-id** *vc-id* is used when configuring the VSI peer, and specified *vc-id* is different from *vsi-id* configured using the **vsi-id** command, you must configure **negotiation-vc-id** *vc-id* when running the **undo peer** command to delete the VSI peer. Otherwise, the VSI peer cannot be deleted.

Example

# Configure the static UPE peer of the current VSI. The sent and received outer labels are 100.

```
<HUAWEI> system-view
[HUAWEI] vsi company1
[HUAWEI-vsi-company1] pwsignal ldp
[HUAWEI-vsi-company1-ldp] vsi-id 1
[HUAWEI-vsi-company1-ldp] peer 3.3.3.3 static-upe trans 100 recv 100
```

10.7.81 ping vpls

Function

The **ping vpls** command detects the status of the PW and reachability of the peer.

Format

ping vpls [**-c** *echo-number* | **-m** *time-value* | **-s** *data-bytes* | **-t** *timeout-value* | **-r** *reply-mode* | **-exp** *exp-value* | **-v**] * **vsi** *vsi-name local-site-id remote-site-id*

ping vpls [**-c** *echo-number* | **-m** *time-value* | **-s** *data-bytes* | **-t** *timeout-value* | **-r** *reply-mode* | **-exp** *exp-value* | **-v**] * **vsi** *vsi-name* **peer** *peer-address* [**negotiate-vc-id** *vc-id*]

Parameters

Parameter	Description	Value
-c *echo-number*	Specifies the number of sent Echo Request packets.	The value is an integer that ranges from 1 to 4294967295. The default value is 5.
-m *time-value*	Specifies the time to wait before sending the next packet.	The value is an integer that ranges from 1 to 10000, in milliseconds. The default value is 2000 milliseconds.
-s *data-bytes*	Specifies the number of bytes of an Echo Request packet to be sent.	The value is an integer that ranges from 65 to 8100. The default value is 100.
-t *timeout-value*	Specifies the timeout period of sending Echo Request packets.	The value is an integer that ranges from 0 to 65535. The default value is 2000.
-r *reply-mode*	Specifies the mode in which the peer sends MPLS Echo Reply packets. The value is a decimal integer. The values are as follows: ● 1: indicates no reply. ● 2: indicates a reply with an IPv4 or IPv6 UDP datagram. ● 3: indicates a reply with an IPv4 or IPv6 UDP datagram carrying a router alert label. ● 4: indicates a reply through the control channel of the application plane.	The value ranges from 1 to 4. The default value is 2.
-exp *exp-value*	Specifies the EXP value of an Echo Request packet to be sent.	The value is an integer that ranges from 0 to 7.
-v	Displays detailed information.	-
vsi *vsi-name*	Specifies the name of a VSI.	The value is an existing VSI.

Parameter	Description	Value
local-site-id	Specifies the ID of the local CE.	The value is an integer that ranges from 0 to 65534.
remote-site-id	Specifies the ID of the remote CE.	The value is an integer that ranges from 0 to 65534.
peer *peer-address*	Specifies the IP address of the peer PE.	-
negotiate-vc-id *vc-id*	Specifies the ID of the local PW.	The value is an integer that ranges from 1 to 4294967295.

Views

All views

Default Level

0: Visit level

Usage Guidelines

Usage Scenario

After VPLS configurations are complete, you can run the **ping vpls** command to check the PW status and reachability of the peer.

- To check the PW status on a Kompella VPLS network, run the following command:

  ping vpls [**-c** *echo-number* | **-m** *time-value* | **-s** *data-bytes* | **-t** *timeout-value* | **-r** *reply-mode* | **-exp** *exp-value* | **-v**] * **vsi** *vsi-name local-site-id remote-site-id*

  .
- To check the PW status on a Martini or BGP AD VPLS network, run the following command:

  ping vpls [**-c** *echo-number* | **-m** *time-value* | **-s** *data-bytes* | **-t** *timeout-value* | **-r** *reply-mode* | **-exp** *exp-value* | **-v**] * **vsi** *vsi-name* **peer** *peer-address* [**negotiate-vc-id** *vc-id*]

  .

Prerequisites

One of the following operations has been performed before the **ping vpls** command is used:

- Configuring Kompella VPLS
- Configuring Martini VPLS

- Configuring BGP AD VPLS

Precautions

The timeout period specified by **-t** is less than the waiting time specified by **-m**.

Note the following points when configuring VPLS:

- If **negotiate-vc-id** is not specified in the **peer** command, *vc-id* is unique and equal to *vsi-id*. To perform the ping operation, you do not need to specify *vc-id* because the VC is unique when **vsi** *vsi-name* and **peer** *peer-address* are specified. In the same case, however, if **negotiate-vc-id** is specified and it is not equal to the actual *vc-id* (that is, *vsi-id*), an error message is displayed.
- If **negotiate-vc-id** (multiple VC IDs can be specified) in the **peer** command, you need to specify **negotiate-vc-id** in addition to **vsi** *vsi-name* and **peer** *peer-address* when performing the ping. If **negotiate-vc-id** is not found or specified, an error message is displayed.

Example

# Run the **ping vpls** command on the PE to check connectivity of the VSI named **bgp1** with remote site ID being 10.

```
<HUAWEI> ping vpls -c 10 -m 10 -s 65 -t 100 -v vsi bgp1 10 10
  Reply from 10.2.2.2: bytes=65 Sequence=1 time=2 ms Return Code 3, Subcode 1
  Reply from 10.2.2.2: bytes=65 Sequence=2 time=2 ms Return Code 3, Subcode 1
  Reply from 10.2.2.2: bytes=65 Sequence=3 time=3 ms Return Code 3, Subcode 1
  Reply from 10.2.2.2: bytes=65 Sequence=4 time=2 ms Return Code 3, Subcode 1
  Reply from 10.2.2.2: bytes=65 Sequence=5 time=3 ms Return Code 3, Subcode 1
  Reply from 10.2.2.2: bytes=65 Sequence=6 time=41 ms Return Code 3, Subcode 1
  Reply from 10.2.2.2: bytes=65 Sequence=7 time=4 ms Return Code 3, Subcode 1
  Reply from 10.2.2.2: bytes=65 Sequence=8 time=4 ms Return Code 3, Subcode 1
  Reply from 10.2.2.2: bytes=65 Sequence=9 time=3 ms Return Code 3, Subcode 1
  Reply from 10.2.2.2: bytes=65 Sequence=10 time=6 ms Return Code 3, Subcode 1

 --- FEC: L2 VPN ENDPOINT. Sender VEID = 10, Remote VEID = 10 ping statistics ---
  10 packet(s) transmitted
  10 packet(s) received
  0.00% packet loss
  round-trip min/avg/max = 2/7/41 ms
```

Table 10-135 Description of the ping vpls command output

Item	Description
Return Code	Return code. Different values have different meanings: ● 0: indicates that no return code is received. ● 1: indicates that an incorrect request is received. ● 2: indicates that an unknown TLV is received. ● 3: indicates that there is the outbound interface of one LSP. ● 4: indicates that there is no mapping on the response router. ● 5: indicates that the mapping does not match that on the downstream device. ● 6: indicates that an unknown upstream interface exists. ● 7: indicates that the field is reserved. ● 8: indicates label switching. ● 9: indicates label switching without MPLS forwarding. ● 10: indicates mapping without labels. ● 11: indicates the entity without labels. ● 12: indicates that no protocol is loaded on the interface. ● 13: indicates that the ping operation terminates because there is only one label.
Subcode	Subcode, indicating the number of layers of the labels. Usually, the value is 1.

# Run the **ping vpls** command on the PE to check the connectivity of a PW in the Martini VPLS.

```
<HUAWEI> ping vpls vsi a2 peer 10.2.2.2
  Reply from 10.2.2.2: bytes=100 Sequence=1 time=3 ms
  Reply from 10.2.2.2: bytes=100 Sequence=2 time=6 ms
  Reply from 10.2.2.2: bytes=100 Sequence=3 time=6 ms
  Reply from 10.2.2.2: bytes=100 Sequence=4 time=6 ms
  Reply from 10.2.2.2: bytes=100 Sequence=5 time=6 ms

 --- FEC: FEC 128 PSEUDOWIRE (NEW). Type = vlan, ID = 10 ping statistics ---
  5 packet(s) transmitted
  5 packet(s) received
  0.00% packet loss
  round-trip min/avg/max = 3/4/6 ms
```

Table 10-136 Description of the ping vpls command output

Item	Description
Reply from x.x.x.x	Response from the destination host to each Echo Request packet: ● bytes: indicates the length of the response packet. ● sequence: indicates the sequence number of the response packet. ● time: indicates the response time, in ms. If no response packet is received after the timeout period, the message "Request time out" is displayed.
FEC: FEC 128 PSEUDOWIRE	Check on FEC 128, namely, check on a Martini VPLS PW.
Type = vlan	VLAN encapsulation on packets.
ID = 10	The VSI ID being 10.

# Run the **ping vpls** command on the PE to check the connectivity of a PW in the BGP AD VPLS.

```
<HUAWEI> ping vpls vsi ad peer 10.2.2.2
   Reply from 10.2.2.2: bytes=100 Sequence=1 time=30 ms
   Reply from 10.2.2.2: bytes=100 Sequence=2 time=60 ms
   Reply from 10.2.2.2: bytes=100 Sequence=3 time=60 ms
   Reply from 10.2.2.2: bytes=100 Sequence=4 time=60 ms
   Reply from 10.2.2.2: bytes=100 Sequence=5 time=60 ms

 --- FEC: FEC 129 PSEUDOWIRE. Sender = 1.1.1.1, Remote = 10.2.2.2 ping statisti
cs ---
   5 packet(s) transmitted
   5 packet(s) received
   0.00% packet loss
   round-trip min/avg/max = 30/54/60 ms
```

Table 10-137 Description of the ping vpls command output

Item	Description
Reply from x.x.x.x	Response from the destination host to each Echo Request packet: ● bytes: indicates the length of the response packet. ● sequence: indicates the sequence number of the response packet. ● time: indicates the response time, in ms. If no response packet is received after the timeout period, the message "Request time out" is displayed.
FEC: FEC 129 PSEUDOWIRE	Check on FEC 129, namely, check on a BGP AD VPLS PW.
Sender = x.x.x.x	Address of the sender.

Item	Description
Remote = x.x.x.x	Address of the destination host.

10.7.82 ping vpls mac vsi

Function

The **ping vpls mac vsi** command checks the connectivity of Layer 2 forwarding links on the VPLS network.

Format

ping vpls mac *mac-address* **vsi** *vsi-name* [**vlan** *vlan-id* | **-c** *count* | **-m** *time-value* | **-s** *packsize* | **-t** *timeout* | **-exp** *exp* | **-r** *replymode* | **-h** *ttl*] *

ping vpls mac *mac-address* **vsi** *vsi-name* **rapid** [**vlan** *vlan-id* | **-c** *count* | **-s** *packsize* | **-t** *timeout* | **-exp** *exp* | **-r** *replymode* | **-h** *ttl*] *

Parameters

Parameter	Description	Value
mac *mac-address*	Specifies the unicast destination MAC address of the VPLS MAC ping, expressed in the format of H-H-H.	An H is a hexadecimal number of 1 to 4 bits, such as 00e0 and fc01. If you enter less than four digits, 0s are padded before the input digits. For example, if e0 is entered, 00e0 is displayed. The value cannot be a broadcast or multicast MAC address.
vsi *vsi-name*	Specifies the name of a VSI.	The value is an existing VSI.
vlan *vlan-id*	Specifies the ID of a VLAN	*vlan-id* specifies the VLAN ID, which is an integer that ranges from 1 to 4094.

Parameter	Description	Value
rapid	Indicates that VPLS MAC ping packets are sent in **rapid** mode. This parameter can be used if each response message is not concerned and multiple ping operations need to be performed within a shot period of time. This configuration allows all packets to be sent at the same time, and only summary statistics are displayed.	-
-c *count*	Specifies the number of VPLS MAC Ping Request packets to be sent.	The value ranges from 1 to 4294967295. The default value is 5.
-m *time-value*	Specifies the time to wait before sending the next VPLS MAC Ping Request packet.	The value ranges from 1 to 10000, in milliseconds. The default value is 2000 ms.
-s *packsize*	Specifies the size of the VPLS MAC Ping Request packet.	The value ranges from 142 to 1442, in bytes. The default value is 142 bytes.
-t *timeout*	Specifies the timeout period for waiting for a Reply packet in response to a VPLS MAC Ping Request packet.	The value ranges from 0 to 65535, in milliseconds. The default value is 2000 ms.
-exp *exp*	Specifies the priority.	The value ranges from 0 to 7. The default value is 0.
-r *replymode*	Specifies the reply mode, that is, the Reply packet is sent from the control layer or the data layer. Enumerated type.	-
-h *ttl*	Specifies the TTL value of an Echo Request packet to be sent.	The value ranges from 1 to 255. The default value is 30.

Views

All views

Default Level

0: Visit level

Usage Guidelines

Using the **ping vpls mac vsi** command, you can check the connectivity of Layer 2 forwarding links on the VPLS network.

Example

# On the VPLS network, check whether the device with the MAC address of 00e0-fc12-3456 is reachable.

```
<HUAWEI> ping vpls mac 00e0-fc12-3456 vsi v123
Ping mac 00e0-fc12-3456 vsi v123 : 100 data bytes , press CTRL_C to break
    Reply from 10.1.1.1 : bytes=100 sequence=1 time = 1ms
    Reply from 10.1.1.1 : bytes=100 sequence=2 time = 1ms
    Reply from 10.1.1.1 : bytes=100 sequence=3 time = 2ms
    Reply from 10.1.1.1 : bytes=100 sequence=4 time = 3ms
    Reply from 10.1.1.1 : bytes=100 sequence=5 time = 2ms
    The IP address of the PE is 5.5.5.5 and the interface on the PE is GigabitEthernet0/0/1.

  --- vsi : v123 00e0-5952-6f01 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 1/2/3 ms
```

10.7.83 ping vpls multicast

Function

The **ping vpls multicast** command starts an MFIB ping test with a specified VSI in the VPLS domain.

