12 VPN Commands

About This Chapter

12.1 L2TP Configuration Commands
12.2 L2TPv3 Configuration Commands
12.3 GRE Configuration Commands
12.4 SVPN Configuration Commands
12.5 DSVPN Configuration Commands
12.6 IPSec Configuration Commands
12.7 A2A VPN Configuration Commands
12.8 SSL VPN Configuration Commands
12.9 BGP/MPLS IP VPN Configuration Commands
12.10 EVPN Configuration Commands
12.11 VLL Configuration Commands
12.12 PWE3 Configuration Commands
12.13 VPLS Configuration Commands
12.14 VXLAN Configuration Commands

12.1 L2TP Configuration Commands

NOTE

AR161EW-M1, AR169EGW-L, AR161EW and AR169EW do not support LAC and LNS, but support L2TP Client.

 Copyright © Huawei Technologies Co., Ltd.

12.1.1 allow l2tp

Function

The **allow l2tp** command specifies a virtual interface template and the name of an LAC tunnel that are used by the LNS to accept an L2TP connection request.

The **undo allow** command rejects an L2TP connection request.

By default, an L2TP connection request is rejected.

Format

allow l2tp virtual-template *virtual-template-number* [**remote** *remote-name* [**vpn-instance** *vpn-instance-name*]]

undo allow

Parameters

Parameter	Description	Value
virtual-template *virtual-template-number*	Specifies the number of a virtual interface template used when the LNS accepts a call connection request.	The value is an integer that ranges from 0 to 1023.
remote *remote-name*	Specifies the name of a remote tunnel end. You can use the **tunnel name** command to configure the name on an LAC in the L2TP group view. When the L2TP group number is not 1, you must specify *remote-name*.	The value is a string of 1 to 30 case-sensitive characters.
vpn-instance *vpn-instance-name*	Specifies the VPN instance to which the IP address of the L2TP connection belongs. The LNS searches for the corresponding L2TP group based on the VPN instance name and *remote-name*. Route information to LACs exists in the routing table of the VPN instance.	The value is a string of 1 to 31 case-sensitive characters.

Views

L2TP group view

Default Level

2: Configuration level

Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

Usage Scenario

The **allow l2tp** command is used on the LNS side to establish an L2TP connection between the LAC and LNS. After receiving an L2TP connection request, the LNS accepts the L2TP connection request and initiates a PPP negotiation on the specified virtual tunnel template (which also used as an L2TP tunnel interface) if the tunnel name contained in the connection request is consistent with the name specified by the **allow l2tp** command.

When L2TP group 1 is used and the tunnel name is not specified, the default L2TP group receives L2TP connection requests sent by any remote end and the tunnel name on the LAC side is not checked. This method can be used when the name of a remote tunnel end is unknown to the LNS.

Precautions

When specify the name of the remote tunnel end, ensure that the name is consistent with the tunnel name configured on the LAC side.

Example

Configure the device to receive L2TP tunnel connection requests sent by the LAC device named **lac**. Create a virtual interface template **virtual-template 1**.

```
<Huawei> system-view
[Huawei] l2tp-group 2
[Huawei-l2tp2] allow l2tp virtual-template 1 remote lac
```

Set L2TP group 1 as the default L2TP group, configure the device to receive L2TP tunnel connection requests sent by any remote end, and create a virtual interface template **virtual-template 1**.

```
<Huawei> system-view
[Huawei] l2tp-group 1
[Huawei-l2tp1] allow l2tp virtual-template 1
```

Configure the device to receive L2TP tunnel connection requests sent by the LAC device named **lac** that belongs to **vpn1**. Create a virtual interface template **virtual-template 1**.

```
<Huawei> system-view
[Huawei] l2tp-group 2
[Huawei-l2tp2] allow l2tp virtual-template 1 remote lac vpn-instance vpn1
```

Related Topics

12.1.9 l2tp-group

12.1.19 tunnel name

12.1.2 display l2tp session

Function

The **display l2tp session** command displays information about L2TP sessions established on the current device.

 Copyright © Huawei Technologies Co., Ltd.