Format

ping vpls multicast vsi *vsi-name* [**-a** *source-ip-address* | **-c** *count* | **-s** *packetsize* | **-t** *timeout* | **-m** *interval* | **-r** *replymode* | **-exp** *exp* | **-v**] * *dest-ip-address*

Parameters

Parameter	Description	Value
vsi *vsi-name*	Specifies the name of the VSI on which the operation is performed.	The value is an existing VSI.
-a *source-ip-address*	Specifies the multicast source IP address. By default, the multicast source IP address is the IP address of the initiator. The value is in dotted decimal notation.	-

Parameter	Description	Value
-c *count*	Specifies the number of Echo Request packets to be sent.	The value is an integer that ranges from 1 to 4294967295. The default value is 5.
-s *packetsize*	Specifies the length of the payload in the Echo Request packet, which should be smaller than the MTU value.	The value ranges from 100 to 1442, in bytes. The default value is 100.
-t *timeout*	Specifies the timeout period for waiting for an Echo Reply packet.	The value ranges from 0 to 65535, in milliseconds. The default value is 2000 milliseconds.
-m *interval*	Specifies the time to wait before sending the next Echo Request packet.	The value ranges from 1 to 10000, in milliseconds. The default value is 2000 milliseconds.
-r *replymode*	Specifies the reply mode. The default value is 2. ● 1: indicates that the peer end does not respond to Echo Request packets. ● 2: indicates that the peer end responds to Echo Request packets with IPv4 or IPv6 UDP packets. ● 3: indicates that the peer end responds to Echo Request packets with IPv4 or IPv6 UDP packets carrying the Router Alert option. ● 4: indicates that the peer end responds to Echo Request packets through the control channel of the application program grade. ● 5: indicates that the peer end responds to Echo Request packets with VPLS IPv4 UDP packets. **NOTE** Currently, the switch only supports mode 1, 2, and 5.	-

Parameter	Description	Value
-exp *exp*	Specifies the priority of Echo Request packets to be sent.	The value is an integer that ranges from 0 to 7. The default value is 0.
-v	Specifies the displayed details.	-
dest-ip-address	Specifies the multicast IP address.	-

Views

All views

Default Level

0: Visit level

Usage Guidelines

Usage Scenario

Using the **ping vpls multicast** command, you can start an MFIB ping test with a specified VSI in the VPLS domain and obtain information about the egress that is in the VPLS domain and can normally receive specified IP multicast packets. In addition, you can check whether the IGMP snooping function is normal.

Precautions

- To check whether the IGMP snooping function is normal, enable IGMP snooping of the VSI to trigger the exchange of IGMP Query packets and Report packets between the multicast source and receiver and specify a non-reserved multicast address as the destination address to initiate the VPLS multicast ping.
- The **ping vpls multicast** command does not support BGP AD VPLS.

After receiving a VPLS multicast Ping packet, the egress in the VPLS domain sends a Reply packet to the sender. The sender can determine the connectivity of the egress and the round trip delay according to the received Reply packet.

You can check the IGMP snooping function in the following scenarios:

- If IGMP snooping is enabled on a PE and the **ping vpls multicast** command run on the PE contains the **-v** parameter, the MPLS Echo packet received by the initiator carries information about interfaces at the AC side of the PE. If the initiator does not receive the Echo Reply packet of the PE, it considers the IGMP snooping function faulty.
- If a certain PE is not enabled with the IGMP snooping function, the Echo Reply packet received by the initiator does not carry information about interfaces at the AC side of the PE.

Example

# Initiate an MFIB ping test with a specified VSI in the VPLS domain.

```
<HUAWEI> ping vpls multicast vsi aaa -a 11.11.11.1 -c 2 -v 225.0.0.1
ping 225.0.0.1 : 56 data bytes , press CTRL-C to break

Seq Node-id Path Size RTT
--------------------------------------------------------------------------------
[Send request Seq. 1.]
1 51.51.51.51: ge0/0/1 Self 100 0ms
1 52.52.52.52: ge0/0/2 In-Band 100 20ms
1 54.54.54.54: ge0/0/2 In-Band 100 10ms

[Send request Seq. 2.]
2 51.51.51.51: ge0/0/1 Self 100 0ms
2 52.52.52.52: ge0/0/2In-Band 100 10ms
2 54.54.54.54: ge0/0/2 In-Band 100 20ms
--------------------------------------------------------------------------------
--225.0.0.1 ping statistics--
2 packets transmitted
4 packets received
round-trip min/avg/max = 10/15/20 ms
```

Table 10-138 Description of the ping vpls multicast command output

Item	Description
Seq	Sequence number of the packet.
Node-id	Response address, which carries the port number if it contains forwarding information about the AC side.
Path	Path. ● Self: indicates that packets are sent from the local end (AC side). ● In-Band: indicates that packets are sent from the data link layer (PW side).
Size	Size of the packet.
RTT	Round trip time.

10.7.84 ping vpn-config

Function

The **ping vpn-config** command checks whether configurations on both ends of a VPN are consistent, which can help you locate faults on the VPN connection.

Format

ping vpn-config peer-address *peer-address* **vsi-name** *vsi-name* [**pw-id** *pw-id*] [**local**] [**remote**]

Parameters

Parameter	Description	Value
peer-address *peer-address*	Specifies the IP address of the peer PE.	-
vsi-name *vsi-name*	Specifies the name of the VSI on which the operation is performed.	The value is an existing VSI.
pw-id *pw-id*	Specifies the ID of the PW.	The value is an integer that ranges from 1 to 4294967295. This parameter cannot be specified in the BGP AD VPLS networking.
local	Indicates that the Request packet is encapsulated in LSP mode.	-
remote	Indicates that the Reply packet is encapsulated in LSP mode.	-

Views

All views

Default Level

0: Visit level

Usage Guidelines

Usage Scenario

Using the **ping vpn-config** command, you can check whether configurations on both ends of a VPN are consistent, which can help you locate faults on the VPN connection.

The **ping vpn-config** command is used to send a Request packet from the local PE to the peer PE to obtain VPN configurations of the peer PE, such as the VSI name, status, PW type, MTU value, and number of CEs. After the local PE receives the VPN configuration of the peer PE, it displays the information on the local. This can help you locate the fault on the VPN.

Precautions

The **ping vpn-config** command is applied to VPLS networks, dynamic PWE3 networks, and VLL accessing the VPLS networks.

NOTE

The timeout period of the **ping vpn-config** command is 10 seconds.

Example

# Run the **ping vpn-config** command to ping the peer PE in Martini VPLS networking.

```
<HUAWEI> ping vpn-config peer-address 3.3.3.9 vsi-name a2
VPN-CONFIG PING: Press CTRL_C to break.
Result Detail: Request Sent - Reply Received
Local VPN description:
Remote VPN description:
PW State: Up
                    local          remote
-----------------------------------------------
VPN Type:           Martini VPLS    Martini VPLS
VSI Name:           a2              a2
VSI ID:             2               2
Admin State:        Up              Up
Oper State:         Up              Up
MTU:                1500            1500
CE Count:           1               1
Control Word:       N/A             N/A
Primary Or Secondary: N/A           N/A

Actual IP Addr:     1.1.1.9         3.3.3.9
Expected Peer IP:   3.3.3.9         1.1.1.9
SPE:                NO              NO

PW-ID:              2               2
VC-Type:            vlan            vlan
Egress Label:       1025            1026
Ingress Label:      1026            1025

LSP Tunnel Used:    NO              NO
```

# Perform a service ping operation with the destination address being 3.3.3.9 in BGP AD VPLS networking.

```
<HUAWEI> ping vpn-config peer-address 3.3.3.9 vsi-name vplsad1
VPN-CONFIG PING: Press CTRL_C to break.
Result Detail: Request Sent - Reply Received
Local VPN description:
Remote VPN description:
PW State: Up
                    local               remote
---------------------------------------------------------------
VPN Type:           BGPAD VPLS          BGPAD VPLS
VSI Name:           vplsad1             vplsad1
Admin State:        Up                  Up
Oper State:         Up                  Up
MTU:                1500                1500
CE Count:           1                   1

Actual IP Addr:     1.1.1.9             3.3.3.9
Expected Peer IP:   3.3.3.9             1.1.1.9
SPE:                NO                  NO

VC-Type:            vlan                vlan
Egress Label:       1026                1027
Ingress Label:      1027                1026

VPLS ID:            168.1.1.1:1         168.1.1.1:1
RD:                 168.1.1.1:1         168.1.1.1:1
Import VPN target:  100:1               100:1
Export VPN target:  100:1               100:1

LSP Tunnel Used:    NO                  NO
```

Table 10-139 Description of the ping vpn-config command output

Item	Description
Result details	Details of the command operation result.
Local VPN description	Description of the local VPN. To set the value, run the **description** command.
Remote VPN description	Description of the peer VPN.
PW State	Status of a PW.
Local	Configuration of the local PE.
Remote	Configuration of the remote PE.
VPN Type	Type of a VPN.
VSI Name	Name of a VSI.
VSI ID	ID of a VSI. To set the value, run the **vsi-id** command.
Admin State	VSI administration status.
Oper State	VSI operating status.
MTU	MTU of the VSI. In PWE3 networking, it refers to the MTU of an AC interface; in VPLS networking, it refers to the MTU of a VSI.
CE Count	Number of AC links.
Control Word	Whether the control word is enabled: ● Enable ● Disable
Primary Or Secondary	Displayed as a PW on the local end and always displayed as N/A on the remote end.
Actual IP Addr	Actual IP address.
Expect IP Addr	Expected IP address.
SPE	Whether it is a SPE
PW ID	ID of a PW.
VC-Type	Encapsulation type of the VC. ● Ethernet: indicates that the encapsulation type of the VC is Ethernet. ● VLAN: indicates that the encapsulation type of the VC is VLAN.
Egress Label	Outgoing label.

Item	Description
Ingress Label	Incoming label.
VPLS ID	VPLS ID To set the value, run the **vpls-id** command.
RD	Route tag. To set the value, run the **route-distinguisher** command.
Import VPN target	Import VPN target.
Export VPN target	Export VPN target.
LSP Tunnel Used	Whether the packet is encapsulated in LSP mode.

10.7.85 protect-group (VSI-LDP view)

Function

The **protect-group** command creates a PW protection group. If the PW protection group to be created already exists, the PW protection group view is displayed.

The **undo protect-group** command deletes a specified PW protection group.

By default, no PW protection group is created in a VSI.

Format

protect-group *group-name*

undo protect-group *group-name*

Parameters

Parameter	Description	Value
group-name	Specifies the name of a PW protection group.	The value is a string of 1 to 15 case-sensitive characters without spaces or hyphens (-). When double quotation marks are used around the string, spaces are allowed in the string.

Views

VSI-LDP view

Default Level

2. Configuration level

Usage Guidelines

Usage Scenario

Multiple PWs can be created in a VSI.

You can create multiple PW protection groups for a VSI. After you add two PWs to a PW protection group, the two PWs will work in backup mode.

Prerequisites

The VSI ID has been configured using the **vsi-id** *vsi-id* command in the VSI-LDP view.

Follow-up Procedure

After creating PW protection groups, configure the PW redundancy mode of each PW protection group, add PWs to these groups, and configure revertive switching policies for these groups.

Example

# Create a PW protection group named group1.

```
<HUAWEI> system-view
[HUAWEI] vsi vsi1
[HUAWEI-vsi-vsi1] pwsignal ldp
[HUAWEI-vsi-vsi1-ldp] vsi-id 10
[HUAWEI-vsi-vsi1-ldp] protect-group group1
```

10.7.86 protect-mode (protect-group view)

Function

The **protect-mode** command specifies the PW redundancy mode of a PW protection group.

The **undo protect-mode** command cancels the PW redundancy mode of a PW protection group.

By default, a PW protection group does not have a PW redundancy mode.

Format

protect-mode pw-redundancy master

undo protect-mode

Parameters

Parameter	Description	Value
pw-redundancy master	Specifies the PW redundancy mode of a PW protection group as master/slave.	-

Views

protect-group view

Default Level

2. Configuration level

Usage Guidelines

Usage Scenario

You can configure PW protection groups to protect PW pairs of a VSI.

In the scenarios, in which the active/standby PWs cannot be determined based on the signaling sent by the remote end, you can create a PW protection group on the UPE, and specify the PW redundancy mode of the group as master/slave. The local UPE determines the active/standby PWs based on the priorities configured using the **peer preference** command.

NOTE

When the mode of the group is master/slave, the local UPE does not determine the active/standby PWs based on the signaling sent by the remote end.

Prerequisites

The PW protection group has been configured using the **protect-group** command.

Precautions

A static hub PW and a static spoke PW cannot be added to the same protection group.

After a PW protection group is configured, you must specify the PW redundancy mode before configuring other parameters. Deleting the PW redundancy mode of a PW protection group will clear all the configurations of the group.

Example

# Configure the PW redundancy mode of a PW protection group as PW redundancy master/slave.

```
<HUAWEI> system-view
[HUAWEI] vsi vsi1
[HUAWEI-vsi-vsi1] pwsignal ldp
[HUAWEI-vsi-vsi1-ldp] protect-group group1
[HUAWEI-vsi-vsi1-ldp-protect-group-group1] protect-mode pw-redundancy master
```

10.7.87 protect-switch (protect-group view)

Function

The **protect-switch** command triggers a manual protection switchover or cancels the manual switchover in a protection group.

Format

protect-switch { **manual** | **clear** }

Parameters

Parameter	Description	Value
manual	Forcibly performs a PW switchover to switch traffic from the high-priority primary PW to the low-priority backup PW.	-
clear	Cancels the **manual** PW switchover to switch traffic from the low-priority backup PW back to the high-priority primary PW.	-

Views

protect-group view

Default Level

2. Configuration level

Usage Guidelines

Usage Scenario

If you want to maintain the device where the primary PW in a PW protection group resides, you must use a command to switch traffic from the primary PW to the secondary PW first. After the device where the primary PW resides is stable, you need to use this command to switch traffic back from the secondary PW to the primary PW.

Prerequisites

A PW protection group has been created and the PW redundancy mode is master/slave. The primary and secondary PWs have joined the PW protection group and their status is Up.

Precautions

After you run the **protect-switch manual** command, traffic switches from the primary PW to the secondary PW. After you run the **protect-switch clear** command, traffic switches from the secondary PW to the primary PW.

After you run the **protect-switch manual** command, service traffic is always transmitted over the low-priority backup PW. To enable service traffic to be transmitted over a high-priority PW, run the **protect-switch clear** command to cancel the manual switchover. The manual switchover is also cancelled when the priorities of the primary and backup PWs change in some situations, for example, a PW is Down or you change their priority values. In these situations, the system selects the PW with a higher priority to transmit service traffic.

Example

# Forcibly perform an active/standby PW switchover in the current PW protection group.

```
<HUAWEI> system-view
[HUAWEI] vsi vsi1
[HUAWEI-vsi-vsi1] pwsignal ldp
[HUAWEI-vsi-vsi1-ldp] protect-group group1
[HUAWEI-vsi-vsi1-ldp-protect-group-group1] protect-switch manual
```

10.7.88 pw

Function

The **pw** command displays the PW view.

The **undo pw** command deletes the PW view.

By default, the PW view is not displayed.

Format

pw *pw-name*

undo pw *pw-name*

Parameters

Parameter	Description	Value
pw-name	Specifies the name of a PW.	The value is a string of 1 to 15 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Views

VSI-LDP view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After a PW is created, you can run the **pw** *pw-name* command to enter the PW view.

Prerequisites

A PW has been created using the **peer** *peer-address* [**negotiation-vc-id** *vc-id*] **pw** *pw-name* command.

Precautions

The PW name must be unique in a VSI, and the PW name can be the same in different VSIs.

Example

# Enter the PW view.

```
<HUAWEI> system-view
[HUAWEI] vsi aa static
[HUAWEI-vsi-aa] pwsignal ldp
[HUAWEI-vsi-aa-ldp] vsi-id 1
[HUAWEI-vsi-aa-ldp] peer 10.1.1.1
[HUAWEI-vsi-aa-ldp] peer 10.1.1.1 pw pw1
[HUAWEI-vsi-aa-ldp-pw-pw1] quit
[HUAWEI-vsi-aa-ldp] pw pw1
```

10.7.89 pwsignal

Function

The **pwsignal** command configures the signaling mode for a VSI.

By default, no signaling mode is configured for a VSI.

Format

pwsignal { **bgp** | **ldp** }

Parameters

Parameter	Description	Value
bgp	Uses the BGP signing mode.	-
ldp	Uses the LDP signaling mode.	-

Views

VSI view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When configuring the Martini or Kompella VPLS, you need to run the **pwsignal** command to configure a signaling mode for a VSI.

Precautions

If the member discovery mode of the VSI is static, the signaling mode must be LDP. If the member discovery mode of the VSI is automatic, the signaling mode must be BGP.

After the signaling mode is configured successfully for the VSI, it cannot be modified. If you want to change the signaling mode, you must delete the VSI and re-create VSI.

Example

# Configure the signaling mode of the VSI as LDP.

```
<HUAWEI> system-view
[HUAWEI] vsi company1 static
[HUAWEI-vsi-company1] pwsignal ldp
[HUAWEI-vsi-company1-ldp]
```

# Configure the signaling mode of the VSI as BGP.

```
<HUAWEI> system-view
[HUAWEI] vsi company2 auto
[HUAWEI-vsi-company2] pwsignal bgp
[HUAWEI-vsi-company2-bgp]
```

10.7.90 pw spoke-mode (VSI-BGPAD view)

Function

The **pw spoke-mode** command configures all PWs of a BGP AD VSI as spoke PWs.

The **undo pw spoke-mode** command restores the default setting.

By default, all PWs of a BGP AD VSI are hub PWs.

Format

pw spoke-mode

undo pw spoke-mode

Parameters

None

Views

VSI-BGPAD view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If a BGP AD VPLS needs to be deployed on a network with a star or tree topology (on which one PE that serves as a server or an authorization device is configured as the hub PE, and other PEs are configured as spoke PEs), all PWs of the VSI on the hub PE must be configured as spoke PWs to disable split horizon of the PWs. Traffic from spoke PWs can be forwarded to spoke PWs and hub PWs, but traffic from hub PWs can only be forwarded to spoke PWs and not to hub PWs.

Prerequisites

The VPLS ID has been configured using the **vpls-id** *vpls-id* command in the VSI-BGPAD view.

Precautions

The **pw spoke-mode** command takes effect on all the PWs of a BGP AD VSI.

After the **pw spoke-mode** command is run, all PWs of the specified VSI become spoke PWs. Split horizon does not function on spoke PWs. This means that packets sent from Spoke PWs can be forwarded to other PWs. If the **undo pw spoke-mode** command is run, all PWs of the VSI will be changed to hub PWs that comply with split horizon rules.

Example

# Create a BGP AD VSI named **company1** and configure all the PWs of the VSI as spoke PWs.

```
<HUAWEI> system-view
[HUAWEI] vsi company1
[HUAWEI-vsi-company1] bgp-ad
[HUAWEI-vsi-company1-bgpad] vpls-id 65535:1
[HUAWEI-vsi-company1-bgpad] pw spoke-mode
```

10.7.91 remote-vpn-target refresh

Function

The **remote-vpn-target refresh** command refreshes the remote VPN target manually.

Format

remote-vpn-target refresh

Parameters

None

Views

VSI-BGP view

Default Level

2: Configuration level

Usage Guidelines

When locating a Kompella VPLS fault, you can use the **remote-vpn-target refresh** command to refresh the remote VPN target manually.

Example

# Refresh the remote VPN target.

```
<HUAWEI> system-view
[HUAWEI] vsi company2
[HUAWEI-vsi-company2] pwsignal bgp
[HUAWEI-vsi-company2-bgp] remote-vpn-target refresh
```

10.7.92 reroute (protect-group view)

Function

The **reroute** command configures a revertive switching policy for a PW protection group with the master/slave PW redundancy mode.

The **undo reroute** command deletes the revertive switching policy for a PW protection group with the master/slave PW redundancy mode.

The default revertive switching policy for a PW protection group with the master/slave PW redundancy mode is delayed switchback and the default delay is 30s.

Format

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

undo reroute

Parameters

Parameter	Description	Value
delay *delay-time*	Specifies that the revertive switching policy is delayed switchback.	The value is an integer ranging from 10 to 600, in seconds. The default value is 30s.
immediately	Specifies that the revertive switching policy is immediate switchback.	-
never	Specifies that the revertive switching policy is non-revertive. Traffic does not switch back to the primary PW even after the primary PW recovers. Traffic will be switched back to the primary PW only when the secondary PW fails.	-

Views

protect-group view

Default Level

2. Configuration level

Usage Guidelines

Usage Scenario

The **reroute** command can configure revertive switching policies for only PW protection groups with the master/slave PW redundancy mode. The revertive switching policy for PW protection groups with the independent PW redundancy mode is immediate switchback and cannot be modified.

Currently, three types of revertive switching policies are available:

- Delayed switchback: Traffic is switched back to the primary PW after the delay time specified in *delay-time*. After the switchover is performed, the UPE notifies the remote PE on the secondary PW of a fault. On a large-scale network, packet loss caused by incomplete route convergence may occur during the switchback. To prevent this problem, configure traffic to be switched back after a delay.
- Immediate switchback: Traffic is immediately switched back to the primary PW. This revertive switching policy applies to scenarios in which users hope traffic to be restored as soon as possible.
- Non-revertive: Traffic will not be switched back to the primary PW even after the primary PW recovers. Traffic will be switched back to the primary PW only when the secondary PW fails. If you do not want traffic to be frequently switched between the primary and secondary PWs, you can use the non-revertive policy.

Prerequisites

The PW redundancy mode of the PW protection group is master/slave.

Precautions

The revertive switching policy determines the switchback behavior of the traffic after the primary PW recovers.

Example

# Configure the primary and secondary PWs in a PW protection group to perform a switchback after a delay of 60s.

```
<HUAWEI> system-view
[HUAWEI] vsi vsi1
[HUAWEI-vsi-vsi1] pwsignal ldp
[HUAWEI-vsi-vsi1-ldp] protect-group group1
[HUAWEI-vsi-vsi1-ldp-protect-group-group1] reroute delay 60
```

10.7.93 reset bgp l2vpn-ad

Function

The **reset bgp l2vpn-ad** command resets the BGP connections associated with L2VPN-AD.

Format

reset bgp l2vpn-ad { **all** | *as-number-plain* | *as-number-dot* | *ipv4-address* | **group** *group-name* | **external** | **internal** } [**graceful**]

Parameters

Parameter	Description	Value
l2vpn-ad	Resets BGP connections associated with L2VPN-AD.	-
all	Resets all the BGP connections.	-
as-number-plain	Integral AS number	The value is an integer ranging from 1 to 4294967295.
as-number-dot	AS number in dotted notation	The value is in the format of *x.y*, where *x* and *y* are integers that range from 1 to 65535 and from 0 to 65535, respectively.
ipv4-address	Resets the connections with a specified BGP peer.	It is in dotted decimal notation.
group *group-name*	Resets the BGP connections with the specified peer group.	The name is a string of 1 to 47 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
external	Resets all EBGP connections.	-
internal	Resets all IBGP connections.	-
graceful	Specifies to reset BGP connections in GR mode.	-

Views

User view

Default Level

2: Configuration level

Usage Guidelines

The **reset bgp l2vpn-ad** command is used to make new BGP configurations associated with L2VPN-AD take effect.

⚠ CAUTION

After you run this command, the TCP connection is reset, and the neighbor relationship between two peers is reestablished. So, confirm the action before you use the command.

Example

# Reset all BGP L2VPN-AD connections.

```
<HUAWEI> reset bgp l2vpn-ad all
```

10.7.94 reset oam-mac statistics

Function

The **reset oam-mac statistics** command clears the statistics about the number of MAC diagnostic packets.

Format

reset oam-mac statistics { **populate** | **purge** | **purge-register** | **all** }

Parameters

Parameter	Description	Value
populate	Indicates the statistics about the number of populate packets.	-
purge	Indicates the statistics about the number of purge packets.	-
purge-register	Indicates the statistics about the number of purge + register packets.	-
all	Indicates the statistics about the number of MAC diagnostic packets.	-

Views

All views

Default Level

3: Management level

Usage Guidelines

Using the **reset oam-mac statistics** command, you can clear the statistics about the number of MAC diagnostic packets.

NOTICE

The statistics about MAC diagnostic packets cannot be restored once they are cleared. Confirm the action before you run the **reset oam-mac statistics** command.

Example

# Display the statistics about the number of all MAC diagnostic packets that are received by the device.

```
<HUAWEI> display oam-mac statistics all
 Received populate packet: 3
 Received purge packet: 1
 Received purge register packet: 2
```

# Clear the statistics about the number of MAC diagnostic packets that are received by the device.

```
<HUAWEI> reset oam-mac statistics all
```

# Display the statistics about the number of MAC diagnostic packets that are received by the device. It is found that all the statistics are cleared.

```
<HUAWEI> display oam-mac statistics all
 Received populate packet: 0
 Received purge packet: 0
 Received purge register packet: 0
```

10.7.95 reset vpls multicast-ping statistics

Function

The **reset vpls multicast-ping statistics** command clears the statistics on the number of MFIB Ping packets.

Format

reset vpls multicast-ping statistics

Parameters

None

Views

User view

Default Level

3: Management level

Usage Guidelines

You can run this command to clear the statistics on the number of sent and received MFIB Ping packets.

Example

# Reset the statistics on the number of MFIB Ping packets.

```
<HUAWEI> reset vpls multicast-ping statistics
```

10.7.96 reset vpls multicast-trace statistics

Function

The **reset vpls multicast-trace statistics** command clears the statistics on the number of MFIB Trace packets.

Format

reset vpls multicast-trace statistics

Parameters

None

Views

User view

Default Level

3: Management level

Usage Guidelines

You can run this command to clear the statistics on the number of sent and received MFIB Trace packets.

Example

# Reset the statistics on the number of MFIB Trace packets.

```
<HUAWEI> reset vpls multicast-trace statistics
```

10.7.97 reset vpls-ping statistics

Function

The **reset vpls-ping statistics** command clears the statistics about the number of VPLS MAC Ping packets.

Format

reset vpls-ping statistics

Parameters

None

Views

User view

Default Level

3: Management level

Usage Guidelines

The **reset vpls-ping statistics** command clears the statistics about the number of sent and received VPLS MAC Ping packets.

Example

# Clear the statistics about the number of VPLS MAC Ping packets.

```
<HUAWEI> reset vpls-ping statistics
```

10.7.98 reset vpls-trace statistics

Function

The **reset vpls-trace statistics** command clears the statistics about the number of VPLS MAC Trace packets.

Format

reset vpls-trace statistics

Parameters

None

Views

User view

Default Level

3: Management level

Usage Guidelines

The **reset vpls-trace statistics** command clears the statistics about the number of sent and received VPLS MAC Trace packets.

Example

# Clear the statistics about the number of VPLS MAC Trace packets.

```
<HUAWEI> reset vpls-trace statistics
```

10.7.99 reset traffic-statistics vsi all

Function

The **reset traffic-statistics vsi all** command clears the statistics about all VPLS PW traffic.

Format

reset traffic-statistics vsi all

Parameters

None

Views

User view

Default Level

2: Configuration level

Usage Guidelines

When the **reset traffic-statistics vsi all** command is run successfully, confirm whether to proceed with the operation. If yes, enter **Y**. If no, enter **N**.

Example

# Reset the statistics about all VPLS PW traffic in the user view.

```
<HUAWEI> reset traffic-statistics vsi all
Warning:Traffic-statistics information will be cleared! Continue? [Y/N]:Y
```

10.7.100 reset traffic-statistics vsi name

Function

The **reset traffic-statistics vsi name** command clears the statistics about the public traffic on all VPLS PWs in the specified VSI.

Format

reset traffic-statistics vsi name *vsi-name*

Parameters

Parameter	Description	Value
vsi-name	Specifies the name of the VSI in which traffic statistics are cleared.	The value is an existing VSI.

Views

User view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the VPLS configuration is complete, you can run the **display traffic-statistics vsi** command to view statistics about all PW traffic in the VSI. To view the statistics about the traffic in a specified period, you can run the **reset traffic-statistics vsi name** command to clear the previous statistics.

Precautions

The **reset traffic-statistics vsi name** command is valid only in Martini VPLS.

After you run this command, statistics about all VPLS PW traffic in the VSI are cleared.

Example

# Clear the statistics about all VPLS PW traffic in the specified VSI in the user view.

```
<HUAWEI> reset traffic-statistics vsi name newvsi
```

10.7.101 reset traffic-statistics vsi name peer

Function

The **reset traffic-statistics vsi name peer** command clears the statistics about public traffic of the PW in the specified VPLS VSI.

Format

reset traffic-statistics vsi name *vsi-name* **peer** *peer-address*

Parameters

Parameter	Description	Value
vsi-name	Specifies the name of the VSI in which traffic statistics are cleared.	The value is an existing VSI.
peer *peer-address*	Specifies the peer IP address of the PW.	-

Views

User view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the VPLS configuration is complete, you can run the **display traffic-statistics vsi peer** command to view statistics about the traffic of the PW. To view the statistics about the traffic in a specified period, you can run the **reset traffic-statistics vsi name peer** command to clear the previous statistics.

Precautions

The **reset traffic-statistics vsi name peer** command is valid only in Martini VPLS.

After you run this command, statistics about the traffic on the corresponding VPLS PW are cleared.

Example

# Clear the statistics about the traffic on the VPLS PW in the user view.

```
<HUAWEI> reset traffic-statistics vsi name newvsi peer 10.1.1.1
```

10.7.102 reset traffic-statistics vsi name peer ldp129

Function

The **reset traffic-statistics vsi name peer ldp129** command clears the statistics about the public traffic on the BGP AD VPLS PW in the specified VSI.

Format

reset traffic-statistics vsi name *vsi-name* **peer** *peer-address* **ldp129**

Parameters

Parameter	Description	Value
name *vsi-name*	Specifies the name of the VSI in which traffic statistics are cleared.	The value is an existing VSI.
peer *peer-address*	Specifies the peer IP address of the PW.	-

Views

User view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the BGP AD VPLS configuration is complete, you can run the **display traffic-statistics vsi peer ldp129** command to view statistics about the PW traffic. To view the statistics about the traffic in a specified period, you can run the **reset traffic-statistics vsi name peer ldp129** command to clear the previous statistics.

Prerequisites

The traffic statistics function has been enabled using the **traffic-statistics enable (VSI-BGPAD view)** command or the **traffic-statistics peer enable (VSI-BGPAD)** command in the VSI-BGPAD view.

Precautions

The **reset traffic-statistics vsi name peer ldp129** command is valid only in BGP AD VPLS.

After you run the **reset traffic-statistics vsi name peer ldp129** command, statistics about the traffic on the corresponding BGP AD VPLS PW are cleared.