Format

display l2tp session [**destination-ip** *d-ip-address* | **session-item** *session-id* | **source-ip** *s-ip-address*]

Parameters

Parameter	Description	Value
destination-ip *d-ip-address*	Specifies the IP address of the L2TP tunnel remote end used to view session information.	The value is in dotted decimal notation.
session-item *session-id*	Specifies IDs of local sessions, and displays session used to view tunnel information.	The value is an integer and the value range depends on device types. • AR100&AR120&AR150&AR160&AR200 series: 1 to 16 • AR1200 series, AR2201-48FE, AR2202-48FE, AR2204E, AR2204E-D, AR2204: 1 to 128 • AR2220, AR2220E, AR2240C: 1 to 512 • AR2204XE, AR2204XE-DC, AR2240, AR3200, and AR3600 (using SRUX5) series: 1 to 1024
source-ip *s-ip-address*	Specifies the IP address of the L2TP tunnel local end and displays session information.	The value is in dotted decimal notation.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

After L2TP sessions are established, you can use this command to view the number of L2TP sessions that are established on the current device, and the session IDs.

You can view statistics of L2TP sessions by the IP address of the L2TP tunnel remote end or local end.

 Copyright © Huawei Technologies Co., Ltd.

If local session IDs are specified, you can view information about L2TP sessions and the tunnel.

Prerequisites

L2TP sessions have been established.

Example

Display information about L2TP sessions.

```
<Huawei> display l2tp session

 Total session : 1
 LocalSID  RemoteSID  LocalTID  Interface          LclTAddr       RmtTAddr       LclSAddr       RmtSAddr
 1         1          4         Virtual-Template0:1 3.3.40.132     3.3.40.140     5.5.5.1        5.5.5.201
```

Table 12-1 Description of the display l2tp session command output

Item	Description
Total session	Total number of sessions established on the local end.
LocalSID	Local session ID.
RemoteSID	Remote session ID.
LocalTID	Local tunnel ID.
Interface	Name of the virtual interface for the local L2TP session. **NOTE** This parameter is supported in V200R010C10 and later versions.
LclTAddr	Local tunnel IP address in the L2TP session. **NOTE** This parameter is supported in V200R010C10 and later versions.
RmtTAddr	Remote tunnel IP address in the L2TP session. **NOTE** This parameter is supported in V200R010C10 and later versions.
LclSAddr	Local session IP address in the L2TP session. **NOTE** This parameter is supported in V200R010C10 and later versions.
RmtSAddr	Remote session IP address in the L2TP session. **NOTE** This parameter is supported in V200R010C10 and later versions.

Display information about L2TP sessions of the tunnel with the destination IP address as 3.3.40.140.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> display l2tp session destination-ip 3.3.40.140

 Total session : 1
 LocalSID  RemoteSID  LocalTID  Interface           LclTAddr        RmtTAddr        LclSAddr        RmtSAddr
 1         1          4         Virtual-Template0:1 3.3.40.132      3.3.40.140      5.5.5.1         5.5.5.201
```

Display information about L2TP sessions of the tunnel with the local session ID as 1.

```
<Huawei> display l2tp session session-item 1
  -------------------------------------------------------------
    Call id             :1
    Remote Call id      :1
    Call State          :Up
    Remote tunnel name  :lac
    Remote Address      :10.1.2.3    port : 1701
    Local tunnel name   :lns
    Local Address       :10.1.2.4    port : 1701
    Call serial number  :1
    Session username    : NULL
    Sequencing is       :off
    Source Interface    :Routing
  -------------------------------------------------------------
```

Table 12-2 Description of the **display l2tp session** command output

Item	Description
Call id	Local session ID.
Remote Call id	Remote session ID.
Call State	Call status. The value is **Up** after an L2TP session is established.
Remote tunnel name	Remote tunnel name.
Remote Address	Remote tunnel address.
Local tunnel name	Local tunnel name.
Local Address	Local IP address.
Call serial number	Call serial number.
Session username	Session username: ● Client: The user name is displayed. ● Sever: **NULL**is displayed.
Sequencing is	Sequencing function. The default value is **off**.
Source Interface	Outbound interface of the tunnel. ● When multiple equal cost routes exist between the local and remote ends, the name of the access-side interface is displayed. ● When no equal cost routes exist between the local and remote ends, **Routing** is displayed.

Copyright © Huawei Technologies Co., Ltd.

Related Topics

12.1.3 display l2tp tunnel

12.1.3 display l2tp tunnel

Function

The **display l2tp tunnel** command displays information about the current L2TP tunnel.

Format

display l2tp tunnel [**tunnel-item** *tunnel-id* | **tunnel-name** *tunnel-name*]

Parameters

Parameter	Description	Value
tunnel-item *tunnel-id*	Specifies the tunnel ID used to view tunnel information.	The value is an integer and the value range depends on device types. • AR100&AR120&AR150&AR160&AR200 series: 1 to 16 • AR1200 series, AR2201-48FE, AR2202-48FE, AR2204E, AR2204E-D, AR2204: 1 to 128 • AR2220, AR2220E, AR2240C: 1 to 512 • AR2204XE, AR2204XE-DC, AR2240, AR3200, and AR3600 (using SRUX5) series: 1 to 1024
tunnel-name *tunnel-name*	Specifies the name of the tunnel remote end used to view tunnel information.	The value is a string of 1 to 30 characters.

Views

All views

Default Level

1: Monitoring level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

Usage Scenario

After L2TP tunnels are established, you can use this command to view the number of L2TP tunnels that are established on the current device, the tunnel IDs, and tunnel addresses.

You can view detailed information about a specified L2TP tunnel by local tunnel ID or remote tunnel name.

Prerequisites

L2TP sessions have been established.

Example

Display information about the current L2TP tunnel.

```
<Huawei> display l2tp tunnel

 Total tunnel : 1
 LocalTID RemoteTID RemoteAddress    Port   Sessions RemoteName
 1        1         10.1.2.4         1701   1        lns
```

NOTE

If a large number of sessions are carried over a tunnel, the sessions may still exist when you tear down the tunnel.

Table 12-3 Description of the display l2tp tunnel command output

Item	Description
Total tunnel	Total number of tunnels established on the local end.
LocalTID	Local tunnel ID.
RemoteTID	Remote tunnel ID.
RemoteAddress	Remote tunnel IP address.
Port	Remote port number. The value is 1701 in general.
Sessions	Number of sessions that an L2TP tunnel carries.
Remote Name	Name of the tunnel remote end.

Display detailed information about L2TP tunnel **1**.

```
<Huawei> display l2tp tunnel tunnel-item 1
 ------------------------------------------------------------
   Tunnel id           :1
   Remote Tunnel id    :1
   Tunnel State        :Up
   Remote tunnel name  :lns
   Remote Address      :10.1.2.4    port : 1701
   ReCall Address      :10.1.2.4
   Local tunnel name   :lac
   Local Address       :10.1.2.3    port : 1701
   active sessions     :1
```

 Copyright © Huawei Technologies Co., Ltd.

```
  Session Limit       :4294967295
  Control Ns          :170
  Control Nr          :169
  Retransmission      :5
  Timeout             :2
  Hello Interval      :60
  Local RWS           :4
  Remote RWS          :128
  OuterDscp           :0xff
  Source Interface    :Routing
-------------------------------------------------------------
```

Table 12-4 Description of the **display l2tp tunnel** command output

Item	Description
Tunnel id	Local tunnel ID.
Remote Tunnel id	Remote tunnel ID.
Tunnel State	Tunnel status. The tunnel status is **Up** after the L2TP tunnel is successfully set up.
Remote tunnel name	Name of the tunnel remote end.
Remote Address	Remote port number and IP address. The port number is 1701 in general.
ReCall Address	Recall address.
Local tunnel name	Name of the tunnel local end.
Local Address	Local port number and IP address. The port number is 1701 in general.
active sessions	Number of sessions established in the current L2TP tunnel.
Session Limit	Maximum number of sessions that can be established in the L2TP tunnel.
Control Ns	Number of control packets sent over the tunnel.
Control Nr	Number of control packets received over the tunnel.
Retransmission	Number of retransmission times after the transmission of control packets fails.
Timeout	Aging time of control packets.
Hello Interval	Interval for sending Hello packets.
Local RWS	Size of the local receiving window.
Remote RWS	Size of the remote receiving window.
OuterDscp	Priority of packets after L2TP encapsulation. This parameter is used in QoS deployment.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Source Interface	Outbound interface of the L2TP tunnel • When multiple equal cost routes exist between the local and remote ends, the name of the access-side interface is displayed. • When no equal cost routes exist between the local and remote ends, **Routing** is displayed.

Related Topics

12.1.2 display l2tp session

12.1.4 display l2tp-group

Function

The **display l2tp-group** command displays configurations of the L2TP group on the device.

Format

display l2tp-group [*group-number*]

Parameters

Parameter	Description	Value
group-number	Specifies an L2TP group.	The value is an integer and the value range depends on device types. • AR100&AR120&AR150&AR160&AR200 series: 1 to 16 • AR1200 series, AR2201-48FE, AR2202-48FE, AR2204E, AR2204E-D, AR2204: 1 to 128 • AR2220, AR2220E, AR2240C: 1 to 512 • AR2204XE, AR2204XE-DC, AR2240, AR3200, and AR3600 (using SRUX5) series: 1 to 1024

Copyright © Huawei Technologies Co., Ltd.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

This command displays the L2TP group and its number.

You can also use this command to view L2TP configurations of a specified group to rectify a fault or check the configurations.

Example

Display the L2TP group existing on the device currently.