Example

# Clear the statistics about the traffic on the specified BGP AD VPLS PW in the user view.

```
<HUAWEI> reset traffic-statistics vsi name newvsi peer 10.1.1.1 ldp129
```

10.7.103 reset traffic-statistics vsi name peer negotiation-vc-id

Function

The **reset traffic-statistics vsi name peer negotiation-vc-id** command clears the statistics about the public traffic on the Martini VPLS PW in a specified VSI.

Format

reset traffic-statistics vsi name *vsi-name* **peer** *peer-address* **negotiation-vc-id** *vc-id*

Parameters

Parameter	Description	Value
vsi-name	Specifies the name of a VSI.	The value is an existing VSI.
peer *peer-address*	Specifies the peer IP address of the PW.	-
negotiation-vc-id *vc-id*	Specifies the ID of the PW.	The value is an integer that ranges from 1 to 4294967295.

Views

User view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the Martini VPLS configuration is complete, you can run the **display traffic-statistics vsi peer negotiation-vc-id** command to view the statistics about the traffic on the PW. To view the statistics about the traffic in a specified period, you can run the **reset traffic-statistics vsi name peer negotiation-vc-id** command to clear the previous statistics.

Precautions

The **reset traffic-statistics vsi name peer negotiation-vc-id** command is valid only in Martini VPLS.

After you run the **reset traffic-statistics vsi name peer negotiation-vc-id** command, statistics about the traffic on the corresponding Martini VPLS PW are cleared.

Example

# Reset the statistics about the traffic on the Martini VPLS PW in the user view.

```
<HUAWEI> reset traffic-statistics vsi name newvsi peer 10.22.33.20 negotiation-vc-id 2
```

10.7.104 reset traffic-statistics vsi name peer remote-site

Function

The **reset traffic-statistics vsi name peer remote-site** command clears the statistics about the public traffic on the Kompella VPLS PW in the specified VSI.

Format

reset traffic-statistics vsi name *vsi-name* **peer** *peer-address* **remote-site** *site-id*

Parameters

Parameter	Description	Value
name *vsi-name*	Specifies the name of a VSI.	The value is an existing VSI.
peer *peer-address*	Specifies the peer IP address of the PW.	-
remote-site *site-id*	Specifies the remote site ID.	The value is an integer that ranges from 0 to 65534.

Views

User view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the Kompella VPLS configuration is complete, you can run the **display traffic-statistics vsi peer remote-site** command to view the statistics about the traffic on the PW. To view the statistics about the traffic in a specified period, you can run the **reset traffic-statistics vsi name peer remote-site** command to clear the previous statistics.

Prerequisites

The traffic statistics function has been enabled using the **traffic-statistics peer remote-site enable (Kompella)** command in the VSI-BGP view.

Precautions

The **reset traffic-statistics vsi name peer remote-site** command is valid only in Kompella VPLS.

After you run the **reset traffic-statistics vsi name peer remote-site** command, statistics about the traffic on the corresponding Kompella VPLS PW are cleared.

Example

# Reset the statistics about the traffic on the Kompella VPLS PW in the user view.

```
<HUAWEI> reset traffic-statistics vsi name newvsi peer 10.22.33.20 remote-site 2
```

10.7.105 route-distinguisher (VSI-BGP view)

Function

The **route-distinguisher** command configures an RD for a VSI.

Format

route-distinguisher *route-distinguisher*

Parameters

Parameter	Description	Value
route-distinguisher	Specifies the value of an RD, which identifies a VSI on a PE.	The formats of an RD are as follows: ● 16-bit AS number:32-bit user-defined number: for example, 101:3. An AS number ranges from 0 to 65535, and a user-defined number ranges from 0 to 4294967295. The AS number and user-defined number cannot be both 0. That is, a VPLS ID cannot be 0:0. ● Integral 4-byte AS number:2-byte user-defined number, for example, 65537:3. An AS number ranges from 65536 to 4294967295. A user-defined number ranges from 0 to 65535. The AS number and user-defined number cannot be both 0s. That is, a VPLS ID cannot be 0:0. ● 4-byte AS number in dotted notation:2-byte user-defined number, for example, 0.0:3 or 0.1:0. A 4-byte AS number in dotted notation is in the format of *x.y*, where *x* and *y* are integers that range from 1 to 65535 and from 0 to 65535, respectively. A user-defined number ranges from 0 to 65535. The AS number and user-

Parameter	Description	Value
		defined number cannot be both 0s. That is, a VPLS ID cannot be 0.0:0. ● 32-bit IP address:16-bit user-defined number: for example, 192.168.122.15:1. An IPv4 address ranges from 0.0.0.0 to 255.255.255.255, and a user-defined number ranges from 0 to 65535.

Views

VSI-BGP view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After you create a VSI in the Kompella VPLS and use the BGP as the PW signaling protocol, run the **route-distinguisher** command to configure the RD. Other parameters can be configured only after the RD is configured.

Prerequisites

The following operations have been performed before this command is used:

1. A VSI has been created using the **vsi** *vsi-name* [**auto**] command.
2. BGP has been configured as the PW signaling protocol using the **pwsignal bgp** command.

Precautions

On the same PE, different VSIs have different RDs. The IDs of the same VSIs on different PEs can be either the same or different.

The RD does not have a default value. After an RD is configured successfully for the VSI, it cannot be modified. If you want to modify the RD, you need to delete the VSI and re-create a VSI.

Kompella VLL and Kompella VPLS must use different RDs.

Example

# Configure an RD in the format of "16-bit ASN:32-bit user-defined number" for the VSI named **company1**.

```
<HUAWEI> system-view
[HUAWEI] vsi company1 auto
[HUAWEI-vsi-company1] pwsignal bgp
[HUAWEI-vsi-company1-bgp] route-distinguisher 101:3
```

# Configure an RD in the format of "32-bit IP address:16-bit user-defined number" for the VSI named **company2**.

```
<HUAWEI> system-view
[HUAWEI] vsi company2 auto
[HUAWEI-vsi-company2] pwsignal bgp
[HUAWEI-vsi-company2-bgp] route-distinguisher 2.2.2.2:1
```

# Configure an RD in the format of "4-byte AS number in dotted notation:2-byte user-defined number" for the VSI named **company2**.

```
<HUAWEI> system-view
[HUAWEI] vsi company2 auto
[HUAWEI-vsi-company2] pwsignal bgp
[HUAWEI-vsi-company2-bgp] route-distinguisher 22.22:22
```

10.7.106 shutdown (VSI view)

Function

The **shutdown** command disables a VSI.

The **undo shutdown** command enables a VSI.

By default, a VSI is enabled.

Format

shutdown

undo shutdown

Parameters

None

Views

VSI view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

For service management such as service debugging or service halting, you can disable a VSI temporarily, and add, cancel, or adjust VSI functions.

Pre-configuration Tasks

Before a VSI is disabled, the PW-Signal must be configured.

Precautions

The **shutdown** command mainly affects PW connections of a VSI. After the command is run, the AC is Down and the Layer 2 forwarding table is deleted.

Example

# Disable the current VSI.

```
<HUAWEI> system-view
[HUAWEI] vsi company1
[HUAWEI-vsi-company1] shutdown
```

# Enable the current VSI.

```
<HUAWEI> system-view
[HUAWEI] vsi company1
[HUAWEI-vsi-company1] undo shutdown
```

10.7.107 signaling

Function

The **signaling** command configures the signaling mode for all peers or peer groups.

The **undo signaling** command restores the default signaling mode of all peers or peer groups.

By default, after the **peer enable** is run in the L2VPN AD address family view, the BGP AD signaling is enabled for all peers or peer groups.

Format

signaling { **vpws** | **vpls** | **vpls-ad disable** }

undo signaling { **vpws** | **vpls** | **vpls-ad disable** }

Parameters

Parameter	Description	Value
vpws	Configures the signaling mode of all peers or peer groups as VPWS.	-
vpls	Configures the signaling mode of all peers or peer groups as VPLS.	-
vpls-ad disable	Disables BGP AD signaling for all peers or peer groups.	-

Views

L2VPN AD address family view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In Kompella VLL, Kompella VPLS, and BGP AD VPLS scenarios, configure the signaling mode for peers or peer groups in the L2VPN AD address family view so that peers can advertise routes to each other. The parameters used in different scenarios are described as follows:

In the Kompella VLL scenario, configure **vpws** in the **signaling** command.

In the Kompella VPLS scenario, configure **vpls** in the **signaling** command.

In the BGP AD VPLS scenario, the BGP AD signaling is enabled for all peers or peer groups in the L2VPN AD address family view by default. Therefore, you need to run the **signaling vpls-ad disable** command to disable the BGP AD signaling for all peers or peer groups in Kompella VLL and Kompella VPLS scenarios.

Prerequisites

The **peer enable** command has been run to establish peers or peer groups.

Precautions

The signaling mode configured for a peer is preferred over that configured for the peer group to which the peer belongs. The signaling mode configured for a peer group is preferred over that configured by running the **signaling** command.

When a signaling mode is not configured for a peer or its peer group, the peer and peer group use the signaling mode configured by running the **signaling** command.

Example

# Configure the signaling mode for all peers or peer groups in the L2VPN AD address family view when Kompella VPLS is enabled.

```
<HUAWEI> system-view
[HUAWEI] bgp 100
[HUAWEI-bgp] l2vpn-ad-family
[HUAWEI-bgp-l2vpn-ad] signaling vpls
[HUAWEI-bgp-l2vpn-ad] signaling vpls-ad disable
```

10.7.108 site

Function

The **site** command configures a site ID for a VSI.

The **undo site** command deletes a site ID of a VSI.

By default, no site ID is configured for the VSI.

Format

site *site-id* [**range** *site-range*] [**default-offset** { **0** | **1** }]

undo site *site-id*

Parameters

Parameter	Description	Value
site-id	Specifies the site ID of a VSI.	The value is an integer that ranges from 0 to 65534.
range *site-range*	Specifies the range of the number of sites in the VSI. If this parameter is specified, the system reserves the required labels for the VSI.	The value is an integer that ranges from 1 to 8000.
default-offset	Specifies the offset of the initial site ID.	The value is an integer. It can be 0 or 1. The default value is 0.

Views

VSI-BGP view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After you configure an RD for the VSI in the Kompella VPLS, run the **site** command to configure site connections.

Prerequisites

The following operations have been performed before this command is used:

1. A VSI has been created using the **vsi** *vsi-name* **auto** command.
2. BGP has been configured as the PW signaling protocol using the **pwsignal bgp** command.
3. The RD of the VSI has been configured using the **route-distinguisher** *route-distinguisher* command.

Precautions

The same VSI on different PEs cannot be configured with the same site ID. *site-id* of the local end must be less than the sum of *site-range* and **default-offset** of the remote end. *site-id* of the local end cannot be less than **default-offset** of the remote end.

A device allocates labels to the ranges of Kompella L2VPN instances and VPLS VSIs from the same label block. Therefore, the ranges of Kompella L2VPN instances and VPLS VSIs cannot be greater than the size of the label block. Otherwise, the system prompts that the required labels exceed the permitted maximum labels, and the labels cannot be allocated. The system fails to create a CE or fails to allocate a site ID to a VSI.

Example

# Configure the site ID of the VSI as 1 and the number of connected sites in this VSI as 100.

```
<HUAWEI> system-view
[HUAWEI] vsi company2
[HUAWEI-vsi-company2] pwsignal bgp
[HUAWEI-vsi-company2-bgp] route-distinguisher 10.1.1.1:1
[HUAWEI-vsi-company2-bgp] site 1 range 100
```

10.7.109 stream-dual-receiving

Function

The **stream-dual-receiving** command enables the secondary PW to receive and forward traffic from the peer.

The **undo stream-dual-receiving** command disables the secondary PW from receiving and forwarding traffic from the peer.

By default, the secondary PW does not receive traffic from the peer.

Format

stream-dual-receiving

undo stream-dual-receiving

Parameters

None

Views

protect-group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the network is unstable or a faulty occurs on the device, traffic may switch between the primary and secondary PW. In this case, you need to run the **stream-dual-receiving** command to enable the secondary PW to receive and forward traffic from the peer. This reduces number of packets lost during switching.

Prerequisites

The master/slave mode has been configured as the PW redundancy mode.

Configuration Impact

The secondary PW can forward data but does not forward data before traffic is switched from the primary PW to the secondary PW.

Example

# Enable the secondary PW to receive and forward traffic from the peer.

```
<HUAWEI> system-view
[HUAWEI] vsi vsi1
[HUAWEI-vsi-vsi1] pwsignal ldp
[HUAWEI-vsi-vsi1-ldp] protect-group group1
[HUAWEI-vsi-vsi1-ldp-protect-group-group1] stream-dual-receiving
```

10.7.110 tnl-policy (VSI view)

Function

The **tnl-policy** command sets a tunnel policy for a VSI.

The **undo tnl-policy** command deletes the tunnel policy of a VSI.

By default, no tunnel policy is applied to a VSI.

Format

tnl-policy *policy-name*

undo tnl-policy

Parameters

Parameter	Description	Value
policy-name	Specifies the policy name of a tunnel.	The value is a string of 1 to 39 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Views

VSI view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When configuring the VPLS to use tunnels for packet exchange, run the **tnl-policy** command.

Prerequisites

One of the following operations has been performed before this command is used:

- The **pwsignal bgp** command and the **route-distinguisher** *route-distinguisher* command have been executed for Kompella VPLS.
- The **pwsignal ldp** command and the **vsi-id** *vsi-id* command have been executed for Martini VPLS.
- The **bgp-ad** command and the **vpls-id** *vpls-id* command have been executed for BGP AD VPLS.

Precautions

After the **tnl-policy** command is executed, the configured tunnel policy determines which tunnel between PE devices is preferred to forward traffic and whether load balancing is used. When creating a tunnel policy, specify the sequence of selecting tunnels. If no tunnel policy is configured, the default tunnel policy is used. That is, only LSP tunnels are selected and no load balancing is performed.

Example

# Configure the tunnel policy name for the VSI.

```
<HUAWEI> system-view
[HUAWEI] vsi company1 static
[HUAWEI-vsi-company1] pwsignal ldp
[HUAWEI-vsi-company1-ldp] vsi-id 100
[HUAWEI-vsi-company1-ldp] quit
[HUAWEI-vsi-company1] tnl-policy tnlpolicyofcompany1
```

10.7.111 track hub-pw (VSI-LDP-PW view)

Function

The **track hub-pw** associates spoke PW status with hub PW status.

The **undo track hub-pw** deletes the association between spoke PW status and hub PW status.

By default, spoke PW status is not associated with hub PW status.

Format

track hub-pw

undo track hub-pw

Parameters

None

Views

VSI-LDP-PW view

Default Level

2. Configuration level

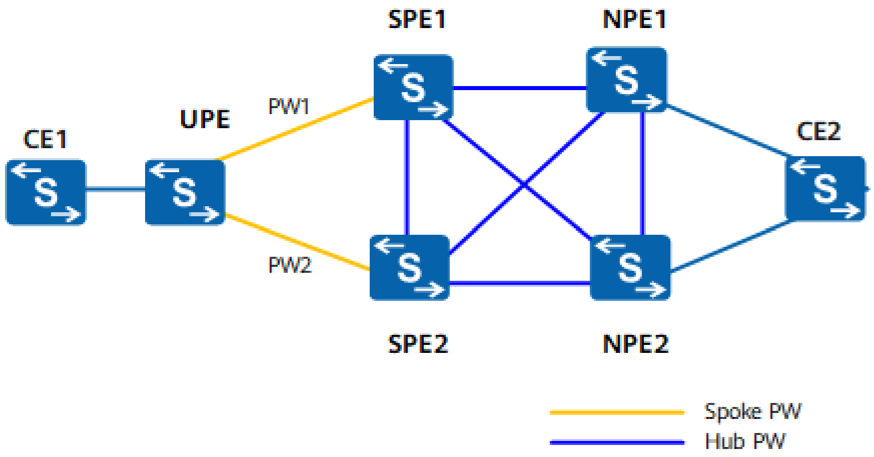
Usage Guidelines

Usage Scenario

Figure 10-3 shows a VPLS PW redundancy scenario. The UPE connects to SPE1 over PW1, a primary PW, and connects to SPE2 over PW2, a secondary PW. PW1 and PW2 work in backup mode. SPEs and NPEs are connected using hub PWs.

Under normal circumstances, if all hub PWs connected to SPE1 go Down but PW1 is Up, the upstream traffic still travels along the primary PW, PW1. As a result, traffic gets lost. To prevent traffic loss, you can run the **track hub-pw** command on SPE1 to associate spoke PW status with hub PW status. After the **track hub-pw** command is configured, SPE1 notifies the UPE of switching traffic to the secondary PW for transmission after detecting that all connected hub PWs go Down.

Figure 10-3 VPLS PW redundancy networking



Prerequisites

The **track hub-pw** command takes effect only if the following conditions are met:

- This command can only be used for a spoke PW to track the status of hub PWs. The **peer** *peer-address* [**negotiation-vc-id** *vc-id*] [**tnl-policy** *policy-name*] **upe** must have been run to create a spoke PW.
- The **peer** *peer-address* [**negotiation-vc-id** *vc-id*] **pw** *pw-name* command must have been run to display the PW view. This is because the **track hub-pw** command can only be run in the VSI-LDP-PW view.

Example

# Enable the association between spoke PW status and hub PW status.

```
<HUAWEI> system-view
[HUAWEI] vsi vsi1
[HUAWEI-vsi-vsi1] pwsignal ldp
[HUAWEI-vsi-vsi1-ldp] peer 2.2.2.2 upe
```

```
[HUAWEI-vsi-vsi1-ldp] peer 2.2.2.2 pw 1
[HUAWEI-vsi-vsi1-ldp-pw-1] track hub-pw
```

10.7.112 traffic-statistics enable (VSI-LDP view)

Function

The **traffic-statistics enable** command enables the statistics about the public traffic on all Martini VPLS PWs.

The **undo traffic-statistics enable** command disables the statistics about the public traffic on all Martini VPLS PWs.

By default, the statistics function is disabled.

Format

traffic-statistics enable

undo traffic-statistics enable

Parameters

None

Views

VSI-LDP view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the Martini VPLS network is configured, you can run the **traffic-statistics enable** command to enable statistics about the traffic on all PWs.

Prerequisites

The VSI ID has been configured using the **vsi-id** *vsi-id* command in the VSI-LDP view.

Precautions

After this command is executed and the statistics reach the upper limit, a peer can still be configured, but the traffic statistics function does not take effect on this peer. When the configuration needs to be restored after the system is restarted, configured the peer first. If the statistics exceed the upper limit after the **traffic-statistics enable** is executed, the configuration cannot be restored.

The **traffic-statistics enable** command cannot be used together with the **traffic-statistics peer enable (Martini)** command in the VSI-LDP view.

Example

# Enable the statistics on all PWs in the VSI 1.

```
<HUAWEI> system-view
[HUAWEI] vsi 1
[HUAWEI-vsi-1] pwsignal ldp
[HUAWEI-vsi-1-ldp] traffic-statistics enable
```

10.7.113 traffic-statistics enable (VSI-BGPAD view)

Function

The **traffic-statistics enable** command enables the statistics about the public traffic on all BGP AD VPLS PWs.

The **undo traffic-statistics enable** command disables the statistics about the public traffic on all BGP AD VPLS PWs.

By default, the statistics function is disabled.

Format

traffic-statistics enable

undo traffic-statistics enable

Parameters

None

Views

VSI-BGPAD view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the BGP AD VPLS network is configured, you can run the **traffic-statistics enable** command to enable statistics about the public traffic on all BGP AD VPLS PWs in the corresponding VSI.

Prerequisites

The VPLS ID has been configured using the **vpls-id** *vpls-id* command in the VSI-BGPAD view.

Precautions

The **traffic-statistics enable** command cannot be used together with the **traffic-statistics peer enable (VSI-BGPAD)** command in the VSI-BGPAD view.

Example

# Enable global traffic statistics for the VSI named **company1** in the BGP AD VPLS domain.

```
<HUAWEI> system-view
[HUAWEI] vsi company1
[HUAWEI-vsi-company1] bgp-ad
[HUAWEI-vsi-company1-bgpad] vpls-id 100:1
[HUAWEI-vsi-company1-bgpad] traffic-statistics enable
```

10.7.114 traffic-statistics peer remote-site enable (Kompella)

Function

The **traffic-statistics peer remote-site enable** command enables the statistics about the public traffic on a specified Kompella VPLS PW.

The **undo traffic-statistics peer remote-site enable** command disables the statistics about the public traffic on a specified Kompella VPLS PW.

By default, the statistics of the public traffic on the Kompella VPLS PW are disabled.

Format

traffic-statistics peer *peer-address* **remote-site** *site-id* **enable**

undo traffic-statistics peer *peer-address* **remote-site** *site-id* **enable**

Parameters

Parameter	Description	Value
peer *peer-address*	Specifies the peer IP address of the PW.	-
remote-site *site-id*	Specifies the remote site ID.	The value is an integer that ranges from 0 to 65534.

Views

VSI-BGP view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the Kompella VPLS network is configured, you can run the **traffic-statistics peer remote-site enable** command to enable statistics about the traffic on the specified PW. You can specify *peer-address* to enable the statistics about the traffic on the corresponding PW.

Prerequisites

The RD of the VSI has been configured using the **route-distinguisher** *route-distinguisher* command in the VSI-BGP view.

Precautions

After you enable the statistics about the public traffic on the specified Kompella VPLS PW, run the **display traffic-statistics vsi peer remote-site** command to view the statistics about the public traffic on the specified PW.

Example

# Enable the statistics about the public traffic on the specified Kompella VPLS PW.

```
<HUAWEI> system-view
[HUAWEI] vsi newvsi auto
[HUAWEI-vsi-newvsi] pwsignal bgp
[HUAWEI-vsi-newvsi-bgp] traffic-statistics peer 10.22.33.20 remote-site 2 enable
```

10.7.115 traffic-statistics peer enable (Martini)

Function

The **traffic-statistics peer enable** command enables the statistics about the public traffic on a specified Martini VPLS PW.

The **undo traffic-statistics peer enable** command disables the statistics about the public traffic on a specified Martini VPLS PW.

By default, the statistics function is disabled.

Format

traffic-statistics peer *peer-address* [**negotiation-vc-id** *vc-id*] **enable**

undo traffic-statistics peer *peer-address* [**negotiation-vc-id** *vc-id*] **enable**

Parameters

Parameter	Description	Value
peer *peer-address*	Specifies the peer IP address of the PW.	-
negotiation-vc-id *vc-id*	Specifies the ID of the PW.	The value is an integer that ranges from 1 to 4294967295.

Views

VSI-LDP view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the Martini VPLS network is configured, you can run the **traffic-statistics peer enable** command to enable statistics about the traffic on the specified PW. You can specify *peer-address* to enable the statistics about the traffic on the corresponding PW.

Prerequisites

The VSI ID has been configured using the **vsi-id** *vsi-id* command in the VSI-LDP view.

Precautions

After you enable the statistics about the public traffic on the specified Martini VPLS PW, run the **display traffic-statistics vsi peer negotiation-vc-id** command to view the statistics about the public traffic on the specified PW.

The **traffic-statistics peer enable** command cannot be used together with the **traffic-statistics enable (VSI-LDP view)** command in the VSI-LDP view.

Example

# Enable the statistics about the public traffic on the specified Martini VPLS PW.

```
<HUAWEI> system-view
[HUAWEI] vsi newvsi static
[HUAWEI-vsi-newvsi] pwsignal ldp
[HUAWEI-vsi-newvsi-ldp] vsi-id 1
[HUAWEI-vsi-newvsi-ldp] traffic-statistics peer 10.22.33.20 negotiation-vc-id 2 enable
```

10.7.116 traffic-statistics peer enable (VSI-BGPAD)

Function

The **traffic-statistics peer enable** command enables the statistics about the public traffic on a specified BGP AD VPLS PW.

The **undo traffic-statistics peer enable** command disables the statistics about the public traffic on a specified BGP AD VPLS PW.

By default, the statistics about the public traffic on a BGP AD VPLS PW are disabled.

Format

traffic-statistics peer *peer-address* **enable**

undo traffic-statistics peer *peer-address* **enable**

Parameters

Parameter	Description	Value
peer-address	Specifies the peer IP address of the PW.	The value is in dotted decimal notation.

Views

VSI-BGPAD view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the BGP AD VPLS network is configured, you can run the **traffic-statistics peer enable** command to enable statistics about the traffic on the specified PW. You can specify *peer-address* to enable the statistics about the traffic on the corresponding PW.

Prerequisites

The VPLS ID has been configured using the **vpls-id** *vpls-id* command in the VSI-BGPAD view.

Precautions

The **traffic-statistics peer enable** command cannot be used together with the **traffic-statistics enable (VSI-BGPAD view)** command in the VSI-BGPAD view.

After you enable the statistics about the public traffic on the specified BGP AD VPLS PW, run the **display traffic-statistics vsi peer ldp129** command to view the statistics about the public traffic on the specified PW.

Example

# Configure the BGP AD VPLS VSI named **company1**, and enable the statistics about the public traffic on the PW with the peer at 1.1.1.1.

```
<HUAWEI> system-view
[HUAWEI] vsi company1
[HUAWEI-vsi-company1] bgp-ad
[HUAWEI-vsi-company1-bgpad] vpls-id 100:1
[HUAWEI-vsi-company1-bgpad] traffic-statistics peer 1.1.1.1 enable
```

10.7.117 trace vpls mac vsi

Function

The **trace vpls mac vsi** command checks PE and P devices on the VPLS network which packets pass through from the source to the destination. This command is used to check the connectivity of Layer 2 forwarding links and locate faults on the network.

Format

trace vpls mac *mac-address* **vsi** *vsi-name* [**vlan** *vlan-id*] [**-t** *timeout* | **-f** *first-ttl* | **-m** *max-ttl* | **-exp** *exp* | **-r** *replymode*] *

Parameters

Parameter	Description	Value
mac *mac-address*	Specifies the unicast destination MAC address of the VPLS MAC trace, expressed in the format of H-H-H.	An H is a hexadecimal number of 1 to 4 bits, such as 00e0 and fc01. If you enter less than four digits, 0s are padded before the input digits. For example, if e0 is entered, 00e0 is displayed. The value cannot be a broadcast or multicast MAC address.
vsi *vsi-name*	Specifies the name of a VSI.	The value is an existing VSI.
vlan *vlan-id*	Specifies the ID of a VLAN	*vlan-id* specifies the VLAN ID, which is an integer that ranges from 1 to 4094.
-t *timeout*	Specifies the timeout period for waiting for a Reply packet in response to a VPLS MAC Trace Request packet.	The value is an integer that ranges from 0 to 65535, in milliseconds. The default value is 2000 ms.
-f *first-ttl*	Specifies the initial TTL.	The value is an integer that ranges from 1 to *max-ttl*. The default value is 1.
-m *max-ttl*	Specifies the maximum TTL.	The value is an integer that ranges from *first-ttl* to 255. The default value is 30.
-exp *exp*	Specifies the priority.	The value is an integer that ranges from 0 to 7. The default value is 0.

Parameter	Description	Value
-r *replymode*	Specifies the reply mode, that is, the Reply packet is sent from the control layer or the data layer. ● 1: indicates that the peer end does not respond to MPLS MAC Trace Request packets. ● 2: indicates that the peer end responds to MPLS MAC Trace Request packets with IPv4 or IPv6 UDP packets. ● 3: indicates that the peer end responds to MPLS MAC Trace Request packets with IPv4 or IPv6 UDP packets containing the Router Alert TLV option. ● 4: indicates that the peer end responds to MPLS MAC Trace Request packets through the control channel of the application program grade. ● 5: indicates that the peer end responds to MPLS MAC Trace Request packets with VPLS IPv4 UDP packets.	Enumerated type. At present, only modes 1, 2, and 5 are supported. When mode 2 is adopted, reply packets are sent from the control layer; when mode 5 is adopted, reply packets are sent from the data layer. The default value is 5.

Views

All views

Default Level

0: Visit level

Usage Guidelines

Usage Scenario

Using the **trace vpls mac vsi** command, you can check the connectivity of Layer 2 forwarding links on the VPLS network, analyze roles of devices, and locate faults on the network.

Prerequisites

Before running this command, ensure that a VSI is configured and the VSI is in the Up state.

Example

# On the VPLS network, trace the device with the MAC address 00e0-fc12-3456.

```
<HUAWEI> trace vpls mac 00e0-fc12-3456 vsi a2
 Traceroute to mac 00e0-fc12-3456 vsi a2, 30 hops max, press CTRL_C to break
 TTL  Num     Replier          Time     Type     Downstream              Hit
            LSR-ID          Out Interface
 --------------------------------------------------------------------------
 0    1                          Ingress  10.1.1.1/[3 ]          N
            1.1.1.9         Vlanif1025
 1    1       10.1.1.1        8 ms     Egress                         Y
            3.3.3.9
Info: Succeed in tracing the destination address 00e0-fc12-3456.
```

Table 10-140 Description of the tracert vpls multicast command output

Item	Description
TTL	Time to live.
Num	Sequence number of the packet sent at each hop.
Replier	IP address of the node sending MPLS Echo Reply packets.
Time	Time the packet is processed, that is, period from the time the Request packet is sent from the source node to the time a Reply packet is received by the source node.
Type	Type of the device that sends the Reply packet, which can be: ● Ingress: indicates an ingress node. ● Transit: indicates a transmit node. ● Egress: indicates an egress node.
Downstream	Address and label of the next hop. For example, 10.1.1.1/[3] indicates that the IP address of the next hop is 10.1.1.1 and the label allocated to the next hop is 3.
Hit	Whether the Request packet reaches the destination. ● Y: The Request packet reaches the destination. ● N: The Request packet does not reach the destination.
LSR-ID	ID of the LSR.
Out Interface	Outbound interface through which packets are forwarded.

10.7.118 tracert vpls

Function

The **tracert vpls** command detects the status of a PW or locates an abnormal node on a PW in Down state.