```
<Huawei> display l2tp-group
-----------------------------------------
 L2TP-GROUP    GROUP-NUMBER
-----------------------------------------
 1             1
 2             2
 4             4
-----------------------------------------
```

Table 12-5 Description of the display l2tp-group command output

Item	Description
L2TP-GROUP	L2TP group identified by a group number.
GROUP-NUMBER	L2TP group number.

Display the configurations of the L2TP group **1**.

```
<Huawei> display l2tp-group 1
 -------------------------------------------------
 L2tp-index         :    1
 GroupType          :    ACCEPT_DIALIN_L2TP
 TunnelAuth         :    Use tunnel authentication
 LocalName          :    lns
 Encrypt            :   0
 Hello              :   60
 Retransmit         :   5
 Timeout            :   2
 IfIndex            :   4294967295
 SrcIp              :   255.255.255.255
 VtNum              :   1
 RemoteName         :   lac1
 ForceChap          :   0
 LcpReg             :   0
 LcpMismatch        :   0
 tunnel each user   :   0
 -------------------------------------------------
```

 Copyright © Huawei Technologies Co., Ltd.

Table 12-6 Description of the display l2tp-group command output

Item	Description
L2tp-index	L2TP group number.
GroupType	L2TP group type. ● REQUEST_DIALIN_L2TP: The device functions as the LAC to receive dial-up calls and initiate L2TP connections to the LNS. ● ACCEPT_DIALIN_L2TP: The device functions as the LNS to receive the L2TP connection requests from the LAC. ● VPDNGROUPTYPE_NONE: The L2TP group function is not configured.
TunnelAuth	Whether tunnel authentication is enabled.
LocalName	Name of the tunnel local end.
Encrypt	Whether the authentication password is configured for tunnel encapsulation. ● 0: no ● 1: yes
Hello	Interval for sending Hello messages (the default interval is 60 seconds).
Retransmit	Number of retransmission times after the transmission of control packets fails (the default number of retransmissions is 5).
Timeout	Aging time of control packets (the default aging time is 2 seconds).
IfIndex	Interface index bound to the tunnel.
SrcIp	IP address of the tunnel source interface.
VtNum	Number of the virtual interface template.
RemoteName	Name of the tunnel remote end.
ForceChap	Whether mandatory CHAP authentication is enabled. ● 0: no ● 1: yes
LcpReg	Whether LCP renegotiation is enabled. ● 0: no ● 1: yes

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
LcpMismatch	Whether mandatory LCP renegotiation is enabled when the PPP authentication mode on the LAC is different from that on the LNS. • 0: no • 1: yes
tunnel each user	Whether an L2TP user exclusively occupies an L2TP tunnel. • 0: no • 1: yes

12.1.5 display l2tp statistics tunnel

Function

The **display l2tp statistics tunnel** command displays L2TP packet statistics.

Format

display l2tp statistics tunnel [**local-id** *tunnel-id*]

Parameters

Parameter	Description	Value
local-id *tunnel-id*	Specifies the local tunnel ID of an L2TP tunnel.	The value is an integer and the value range depends on device types. • AR100&AR120&AR150&AR160&AR200 series: 1 to 16 • AR1200 series, AR2201-48FE, AR2202-48FE, AR2204E, AR2204E-D, AR2204: 1 to 128 • AR2220, AR2220E, AR2240C: 1 to 512 • AR2204XE, AR2204XE-DC, AR2240, AR3200, and AR3600 (using SRUX5) series: 1 to 1024

Copyright © Huawei Technologies Co., Ltd.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

When L2TP users go online, there are packet exchanges of multiple protocols. You can run the **display l2tp statistics tunnel** command to check L2TP packet statistics.

Prerequisites

A tunnel is established successfully before you run the **display l2tp statistics tunnel local-id** *tunnel-id* command. You can run the **display l2tp tunnel** command to check the value of **local-id**.

Example

Display L2TP packet statistics of the device.

```
<Huawei> display l2tp statistics tunnel

              SEND        RESEND          RCVD
          ==========    ==========    ==========
SCCRQ              0             0             9
SCCRP              9            30             0
SCCCN              0             0             2
StopCCN            7             0             0
ICRQ               0             0             2
ICRP               2             0             0
ICCN               0             0             2
CDN                0             0             0
Hello              5             0             5
Total             23            30            20
```

Display L2TP packet statistics of tunnel 1.