Format

tracert vpls [**-exp** *exp-value* | **-f** *first-ttl* | **-m** *max-ttl* | **-r** *reply-mode* | **-t** *timeout-value*] * **vsi** *vsi-name* { *local-site-id remote-site-id* | **peer** *peer-address* [**negotiate-vc-id** *vc-id*] } [**full-lsp-path**]

Parameters

Parameter	Description	Value
-exp *exp-value*	Specifies the value of the EXP field in the outer label of an MPLS Echo Request packet.	The value is an integer that ranges from 0 to 7.
-f *first-ttl*	Specifies an initial TTL.	The value is an integer that ranges from 1 to 255 and must be smaller than the value of *max-ttl*. The default value is 1.
-m *max-ttl*	Specifies a maximum TTL.	The value is an integer that ranges from 1 to 255 and must be greater than the value of *first-ttl*. The default value is 30.
-r *reply-mode*	Specifies the mode for the peer end to return MPLS Echo Reply packets. The values are as follows: ● 1: indicates no reply. ● 2: indicates a reply with an IPv4 or IPv6 UDP datagram. ● 3: indicates a reply with an IPv4 or IPv6 UDP datagram carrying a router alert label. ● 4: indicates a reply through the control channel of the application plane.	The value is an integer that ranges from 1 to 4. The default value is 2.

Parameter	Description	Value
-t *timeout-value*	Specifies the timeout period for waiting for an MPLS Echo Reply packet.	The value is an integer that ranges from 0 to 65535, in milliseconds. The default value is 5.
vsi *vsi-name*	Specifies the VPN name.	The value is an existing VSI.
local-site-id	Specifies the ID of the local CE.	The value is an integer that ranges from 0 to 65534.
remote-site-id	Specifies the ID of the remote CE.	The value is an integer that ranges from 0 to 65534.
full-lsp-path	Displays the responses from all nodes on the LSP that the MPLS Echo Request packets pass through. If this parameter is not specified, the responses from only the PW nodes along the LSP are displayed.	-
peer *peer-address*	Specifies the IP address of the peer PE.	-
negotiate-vc-id *vc-id*	Specifies the ID of the local PW.	The value is an integer that ranges from 1 to 4294967295.

Views

All views

Default Level

0: Visit level

Usage Guidelines

Usage Scenario

After the VPLS network is configured, if the VSI is in the Down state, you can run the **tracert vpls** command to locate the faulty device on the PW.

The **tracert vpls** command applies to the following networking scenarios:

- VPLS networking

  Based on VPLS types, VPLS PW tracert is classified into:

  - Martini VPLS PW tracert

Martini VPLS PW tracert only supports the label alert mode. On a Hierarchical Virtual Private LAN Service (HVPLS) network, only single-segment PWs can be detected. If a PW ID that is optional is set and specified, the PW with the specified PW ID is detected. If no PW ID is specified, the PW associated with the VSI ID is detected.

– Kompella VPLS PW tracert

  Kompella VPLS PW tracert only supports the label alert mode.

  After a faulty PW is detected using the **ping vc** command, run the **tracert vc** command to locate the fault. The **ping vc** and **tracert vc** commands can efficiently check PW connectivity and locate faults on PWs.

Prerequisites

One of the following operations has been performed before this command is used:

- Configuring Kompella VPLS
- Configuring Martini VPLS
- Configuring BGP AD VPLS

Example

# Perform the tracert operation on the VPLS link with the remote site ID being 10.

```
<HUAWEI>tracert vpls vsi test 10 10 full-lsp-path
 TTL   Replier           Time    Type      Downstream
 0                          Ingress   10.1.1.2/[4032 3 ]
 1     10.0.0.181         7 ms    Egress
```

Table 10-141 Description of the tracert vpls command output

Item	Description
TTL	TTL in an MPLS Echo Request packet. It indicates the number of hops through which an MPLS Echo Request packet passes from the source node to this node.
Replier	IP address of the node sending MPLS Echo Reply packets.
Time	Time that the packet is processed.
Type	Type of a node: ● Ingress: indicates an ingress node. ● Transit: indicates a transmit node. ● Egress: indicates an egress node.
Downstream	IP address and label of the downstream node.

# Perform the tracert operation to test the connectivity of the BGP AD VPLS PW.

```
<HUAWEI> tracert vpls vsi ad peer 10.2.2.2
 TTL   Replier           Time    Type      Downstream
 0                          Ingress   10.1.1.2/[1025 3 ]
 1     10.2.2.2          30 ms   Egress
```

Table 10-142 Description of the tracert vpls command output

Item	Description
TTL	TTL in an MPLS Echo Request packet. It indicates the number of hops through which an MPLS Echo Request packet passes from the source node to this node.
Replier	IP address of the node sending MPLS Echo Reply packets.
Time	Time the packet is processed. That is, period from the time an MPLS Echo Request packet is sent to the time an MPLS Echo Reply packet is received.
Type	Type of a node: ● Ingress: indicates an ingress node. ● Transit: indicates a transmit node. ● Egress: indicates an egress node.
Downstream	IP address and label of the downstream node. The inner label and the outer label are arranged from left to right, both are outgoing labels.

10.7.119 tracert vpls multicast

Function

The **trace vpls multicast** command starts an MFIB Trace test with a specified VSI in the VPLS domain.

Format

tracert vpls multicast vsi *vsi-name* [**-a** *source-ip-address* | **-t** *timeout* | **-r** *reply-mode* | **-exp** *exp* | **-f** *first-ttl* | **-m** *max-ttl*] * **multicast-address** *multicast-ip-address* **remote-address** *remote-ip-address*

Parameters

Parameter	Description	Value
vsi *vsi-name*	Specifies the name of the VSI on which the operation is performed.	The value is an existing VSI.
-a *source-ip-address*	Specifies the IP address of the multicast source. By default, the multicast source IP address is the IP address of the initiator. The value is in dotted decimal notation.	-

Parameter	Description	Value
-t *timeout*	Specifies the timeout period for waiting for an Echo Reply packet.	The value ranges from 0 to 65535, in milliseconds. The default value is 2000 milliseconds.
-r *reply-mode*	Specifies the reply mode. The default value is 2. ● 1: indicates that the peer end does not respond to Echo Request packets. ● 2: indicates that the peer end responds to Echo Request packets with IPv4 or IPv6 UDP packets. ● 3: indicates that the peer end responds to Echo Request packets with IPv4 or IPv6 UDP packets carrying the Router Alert option. ● 4: indicates that the peer end responds to Echo Request packets through the control channel of the application program grade. ● 5: indicates that the peer end responds to Echo Request packets with VPLS IPv4 UDP packets. **NOTE** Currently, the switch only supports mode 1, 2, and 5.	-
-exp *exp*	Specifies the priority of Echo Request packets to be sent.	The value is an integer that ranges from 0 to 7. The default value is 0.
-f *first-ttl*	Specifies the initial TTL.	The value ranges from 1 to 255.
-m *max-ttl*	Specifies the maximum TTL, which is not smaller than the initial TTL.	The value ranges from 1 to 255.
multicast-address *multicast-ip-address*	Adds a PW to the multicast group with the specified IP address.	-
remote-address *remote-ip-address*	Specifies a unicast IP address.	-

Views

All views

Default Level

0: Visit level

Usage Guidelines

Usage Scenario

You can run the **tracert vpls multicast** command on the PE, SPE, and UPE to implement the monitoring functions:

- The command is used to locate the faulty PE on the VPLS network when IGMP Snooping is enabled.
- The command is used for path discovery on the VPLS network when the IGMP Snooping is disabled.

Precautions

The **trace vpls multicast** command does not support BGP AD VPLS.

Example

# Initiate a Trace test in a specified VSI with the multicast address being 226.0.0.1 in the VPLS domain.

```
<HUAWEI> tracert vpls multicast vsi a2 multicast-address 226.0.0.1 remote
-address 10.3.3.9
traceroute to 10.3.3.9 vsi a2, 30 hops max , press CTRL+C to break
-----------------------------------------------------------------
TTL  0
 Num     : 1           Replier: UNKNOWN         Upstream: UNKNOWN
 Time    : 0           Snpg   : N               Version : 2
 Proxy   : N           Port   : N               FW Mode : IP
 Hit Flag: NotInMFIB   PW Info: Y               Alert   : N
 Policy  : Permit      CAC    : N
 Query   : 0           Report : 0               Leave   : 0
-----------------------------------------------------------------
TTL  1
 Num     : 1           Replier: 10.3.3.9        Upstream: 10.1.1.9
 Time    : 7           Snpg   : N               Version : 2
 Proxy   : N           Port   : N               FW Mode : IP
 Hit Flag: NotInMFIB   PW Info: N               Alert   : N
 Policy  : Permit      CAC    : N
 Query   : 0           Report : 0               Leave   : 0
-----------------------------------------------------------------
Info: Succeed in tracing the destination address  10.3.3.9
```

Table 10-143 Description of the tracert vpls multicast command output

Item	Description
TTL	Time to live.
Num	Sequence number of the received packet.
Replier	Address of the replier.
Upstream	Address of the PE that sends or forwards the packet.

Item	Description
Time	Time the packet is processed. That is, period from the time the Request packet is sent from the source node to the time a Reply packet is received by the source node.
Snpg	Whether IGMP Snooping is enabled.
Version	Version of IGMP Snooping enabled in the VSI.
Proxy	Whether IGMP Snooping proxy is enabled.
Port	Whether the interface learning function is enabled.
FW Mode	MAC address-based forwarding mode or IP address-based forwarding mode.
Hit Flag	Whether corresponding multicast forwarding information exists in the MFIB.
PW Info	Whether the PWs forwarding the packet can be obtained according to the ingoing label.
Alert	State in which the interface only receives IGMP messages with Router-Alert options.
Policy	Whether the packet meets the deny rule or permit rule according to the ACL.
CAC	Whether connection admission control is configured in the VSI.
Query	The number of Query packets using the current IGMP version received by the replier.
Report	The number of Report packets using the current IGMP version received by the replier.
Leave	The number of Leave packets using the current IGMP version received by the replier.

10.7.120 unknown-frame

Function

The **unknown-frame** command specifies the processing mode for received unknown frames.

By default, the system broadcasts unknown multicast frames.

Format

unknown-frame multicast { **drop** | **broadcast** }

Parameters

Parameter	Description	Value
multicast	Indicates the unknown frames are of the multicast type.	-
drop	Drops the unknown frames.	-
broadcast	Broadcasts the unknown frames.	-

Views

VSI view

Default Level

2: Configuration level

Usage Guidelines

After a VSI receives a frame, if an entry that matches the destination address cannot be found in the MAC address table, the frame is regarded as an unknown frame.

Example

# Configure the VSI to discard unknown frames.

```
<HUAWEI> system-view
[HUAWEI] vsi company1 auto
[HUAWEI-vsi-company1] unknown-frame multicast drop
```

10.7.121 unknown-unicast-suppression cir cbs (VSI view)

Function

The **unknown-unicast-suppression cir cbs** command enables unknown unicast traffic suppression in the VSI.

The **undo unknown-unicast-suppression** command disables unknown unicast traffic suppression in the VSI.

By default, unknown unicast traffic in a VSI is not suppressed.

Format

unknown-unicast-suppression cir *cir-value* **cbs** *cbs-value*

undo unknown-unicast-suppression

Parameters

Parameter	Description	Value
cir *cir-value*	Specifies the CIR, that is, the allowed rate at which traffic can pass through.	The value is an integer that ranges from 0 to 10000000, in kbit/s.
cbs *cbs-value*	Specifies the CBS, that is, the traffic that can pass instantly, or the depth of the first token bucket.	The value is an integer that ranges from 10000 to 4294967295, in bytes.

Views

VSI view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On a VPLS network, broadcast packets, multicast packets, and unknown unicast packets are transmitted in broadcast mode and copied to neighboring ACs and PWs. If large quantities of unknown unicast packets are on the VPLS network, the device has to make a lot of copies of these unknown unicast packets, which wastes bandwidth and resources, and deteriorates system performance. You can run the **unknown-unicast-suppression cir cbs** command to suppress the unknown unicast traffic in the VSI. The rate of unknown unicast traffic on the VPLS network is limited.

Prerequisites

A VSI has been created using the **vsi** *vsi-name* [**auto** | **static**] command.

Example

# Set the CIR to 100 kbit/s and the CBS to 18800 bytes for the unknown unicast traffic that can pass for VSI1.

```
<HUAWEI> system-view
[HUAWEI] vsi VSI1
[HUAWEI-vsi-VSI1] unknown-unicast-suppression cir 100 cbs 18800
```

10.7.122 upe-npe mac-withdraw enable

Function

The **upe-npe mac-withdraw enable** command enables an SPE to forward the LDP MAC Withdraw messages received from UPEs to other SPEs.

The **undo upe-npe mac-withdraw enable** command disables an SPE from forwarding the LDP MAC Withdraw messages received from UPEs to other SPEs.

By default, an SPE does not forward the LDP MAC Withdraw messages received from UPEs to other SPEs.

Format

upe-npe mac-withdraw enable

undo upe-npe mac-withdraw enable

Parameters

None

Views

VSI-LDP view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On enterprise networks, run the **upe-npe mac-withdraw enable** command to enable an SPE to forward the LDP MAC Withdraw messages received from UPEs to other SPEs.

Prerequisites

LDP has been configured as the PW signaling protocol using the **pwsignal ldp** command.

Precautions

The **upe-npe mac-withdraw enable** command is used on SPEs.

- An SPE refers to the network-side peer of the local VSI in HVPLS. You can run the **peer** *peer-address* [**negotiation-vc-id** *vc-id*] [**tnl-policy** *policy-name*] command to specify an SPE.
- A UPE refers to the user-side peer of the local VSI in HVPLS. You can run the **peer** *peer-address* [**negotiation-vc-id** *vc-id*] [**tnl-policy** *policy-name*] **upe** command to specify a UPE.
- If HVPLS is not configured on the local device, the **upe-npe mac-withdraw enable** command is not required.

Example

# Enable the SPE to forward the LDP MAC Withdraw messages received from UPEs to other SPEs.

```
<HUAWEI> system-view
[HUAWEI] vsi v1 static
```

```
[HUAWEI-vsi-v1] pwsignal ldp
[HUAWEI-vsi-v1-ldp] upe-npe mac-withdraw enable
```

10.7.123 upe-upe mac-withdraw enable

Function

The **upe-upe mac-withdraw enable** command enables an SPE to forward the LDP MAC Withdraw messages received from a UPE to other UPEs.

The **undo upe-upe mac-withdraw enable** command disables an SPE from forwarding the LDP MAC Withdraw messages received from a UPE to other UPEs.

By default, an SPE does not forward the LDP MAC Withdraw messages received from a UPE to other UPEs.

Format

upe-upe mac-withdraw enable

undo upe-upe mac-withdraw enable

Parameters

None

Views

VSI-LDP view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On enterprise networks, run the **upe-upe mac-withdraw enable** command to enable an SPE to forward the LDP MAC Withdraw messages received from a UPE to other UPEs.

Prerequisites

LDP has been configured as the PW signaling protocol using the **pwsignal ldp** command.