```
<Huawei> display l2tp tunnel

 Total tunnel : 1
 LocalTID RemoteTID RemoteAddress    Port   Sessions RemoteName
 1        1         10.1.2.4         1701   1        lns
<Huawei> display l2tp statistics tunnel local-id 1
Tunnel LocalID: 1
Tunnel RemoteID: 1
Local Address: 10.1.1.1
Remote Address: 10.1.1.2

              SEND        RESEND          RCVD
          ==========    ==========    ==========
SCCRQ              0             0             1
SCCRP              1             0             0
SCCCN              0             0             1
StopCCN            0             0             0
ICRQ               0             0             1
ICRP               1             0             0
ICCN               0             0             1
CDN                0             0             0
```

 Copyright © Huawei Technologies Co., Ltd.

```
Hello                5           0           5
Total                7           0           9
```

Table 12-7 Description of the **display l2tp statistics tunnel** command output

Item	Description
Tunnel LocalID	Local ID of the L2TP tunnel.
Tunnel RemoteID	Remote ID of the L2TP tunnel.
Local Address	Local IP address of the L2TP tunnel.
Remote Address	Remote IP address of the L2TP tunnel.
SEND	Number of sent L2TP packets.
RESEND	Number of resent L2TP packets.
RCVD	Number of received L2TP packets.
SCCRQ	Start control connection request packet.
SCCRP	Start control connection reply packet.
SCCCN	Start control connection connected packet.
StopCCN	Stop control connection notification packet.
ICRQ	Incoming call request packet.
ICRP	Incoming call reply packet.
ICCN	Incoming call connected packet.
CDN	Call disconnection packet.
Hello	Hello packet.
Total	Total number of sent, resent, and received packets of various types.

NOTE

The device only receives SCCRQ, SCCCN, ICRQ, and ICCN packets.
The device only sends and resends SCCRP and ICRP packets.
The device only sends and receives StopCCN, CDN, and Hello packets.

Related Topics

12.1.3 display l2tp tunnel

 Copyright © Huawei Technologies Co., Ltd.

12.1.6 l2tp aging

Function

The **l2tp aging** command sets the LNS locking duration.

The **undo l2tp aging** command restores the default value.

By default, the LNS locking duration is 30 seconds.

Format

l2tp aging *time*

undo l2tp aging

Parameters

Parameter	Description	Value
time	Specifies the LNS aging time.	The value is an integer that ranges from 1 to 3600, in seconds.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

When the device attempts to set up a tunnel to an LNS but the LNS runs abnormally, the device marks the LNS as unusable and does not set up a tunnel to the LNS in a period. This period is the LNS locking duration. After the locking duration, the device attempts to set up a tunnel to the LNS again.

Example

Set the LNS aging time to 60 seconds.

```
<Huawei> system-view
[Huawei] l2tp aging 60
```

12.1.7 l2tp enable

Function

The **l2tp enable** command enables L2TP globally.

The **undo l2tp enable** command disables L2TP.

By default, L2TP is disabled.

 Copyright © Huawei Technologies Co., Ltd.

Format

l2tp enable

undo l2tp enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

TheL2TP function enables remote users to dial up to access resources in the enterprise headquarters. You can complete L2TP configurations and then enable L2TP. You can also enable L2TP first and then complete L2TP configurations.

Precautions

The L2TP configurations take effect only after you run the **l2tp enable** command. If you run the **undo l2tp enable** command, the L2TP configurations do not take effect.

Example

Enable L2TP on the router.

```
<Huawei> system-view
[Huawei] l2tp enable
```

12.1.8 l2tp-auto-client enable

Function

The **l2tp-auto-client enable** command enables a virtual PPP user on the device to initiate an L2TP connection request.

The **undo l2tp-auto-client enable** command disables a virtual PPP user on the device from initiating an L2TP connection request.

By default, a virtual PPP user cannot initiate an L2TP connection request.

Format

l2tp-auto-client enable

undo l2tp-auto-client enable

 Copyright © Huawei Technologies Co., Ltd.

Parameters

None

Views

VT interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

An L2TP connection request is initiated in the following cases:

- The LAC receives a dial-up call from a remote user, and then initiates an L2TP connection request.
- A virtual PPP user on the L2TP Client automatically dials up, and the L2TP Client initiates an L2TP connection request.

In auto L2TP Client-initiated mode, users in the branch do not need to be managed by the headquarters in a centralized manner. Instead, the LNS in the headquarters authenticates only the gateway in the branch. The branch gateway functions as the L2TP Client on which virtual PPP users are created. The virtual users automatically dial up to initiate L2TP connections to the LNS. No additional devices or configurations are required for branch users to access the headquarters resources.

Prerequisites

L2TP has been enabled globally by running the **l2tp enable** command on the LAC or L2TP Client.

Example

Enable a virtual PPP user to initiate an L2TP tunnel.

```
<Huawei> system-view
[Huawei] l2tp enable
[Huawei] interface virtual-template 1
[Huawei-Virtual-Template1] l2tp-auto-client enable
```

Related Topics

12.1.7 l2tp enable

12.1.9 l2tp-group

Function

The **l2tp-group** command creates an L2TP group or displays an L2TP group with a specified group number.

The **undo l2tp-group** command deletes an L2TP group.

 Copyright © Huawei Technologies Co., Ltd.

By default, no L2TP group is created.

Format

l2tp-group *group-number*

undo l2tp-group *group-number*

Parameters

Parameter	Description	Value
group-number	Specifies the L2TP group number.	The value is an integer and the value range depends on device types. • AR100&AR120&AR150&AR160&AR200 series: 1 to 16 • AR1200 series, AR2201-48FE, AR2202-48FE, AR2204E, AR2204E-D, AR2204: 1 to 128 • AR2220, AR2220E, AR2240C: 1 to 512 • AR2204XE, AR2204XE-DC, AR2240, AR3200, and AR3600 (using SRUX5) series: 1 to 1024

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

An L2TP tunnel is established after the LAC and LNS negotiate L2TP parameters successfully. These L2TP parameters are set in the L2TP group view. An L2TP group is an end of a tunnel. A local end and a remote end constitute an L2TP tunnel.

When the group number is 1, it is the default group. When the default group is configured on the LNS and no remote tunnel name is specified, the LNS accepts any L2TP connection request initiated by the LAC.

 Copyright © Huawei Technologies Co., Ltd.

Prerequisites

L2TP has been enabled by running the **l2tp enable** command in the system view.

Follow-up Procedure

Configure L2TP parameters on the LAC or LNS.

Precautions

After you run the **undo l2tp-group** command to delete an L2TP group, all information about this group is deleted.

If an L2TP tunnel with the group as one end exists, this group cannot be deleted. Run the **reset l2tp tunnel** { **local-id** *local-id* | **peer-name** *peer-name* } command in the user view to forcibly disconnect the L2TP tunnel based on the tunnel ID or remote tunnel name, and then delete the L2TP group.

Example

Create L2TP group 2 and enter the L2TP group 2 view.

```
<Huawei> system-view
[Huawei] l2tp-group 2
[Huawei-l2tp2]
```

Related Topics

12.1.1 allow l2tp

12.1.16 start l2tp

12.1.14 reset l2tp tunnel

12.1.10 mandatory-chap

Function

The **mandatory-chap** command enables the LNS to perform mandatory CHAP authentication on remote users.

The **undo mandatory-chap** command disables mandatory CHAP authentication.

By default, mandatory CHAP authentication is disabled on the LNS.

Format

mandatory-chap

undo mandatory-chap

Parameters

None

Views

L2TP group view

 Copyright © Huawei Technologies Co., Ltd.

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Mandatory CHAP authentication is enabled on networks that demand high security. The LNS authenticates remote users using CHAP authentication. If PAP authentication mode is configured on the LAC, the LNS will not perform PPP negotiation with the LAC immediately after receiving the authentication success message. Instead, the LNS requires that the remote user initiates secondary CHAP authentication.

Prerequisites

The **l2tp-group** *l2tp-group* command has been executed to create an L2TP group and enter the L2TP group view.

Precautions

Some PPP clients may not support the second authentication. In this case, the L2TP connection fails if mandatory CHAP authentication is enabled.

When LCP renegotiation and mandatory CHAP authentication are configured simultaneously in an L2TP group, the LCP renegotiation takes effect.

Example

Enable mandatory CHAP authentication.

```
<Huawei> system-view
[Huawei] l2tp-group 1
[Huawei-l2tp1] mandatory-chap
```

Related Topics

12.1.11 mandatory-lcp

12.1.11 mandatory-lcp

Function

The **mandatory-lcp** command enables LCP renegotiation on the LNS.

The **undo mandatory-lcp** command disables LCP renegotiation.

By default, LCP renegotiation is disabled on the LNS.

Format

mandatory-lcp

undo mandatory-lcp

 Copyright © Huawei Technologies Co., Ltd.

Parameters

None

Views

L2TP group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On networks that demand high security, the LNS does not trust the authentication result on remote users performed by the LAC. In this case, enable LCP renegotiation to perform second authentication on remote users. L2TP tunnels can be set up after PPP renegotiation between the LNS and remote users succeeds.

Prerequisites

The **l2tp-group** *l2tp-group* command has been executed to create an L2TP group and enter the L2TP group view.

Precautions

Some PPP clients may not support the second authentication. In this case, the L2TP connection fails when LCP renegotiation is enabled.

When LCP renegotiation and mandatory CHAP authentication are configured simultaneously in an L2TP group, the LCP renegotiation takes effect.

Example

Enable LCP renegotiation.