Precautions

The **upe-upe mac-withdraw enable** command is used on SPEs.

- An SPE refers to the network-side peer of the local VSI in HVPLS. You can run the **peer** *peer-address* [**negotiation-vc-id** *vc-id*] [**tnl-policy** *policy-name*] command to specify an SPE.
- A UPE refers to the user-side peer of the local VSI in HVPLS. You can run the **peer** *peer-address* [**negotiation-vc-id** *vc-id*] [**tnl-policy** *policy-name*] **upe** command to specify a UPE.

- If HVPLS is not configured on the local device, the **upe-upe mac-withdraw enable** command is not required.

Example

# Enable the SPE to forward the LDP MAC Withdraw messages received from a UPE to other UPEs.

```
<HUAWEI> system-view
[HUAWEI] vsi v1 static
[HUAWEI-vsi-v1] pwsignal ldp
[HUAWEI-vsi-v1-ldp] upe-upe mac-withdraw enable
```

10.7.124 vpls bgp encapsulation

Function

The **vpls bgp encapsulation** command specifies the re-encapsulation mode of a VPLS packet after the local PE receives the VPLS packet whose encapsulation type is 19.

By default, the local PE re-encapsulates the received VPLS packet with the encapsulation type as 19 in VLAN mode.

Format

vpls bgp encapsulation { **ethernet** | **vlan** }

Parameters

Parameter	Description	Value
ethernet	Indicates that the received VPLS packet whose encapsulation type is 19 is re-encapsulated in Ethernet mode.	-
vlan	Indicates that the received VPLS packet whose encapsulation type is 19 is re-encapsulated in VLAN mode.	-

Views

MPLS-L2VPN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **vpls bgp encapsulation** command is run only when a Huawei device is connected to a non-Huawei device.

As defined by the latest RFC, the encapsulation type of PW in the Kompella VPLS is 19. Huawei devices support only the Ethernet encapsulation and VLAN encapsulation. If the **vpls bgp encapsulation** command is used, upon receiving a VPLS packet with the encapsulation type as 19, the system re-encapsulates the VPLS packet according to the configuration so that Huawei devices can interwork with non-Huawei devices.

Precautions

Huawei devices can interwork with non-Huawei devices only when the **vpls bgp encapsulation** command is used together with the **ignore-mtu-match** command.

Example

# Re-encapsulate the received VPLS packet with the encapsulation type as 19 in Ethernet mode.

```
<HUAWEI> system-view
[HUAWEI] mpls lsr-id 1.1.1.1
[HUAWEI] mpls
[HUAWEI-mpls] quit
[HUAWEI] mpls l2vpn
[HUAWEI-l2vpn] vpls bgp encapsulation ethernet
```

10.7.125 vpls ignore-ac-state

Function

The **vpls ignore-ac-state** command prevents the status of a VSI from being affected by the status of the Attachment Circuit (AC).

The **undo vpls ignore-ac-state** command restores the default setting.

By default, changes in the status of the AC affect the VSI status.

Format

vpls ignore-ac-state

undo vpls ignore-ac-state

Parameters

None

Views

MPLS-L2VPN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **vpls ignore-ac-state** command is used only before a service switchover between a new network and an old one. Before the devices on an old VPLS network switch to a new network, if you want to check whether the VSI on the new VPLS network can work normally, you can run this command to configure the VSI to ignore the AC status so that the VSI maintains the Up state before the switchover.

Precautions

After the **vpls ignore-ac-state** command is executed, a VSI can keep Up if the VSI PW is Up, and the VSI status is not affected by the AC status.

The AC status refers to the status of the physical or logical interface bound to the VSI.

After the devices on the old network switch to a new network, run the **undo vpls ignore-ac-state** command to restore the default setting.

Example

# Configure a VSI to ignore the AC status.

```
<HUAWEI> system-view
[HUAWEI] mpls l2vpn
[HUAWEI-l2vpn] vpls ignore-ac-state
```

10.7.126 vpls-family

Function

The **vpls-family** command displays the BGP VPLS address family view.

The **undo vpls-family** command deletes all configurations of the BGP VPLS address family.

By default, the BGP VPLS address family is not configured in the BGP view.

Format

vpls-family

undo vpls-family

Parameters

None

Views

BGP view

Default Level

2: Configuration level

Usage Guidelines

When configuring Kompella VPLS, you need to enable BGP peers to exchange VPLS information. In this case, run the **vpls-family** command to enter the BGP VPLS address family view.

Example

# Enter the VPLS address family view.

```
<HUAWEI> system-view
[HUAWEI] bgp 100
[HUAWEI-bgp] vpls-family
[HUAWEI-bgp-af-vpls]
```

10.7.127 vpls-id

Function

The **vpls-id** command specifies the ID of a VPLS domain to which a VSI belongs.

By default, no VPLS VSI ID is specified.

Format

vpls-id *vpls-id*

Parameters

Parameter	Description	Value
vpls-id	Specifies the ID of a VPLS domain to which multiple VSIs on PEs belong.	A VPLS ID is in one of the following formats: ● 16-bit AS number: a 32-bit user-defined number, for example, 1:3. The AS number ranges from 0 to 65535. The user-defined number ranges from 0 to 4294967295. The AS number and the user-defined number cannot both be 0. That is, a VPN target cannot be 0:0. ● 32-bit IP address: a 16-bit user-defined number, for example, 192.168.122.15:1. The IP address ranges from 0.0.0.0 to 255.255.255.255. The user-defined number ranges from 0 to 65535. ● Integral 4-byte AS number:2-byte user-defined number, for example, 65537:3. An AS number ranges from 65536 to 4294967295. A user-defined number ranges from 0 to 65535. The AS number and user-defined number cannot be both 0s. That is, a VPN target cannot be 0:0. ● 4-byte AS number in dotted notation:2-byte user-defined number, for example, 0.0:3 or 0.1:0. A 4-byte AS number in

Parameter	Description	Value
		dotted notation is in the format of *x.y*, where *x* and *y* are integers that range from 1 to 65535 and from 0 to 65535, respectively. A user-defined number ranges from 0 to 65535. The AS number and user-defined number cannot be both 0s. That is, a VPN target cannot be 0.0:0.

Views

VSI-BGPAD view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

VSIs in a BGP AD VPLS domain use BGP signaling to automatically discover members in the same VPLS domain. A VPLS domain is uniquely identified by a VPLS ID. When creating BGP AD VSIs on different PEs, specify the same VPLS ID for the VSIs so that they can join the same VPLS domain. Different BGP AD VSIs on the same PE cannot be added to the same VPLS domain.

Prerequisites

Automatic VPLS member discovery and automatic PW deployment have been configured for the current VSI using the **bgp-ad** command in the VSI view, and the VSI-BGPAD view has been displayed.

Precautions

An ID is specified for the BGP AD VSI. A VPLS domain is uniquely identified by a VPLS ID. Different VPLS IDs must be configured for different VSIs on the same PE. If the VPLS ID specified using the **vpls-id** command for a VSI on a PE has been used by another VSI on that PE, the **vpls-id** command does not take effect and an error message will be displayed. The VSIs that belong to the same VPLS domain and reside on different PEs must be configured with the same VPLS ID.

After a VPLS ID is configured for a VSI, it cannot be directly changed. To change the VPLS ID, you need to delete the VSI, re-create a VSI, and reconfigure the VPLS ID.

Example

# Configure a VPLS ID in the format of 16-bit AS number:32-bit user-defined number for the VSI named **company1**.

```
<HUAWEI> system-view
[HUAWEI] vsi company1
[HUAWEI-vsi-company1] bgp-ad
[HUAWEI-vsi-company1-bgpad] vpls-id 101:3
```

# Configure a VPLS ID in the format of 32-bit IP address:16-bit user-defined number for the VSI named **company2**.

```
<HUAWEI> system-view
[HUAWEI] vsi company2
[HUAWEI-vsi-company2] bgp-ad
[HUAWEI-vsi-company2-bgpad] vpls-id 2.2.2.2:1
```

# Configure a VPLS ID in the format of 32-bit AS number:16-bit user-defined number for the VSI named **company3**.

```
<HUAWEI> system-view
[HUAWEI] vsi company3
[HUAWEI-vsi-company3] bgp-ad
[HUAWEI-vsi-company3-bgpad] vpls-id 16.20:30
```

10.7.128 vpls mac-withdraw loop-detect enable

Function

The **vpls mac-withdraw loop-detect enable** command enables MAC withdraw loop detection.

The **undo vpls mac-withdraw loop-detect enable** command disables MAC withdraw loop detection.

By default, MAC withdraw loop detection is disabled.

Format

vpls mac-withdraw loop-detect enable

undo vpls mac-withdraw loop-detect enable

Parameters

None

Views

MPLS-L2VPN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On a dual-homing VPLS or hierarchical VPLS (HVPLS) network, MAC withdraw messages can be forwarded between hub and spoke PWs and between spoke PWs. Incorrect configurations may cause a MAC withdraw message loop, which results in traffic loss. If the loop involves a large number of MAC withdraw messages, denial of service (DoS) attacks may occur. To resolve these problems, run the **vpls mac-withdraw loop-detect enable** command to enable MAC withdraw loop detection. After you enable MAC withdraw loop detection, a PE immediately discards MAC withdraw message when it detects a MAC withdraw message loop.

Prerequisites

MPLS L2VPN has been enabled using the **mpls l2vpn** command.

Example

# Enable MAC withdraw loop detection.

```
<HUAWEI> system-view
[HUAWEI] mpls l2vpn
[HUAWEI-l2vpn] vpls mac-withdraw loop-detect enable
```

10.7.129 vpn-target (VSI-BGP view)

Function

The **vpn-target** command associates a VSI with one or more VPN targets.

The **undo vpn-target** command deletes a VPN target associated with a VSI.

By default, a VSI is not associated with any VPN target.

Format

vpn-target *vpn-target* &<1-16> [**both** | **export-extcommunity** | **import-extcommunity**]

undo vpn-target { **all** | *vpn-target* &<1-16> } [**both** | **export-extcommunity** | **import-extcommunity**]

Parameters

Parameter	Description	Value
vpn-target	Specifies a VPN target that is added to a VSI.	You can choose one of the following formats to express a VPN target: ● 16-bit AS number: a 32-bit user-defined number, for example, 1:3. The AS number ranges from 0 to 65535. The user-defined number ranges from 0 to 4294967295. The AS number and the user-defined number cannot both be 0. That is, a VPN target cannot be 0:0. ● 32-bit IP address: a 16-bit user-defined number, for example, 192.168.122.15:1. The IP address ranges from 0.0.0.0 to 255.255.255.255. The user-defined number ranges from 0 to 65535. ● Integral 4-byte AS number:2-byte user-defined number, for example, 65537:3. An AS number ranges from 65536 to 4294967295. A user-defined number ranges from 0 to 65535. The AS number and user-defined number cannot be both 0s. That is, a VPN target cannot be 0:0. ● 4-byte AS number in dotted notation:2-byte user-defined number, for example, 0.0:3 or 0.1:0. A 4-

Parameter	Description	Value
		byte AS number in dotted notation is in the format of *x.y*, where *x* and *y* are integers that range from 0 to 65535. A user-defined number ranges from 0 to 65535. The AS number and user-defined number cannot be both 0s. That is, a VPN target cannot be 0.0:0.
export-extcommunity	Indicates the extended community attributes carried in the data to be sent.	-
import-extcommunity	Indicates the extended community attributes carried in the received data.	-
both	Indicates the import routing information from the extended community of the destination VPN and the export routing information sent to the extended community of the destination VPN.	-
all	Deletes all attributes of VPN targets.	-

Views

VSI-BGP view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When sending routing information to other PE devices according to the VSI, a PE device adds export VPN targets to the routing information. When receiving routing information from other PE devices, the PE determines whether to add the data to the VSI according to import VPN targets. Therefore, VPN targets can be used to control the route advertisement between nodes.

Prerequisites

The RD of the VSI has been configured using the **route-distinguisher** *route-distinguisher* command.

Example

# Associate the current VSI with a VPN target.

```
<HUAWEI> system-view
[HUAWEI] vsi company2
[HUAWEI-vsi-company2] pwsignal bgp
[HUAWEI-vsi-company2-bgp] route-distinguisher 2.2.2.2:1
[HUAWEI-vsi-company2-bgp] vpn-target 3:3 export-extcommunity
[HUAWEI-vsi-company2-bgp] vpn-target 4:4 import-extcommunity
[HUAWEI-vsi-company2-bgp] vpn-target 5:5 both
```

10.7.130 vpn-target (VSI-BGPAD view)

Function

The **vpn-target** command associates a VSI in a BGP AD VPLS domain with one or more VPN targets.

The **undo vpn-target** command removes the VPN targets associated with the VSI.

By default, a VSI is not associated with any VPN target. The association must be configured when a VSI is created.

Format

vpn-target *vpn-target* &<1-16> [**both** | **export-extcommunity** | **import-extcommunity**]

undo vpn-target { **all** | *vpn-target* &<1-16> } [**both** | **export-extcommunity** | **import-extcommunity**]

Parameters

Parameter	Description	Value
vpn-target	Associates a VPN target with a VSI.	The format of a VPN target can be one of the following: ● 16-bit AS number:32-bit user-defined number. For example, 1:3. The AS number ranges from 0 to 65535, and the user-defined number ranges from 0 to 4294967295. The AS number and user-defined number cannot be both 0. This means that the VPN target value cannot be 0:0. ● 32-bit IP address:16-bit user-defined number. For example, 192.168.122.15:1. The IP address ranges from 0.0.0.0 to 255.255.255.255, and the user-defined number ranges from 0 to 65535. ● Integral 4-byte AS number:2-byte user-defined number, for example, 65537:3. An AS number ranges from 65536 to 4294967295. A user-defined number ranges from 0 to 65535. The AS number and user-defined number cannot be both 0s. That is, a VPN target cannot be 0:0. ● 4-byte AS number in dotted notation: 2-byte user-defined number, for example, 0.0:3 or 0.1:0. A 4-byte AS number in dotted notation is in the format of *x.y*, where *x* and *y* are integers that range from 0 to 65535. A user-defined number ranges from 0 to 65535. The AS number and user-defined number cannot be both 0s. That is, a VPN target cannot be 0.0:0.
both	Specifies the extended community attributes of the received and sent routing information.	-

Parameter	Description	Value
export-extcommunity	Specifies the extended community attributes carried in routing information to be sent.	-
import-extcommunity	Receives routing information carrying specified extended community attributes.	-
all	Deletes all VPN targets.	-

Views

VSI-BGPAD view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

VPN targets can be used in a BGP AD VPLS domain to control the route advertisement and communication between nodes. When a PE advertises routing information to other PEs of different VSIs, it adds export VPN targets to the routing information. When the PE receives routing information from other PEs, it uses import VPN targets to determine whether to import the routing information to the VSIs on it.

Prerequisites

The VPLS ID has been configured using the **vpls-id** *vpls-id* command in the VSI-BGPAD view.

Precautions

A PW can be set up between two VSIs in a BGP AD VPLS domain only when the import VPN target associated with a VSI is the same as the export VPN target associated with the other VSI.