```
<Huawei> system-view
[Huawei] l2tp-group 1
[Huawei-l2tp1] mandatory-lcp
```

Related Topics

12.1.10 mandatory-chap

12.1.12 multichassis-mp enable

Function

The **multichassis-mp enable** command enables Multi-Chassis Multilink PPP (MMP) for an L2TP group.

The **undo multichassis-mp enable** command disables MMP for an L2TP group.

By default, MMP is disabled for an L2TP group.

 Copyright © Huawei Technologies Co., Ltd.

Format

multichassis-mp enable

undo multichassis-mp enable

Parameters

None

Views

L2TP group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

MMP allows multiple dialup requests sent by the same branch device to multiple access servers to be terminated in the same bundle through L2TP, which increases bandwidth of the branch device. In MMP scenarios, run the **multichassis-mp enable** command for an L2TP group on the access server (LAC/LNS).

The access server processes ISDN requests from the branch device as follows:

- If an MP bundle has been created, the access server adds ISDN requests to the MP bundle and does not initiate L2TP dialup.
- If no MP bundle is created, the access server initiates L2TP dialup according to user information and searches an MP bundle on another access server.

  If an MP bundle exists on another access server, the access server adds ISDN requests to the MP bundle. If no MP bundle is created, the access server creates an MP bundle and adds ISDN requests to the MP bundle so that ISDN users can connect to the ISDN.

Precautions

Before disabling MMP, ensure that the triggering condition of initiating calls is not specified when the local end serves as the L2TP LAC end. If the triggering condition has been specified, run the **undo start** command to delete the triggering condition.

Example

Enable MMP.

```
<Huawei> system-view
[Huawei] l2tp-group 1
[Huawei-l2tp1] multichassis-mp enable
```

Related Topics

12.1.11 mandatory-lcp

 Copyright © Huawei Technologies Co., Ltd.

12.1.13 reset l2tp session

Function

The **reset l2tp session** command forcibly disconnects a specified L2TP session.

Format

reset l2tp session session-id *session-id*

Parameters

Parameter	Description	Value
session-id *session-id*	Specifies the session ID of the L2TP tunnel local end.	The value is an integer and the value range depends on device types. • AR100&AR120&AR150&AR160&AR200 series: 1 to 16 • AR1200 series, AR2201-48FE, AR2202-48FE, AR2204E, AR2204E-D, AR2204: 1 to 128 • AR2220, AR2220E, AR2240C: 1 to 512 • AR2204XE, AR2204XE-DC, AR2240, AR3200, and AR3600 (using SRUX5) series: 1 to 1024

Views

User view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A session can be set up only after a tunnel is created successfully. An L2TP session corresponds to a remote dial-up user.

When a security problem occurs or when you locate a fault, run the **reset l2tp session** command to forcibly disconnect the specified L2TP session to force the specified remote user to go offline.

When the remote user calls in again, the session can be reestablished.

Precautions

The **reset l2tp session** command disconnects the specified L2TP session. Exercise caution before you run this command.

Copyright © Huawei Technologies Co., Ltd.

Example

Disconnect the L2TP session **1**.

```
<Huawei> reset l2tp session session-id 1
```

Related Topics

12.1.2 display l2tp session

12.1.14 reset l2tp tunnel

Function

The **reset l2tp tunnel** command forcibly disconnects a specified tunnel connection and all sessions in the tunnel.

Format

reset l2tp tunnel { **peer-name** *remote-name* | **local-id** *tunnel-id* }

Parameters

Parameter	Description	Value
peer-name *remote-name*	Specifies the remote tunnel name of the L2TP tunnel.	The value is a string of 1 to 30 characters.
local-id *tunnel-id*	Specifies the remote tunnel ID of the L2TP tunnel.	The value is an integer and the value range depends on device types. • AR100&AR120&AR150&AR160&AR200 series: 1 to 16 • AR1200 series, AR2201-48FE, AR2202-48FE, AR2204E, AR2204E-D, AR2204: 1 to 128 • AR2220, AR2220E, AR2240C: 1 to 512 • AR2204XE, AR2204XE-DC, AR2240, AR3200, and AR3600 (using SRUX5) series: 1 to 1024

Views

User view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

 Copyright © Huawei Technologies Co., Ltd.

When no L2TP remote user exists, a fault occurs on the network, or the L2TP tunnel is not required, you can use this command to disconnect a tunnel connection and all sessions in the tunnel.

If the specified remote tunnel name does not exist, the command has no effect on the current tunnel connection. If multiple tunnels with the same specified remote tunnel name exist, all these tunnel connections and sessions are disconnected. If a tunnel ID is specified, only the specified tunnel connection is disconnected.

When the remote user calls in again, the tunnel can be reestablished.

Follow-up Procedure

You can change parameters of an L2TP group or delete the L2TP group after the L2TP tunnel is disconnected and before a new L2TP tunnel is established.

Precautions

The **reset l2tp tunnel** command disconnects the specified L2TP tunnel and all sessions in the tunnel. Exercise caution when you run this command.

Example

Disconnect the L2TP tunnel with a remote tunnel named **lac**.