After the **vpn-target** command is run, the PE only advertises the routing information that contains the export VPN targets and imports the routing information that contains the import VPN targets. Two PEs are allowed to communicate with each other only when the VPN targets carried in their exchanged routing information match.

Example

# Configure a VSI named **company2**, and associate the VSI with import VPN targets 4:4 and 5:5 and with export VPN targets 3:3 and 5:5.

```
<HUAWEI> system-view
[HUAWEI] vsi company2
[HUAWEI-vsi-company2] bgp-ad
[HUAWEI-vsi-company2-bgpad] vpls-id 100:1
[HUAWEI-vsi-company2-bgpad] vpn-target 3:3 export-extcommunity
[HUAWEI-vsi-company2-bgpad] vpn-target 4:4 import-extcommunity
[HUAWEI-vsi-company2-bgpad] vpn-target 5:5 both
```

10.7.131 vsi

Function

The **vsi** command creates a VSI or displays the VSI view.

The **undo vsi** command deletes a VSI.

By default, no VSI is created.

Format

vsi *vsi-name* [**auto** | **static**]

undo vsi *vsi-name*

Parameters

Parameter	Description	Value
vsi-name	Specifies the name of a VSI.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string. Names of the VSIs on one device cannot be identical.
auto	Indicates that the automatic member discovery mode is used in the VSI.	-
static	Indicates that the static member discovery mode is used in the VSI.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To configure VPLS, you need to create VSIs first. Each device in a VPLS domain needs to be configured with a VSI that belongs to the domain.

On a Martini or Kompella VPLS network, the VPLS member discovery mode for a created VSI can be set to static or auto. You can set the signaling mode using the **pwsignal** { **bgp** | **ldp** } command after a VSI is created. Use the LDP signaling mode if the static member discovery mode is used. Use the BGP signaling mode if the automatic member discovery mode is used. The member discovery mode cannot be modified. To modify the member discovery mode of the VSI, you need to delete the VSI. Then, re-create a VSI and specify the member discovery mode.

When creating a BGP AD VSI, do not specify a member discovery mode of the VSI. A VSI without a specified member discovery mode can be configured to use the LDP, BGP, or BGP AD signaling mode.

If you have specified a member discovery mode for a VSI, specify the same member discovery mode in the **vsi** command when you want to re-enter the VSI view. If the member discovery mode in the **vsi** command is different from the member discovery mode specified for the VSI, you cannot enter the VSI view.

Prerequisites

The MPLS L2VPN function has been enabled on the device.

Precautions

Note the following points when configuring VSIs in a VPLS domain:

- VSIs on different PEs can have different names.
- A VSI on a PE must be configured with a unique VSI ID or VPLS ID.
- Multiple peers can be specified for a VSI on a PE.

If the specified VSI exists, you can use the **vsi** command to enter the VSI view.

After VPLS configurations are complete, VPLS packets are forwarded based on VSIs. Exercise caution when using the **undo vsi** command because VPLS traffic will be interrupted.

Example

# Create a Martini VPLS VSI named **company1**.

```
<HUAWEI> system-view
[HUAWEI] mpls lsr-id 10.1.1.1
[HUAWEI] mpls
[HUAWEI-mpls] quit
[HUAWEI] mpls l2vpn
[HUAWEI-l2vpn] quit
[HUAWEI] vsi company1 static
[HUAWEI-vsi-company1] pwsignal ldp
```

# Create a Kompella VPLS VSI named **company2**.

```
<HUAWEI> system-view
[HUAWEI] mpls lsr-id 10.1.1.1
[HUAWEI] mpls
[HUAWEI-mpls] quit
[HUAWEI] mpls l2vpn
[HUAWEI-l2vpn] quit
[HUAWEI] vsi company2 auto
[HUAWEI-vsi-company2] pwsignal bgp
```

# Create a BGP AD VPLS VSI named **company3**.

```
<HUAWEI> system-view
[HUAWEI] mpls lsr-id 10.1.1.1
[HUAWEI] mpls
[HUAWEI-mpls] quit
[HUAWEI] mpls l2vpn
[HUAWEI-l2vpn] quit
[HUAWEI] vsi company3
```

# Create a Martini VPLS VSI named **company4**, and do not specify the VSI member discovery mode.

```
<HUAWEI> system-view
[HUAWEI] mpls lsr-id 10.1.1.1
[HUAWEI] mpls
[HUAWEI-mpls] quit
[HUAWEI] mpls l2vpn
[HUAWEI-l2vpn] quit
[HUAWEI] vsi company4
[HUAWEI-vsi-company4] pwsignal ldp
```

# Create a Martini Kompella VPLS VSI named **company5**, and do not specify the VSI member discovery mode.

```
<HUAWEI> system-view
[HUAWEI] mpls lsr-id 10.1.1.1
[HUAWEI] mpls
[HUAWEI-mpls] quit
[HUAWEI] mpls l2vpn
[HUAWEI-l2vpn] quit
[HUAWEI] vsi company5
[HUAWEI-vsi-company5] pwsignal bgp
```

10.7.132 vsi-id

Function

The **vsi-id** command sets an ID for a VSI.

By default, no VSI ID is set.

Format

vsi-id *vsi-id*

Parameters

Parameter	Description	Value
vsi-id	Specifies the unique ID of a VSI.	The value is an integer that ranges from 1 to 4294967295.

Views

VSI-LDP view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After you create a VSI in the Martini VPLS and use the LDP as the PW signaling protocol, run the **vsi-id** command to configure the VSI ID. Other parameters can be configured only after the VSI ID is configured.

Precautions

Different VSIs have different IDs.

VSI IDs on all devices in the same VPLS domain must be the same.

The VSI ID cannot be changed after being set. If you want to change the VSI ID, you need to delete the VSI and re-create a VSI.

Example

# Set the ID of the current VSI to 1.

```
<HUAWEI> system-view
[HUAWEI] vsi company1 static
[HUAWEI-vsi-company1] pwsignal ldp
[HUAWEI-vsi-company1-ldp] vsi-id 1
```

10.8 L2VPN Access to L3VPN Configuration Commands

10.8.1 Command Support

Only the following switch models support L2VPN access to L3VPN:

S5731-S, S5731-H, S5731S-H, S5732-H, S6730-S, S6730S-H, and S6730-H

10.8.2 display virtual-ethernet ve-group

Function

The **display virtual-ethernet ve-group** command displays the binding relationship between Virtual Ethernet (VE) interfaces and a VE group.

Format

display virtual-ethernet ve-group [*ve-group-id*]

Parameters

Parameter	Description	Value
ve-group-id	Specifies the ID of a VE group.	The value is an integer ranging from 1 to 8.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

If a device is configured with many VE groups, you can use this command to view the relationship between VE interfaces and VE groups.

Example

# Display the binding relationship between all VE interfaces and VE groups on a switch.

```
<HUAWEI> display virtual-ethernet ve-group
 Ve-groupID    TerminateVE                 AccessVE
 1             Virtual-Ethernet0/0/1(L2)   Virtual-Ethernet0/0/2(L3)
Total 1, 1 printed
```

Table 10-144 Description of the **display virtual-ethernet ve-group** command output

Item	Description
Ve-groupID	ID of a VE group.
TerminateVE	L2VE interface terminating an L2VPN.
AccessVE	L3VE interface accessing an L3VPN.
Total 1, 1 printed	Total number of VE groups.

10.8.3 display mpls l2vpn track route

Function

The **display mpls l2vpn track route** command displays information about the PWs that track VPNv4 route status.

Format

display mpls l2vpn track route [*ipv4-address* { *mask* | *mask-length* } **vpn-instance** *vpn-instance-name*]

Parameters

Parameter	Description	Value
ipv4-address	Specifies the destination IP address of a VPNv4 route.	The value is in dotted decimal notation.
mask	Specifies a mask in dotted decimal notation.	The value is in dotted decimal notation.
mask-length	Specifies the mask length.	The value is an integer ranging from 0 to 32.
vpn-instance *vpn-instance-name*	Specifies the VPN instance name.	The value must be an existing VPN instance name.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

In an L2VPN access to L3VPN scenario, if all L3VPN-side links of an NPE become unavailable, a black-hole route comes into existence. The user-side UPE cannot detect the link failures and still sends traffic to the NPE. As a result, traffic loss occurs. To prevent traffic loss, run the **mpls l2vpn track route** command to configure the PW to track VPNv4 route status. Then, after the NPE detects that all its L3VPN-side links become unavailable, the NPE instructs the UPE to switch traffic to the secondary PW.

To check information about the PWs that track VPNv4 route status, run the **display mpls l2vpn track route** command.

Example

# Display information about all PWs that track VPNv4 route status.

```
<HUAWEI> display mpls l2vpn track route
Total route number:1      reachable:0      unreachable:1
--------------------------------------------------------------

VPN instance name : vpna
Route             : 10.1.1.1/32
Route status      : reachable
PW number         : 1
VC ID      VC Type                 Peer IP             VC State
--------------------------------------------------------------
101        VLAN                    10.1.1.2            up
```

Table 10-145 Description of the **display mpls l2vpn track route** command output

Item	Description
Total route number	Total number of VPNv4 routes tracked by a PW.
reachable	Number of reachable VPNv4 routes.
unreachable	Number of unreachable VPNv4 routes.
VPN instance name	VPN instance name.
Route	Destination IP address of a VPNv4 route.
Route status	VPNv4 route status: ● reachable ● unreachable
VC ID	ID of a VC, which uniquely identifies the VC.
VC Type	Encapsulation type of the VC: ● VLAN ● Ethernet
Peer IP	Peer IP address.
VC State	VC status: ● up: The VC is established. ● Down: The VC is not established.

10.8.4 mpls l2vpn track route

Function

The **mpls l2vpn track route** command configures a PW to track VPNv4 route status.

The **undo mpls l2vpn track route** command configures a PW not to track VPNv4 route status.

By default, a PW does not track VPNv4 route status.

Format

mpls l2vpn track route *ipv4-address* { *mask* | *mask-length* } **vpn-instance** *vpn-instance-name*

undo mpls l2vpn track route

Parameters

Parameter	Description	Value
ipv4-address	Specifies the destination IP address of a VPNv4 route.	The value is in dotted decimal notation.
mask	Specifies a mask in dotted decimal notation.	The value is in dotted decimal notation.
mask-length	Specifies the mask length.	The value is an integer ranging from 0 to 32.
vpn-instance *vpn-instance-name*	Specifies the name of a VPN instance.	The value must be an existing VPN instance name.

Views

VE sub-interface view

Default Level

2: Configuration level

Usage Guidelines

In an L2VPN access to L3VPN scenario, if all L3VPN-side links of an NPE become unavailable, a black-hole route comes into existence. The user-side UPE cannot detect the link failures and still sends traffic to the NPE. As a result, traffic loss occurs. To prevent traffic loss, run the **mpls l2vpn track route** command to configure the PW to track VPNv4 route status. Then, after the NPE detects that all its L3VPN-side links become unavailable, the NPE instructs the UPE to switch traffic to the secondary PW.

Example

# Configure a PW to track VPNv4 route status.

```
<HUAWEI> system-view
[HUAWEI] interface virtual-ethernet 0/0/1
[HUAWEI-Virtual-Ethernet0/0/1] ve-group 1 l2-terminate
[HUAWEI-Virtual-Ethernet0/0/1] quit
[HUAWEI] interface virtual-ethernet 0/0/1.1
[HUAWEI-Virtual-Ethernet0/0/1.1] mpls l2vc 10.1.1.2 101
[HUAWEI-Virtual-Ethernet0/0/1.1] mpls l2vpn track route 10.1.1.1 32 vpn-instance vpna
```

10.8.5 statistic enable (VE interface view)

Function

The **statistic enable** command enables the traffic statistics collection function on a Virtual Ethernet (VE) interface.

The **undo statistic enable** command disables the traffic statistics collection function on a VE interface.

By default, the traffic statistics collection function is disabled on a VE interface.

Format

statistic enable { **both** | **inbound** | **outbound** }

undo statistic enable { **both** | **inbound** | **outbound** }

Parameters

Parameter	Description	Value
both	Enables the traffic statistics collection function for incoming and outgoing traffic.	-
inbound	Enables the traffic statistics collection function for incoming traffic.	-
outbound	Enables the traffic statistics collection function for outgoing traffic.	-

Views

VE interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can enable the traffic statistics collection function on the VE interfaces if you want to check the network status or troubleshoot network faults.

Prerequisites

The VE interfaces have been bound to VE groups by using the **ve-group** command. Otherwise, the **statistic enable** command does not take effect.

Precautions

- After you run the **undo statistic enable** command on a VE interface, the switch stops collecting traffic statistics on the VE interface and the collected traffic statistics will be deleted.
- The switch uses ACL resources when collecting traffic statistics. If the traffic statistics collection function is enabled on too many VE interfaces, other services may fail to obtain ACL resources.

- The switch can only collect statistics of unicast, multicast, and broadcast packets on VE interfaces.
- On the VE interface enabled with the traffic statistics collection function, the packets such as ping packets sent from the switch cannot be counted.

Example

# Enable the traffic statistics collection function for incoming and outgoing traffic on the VE interface.

```
<HUAWEI> system-view
[HUAWEI] interface virtual-ethernet 0/0/1
[HUAWEI-Virtual-Ethernet0/0/1] ve-group 1 l2-terminate
[HUAWEI-Virtual-Ethernet0/0/1] statistic enable both
```

10.8.6 ve-group

Function

The **ve-group** command configures a VE interface to work in multi-service access mode and binds the VE interface to a specified VE group.

The **undo ve-group** command restores a VE interface to common mode.

By default, a VE interface works in common mode.

Format

ve-group *ve-group-id* { **l2-terminate** | **l3-access** }

undo ve-group

Parameters

Parameter	Description	Value
ve-group-id	Specifies the ID of a VE group.	The value is an integer ranging from 1 to 8.
l2-terminate	Sets the VE interface to an L2VE interface that terminates the L2VPN.	-
l3-access	Sets the VE interface to an L3VE interface that accesses the L3VPN.	-

Views

VE interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In L2VPN access to L3VPN scenarios:

- To change a VE interface to an L2VE interface, run the **ve-group** *ve-group-id* **l2-terminate** command.
- To change a VE interface to an L3VE interface, run the **ve-group** *ve-group-id* **l3-access** command.

Precautions

- A VE group has only one L2VE interface and one L3VE interface.
- The two VE interfaces in a VE group must be on the same chassis.
- Multiple sub-interfaces can be created for each L2VE or L3VE interface to provide access for different VLAN services.

Example

# Set Virtual-Ethernet 0/0/1 to an L2VE interface.

```
<HUAWEI> system-view
[HUAWEI] interface virtual-ethernet 0/0/1
[HUAWEI-Virtual-Ethernet0/0/1] ve-group 1 l2-terminate
```

# Set Virtual-Ethernet 0/0/2 to an L3VE interface.

```
<HUAWEI> system-view
[HUAWEI] interface virtual-ethernet 0/0/2
[HUAWEI-Virtual-Ethernet0/0/2] ve-group 1 l3-access
```