```
<Huawei> reset l2tp tunnel peer-name lac
 Clear tunnel remote name = lac
```

Related Topics

12.1.3 display l2tp tunnel

12.1.15 reset l2tp statistics tunnel

Function

The **reset l2tp statistics tunnel** command resets L2TP packet statistics.

Format

reset l2tp statistics tunnel [**local-id** *tunnel-id*]

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
local-id *tunnel-id*	Specifies the local tunnel ID of an L2TP tunnel.	The value is an integer and the value range depends on device types. • AR100&AR120&AR150&AR160&AR200 series: 1 to 16 • AR1200 series, AR2201-48FE, AR2202-48FE, AR2204E, AR2204E-D, AR2204: 1 to 128 • AR2220, AR2220E, AR2240C: 1 to 512 • AR2204XE, AR2204XE-DC, AR2240, AR3200, and AR3600 (using SRUX5) series: 1 to 1024

Views

User view

Default Level

2: Configuration level

Usage Guidelines

To view statistics on L2TP packets within a period of time, you can run the **reset l2tp statistics tunnel** command to clear the existing packet statistics.

Example

Reset L2TP packet statistics of the device.

```
<Huawei> reset l2tp statistics tunnel
 Info: Reset tunnel Statistics success.
```

Reset L2TP packet statistics of tunnel 1.

```
<Huawei> reset l2tp statistics tunnel local-id 1
 Info: Reset tunnel Statistics success, LocID = 1.
```

 Copyright © Huawei Technologies Co., Ltd.

12.1.16 start l2tp

Function

The **start l2tp** command specifies the triggering condition of initiating calls when the local end functions as the LAC.

The **undo start** command deletes the triggering condition.

By default, no triggering condition is configured.

Format

start l2tp ip *ip-address* &<1-4> { **domain** *domain-name* | **fullusername** *user-name* | **interface** *interface-type interface-number* | **vpn-instance** *vpn-instance-name* **fullusername** *user-name* }

start l2tp host *hostname* { **domain** *domain-name* | **fullusername** *user-name* }

undo start

Parameters

Parameter	Description	Value
ip *ip-address*	Specifies the IP address of the LNS. You can specify a maximum of four IP addresses in the primary and secondary LNSs scenario. The IP addresses are in descending order of priorities, that is, the IP address configured first has the highest priority.	-
host *hostname*	Specifies the LNS domain name.	The value is a string of 1 to 255 case-sensitive characters
domain *domain-name*	Specifies the domain name that triggers the L2TP connection request. **NOTE** Run the **domain** *domain-name* command to create a domain first. Otherwise, the domain name cannot be specified.	The value is a string of 1 to 20 case-insensitive characters.
vpn-instance *vpn-instance-name*	Specifies the VPN instance to which the IP address of the L2TP connection belongs. Route information to LNSs exists in the routing table of the VPN instance.	The value is a string of 1 to 31 case-sensitive characters.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
fullusername *username*	Specifies the full user name that triggers the L2TP connection request.	The value is a string of 1 to 64 case-insensitive characters.
interface *interface-type interface-number*	Specifies the name of an interface that triggers L2TP connection requests. • *interface-type* specifies the interface type. • *interface-number* specifies the interface number.	-

Views

L2TP group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Run the **start l2tp** command on the LAC. L2TP connection requests are triggered on the device in the following situations:

- Triggered based on the domain name. For example, you can specify users with the domain name **huawei.com** as VPDN users.
- Triggered based on the full user name. For example, you can specify users with the full name **user@huawei.com** as VPDN users. L2TP connections are triggered only after the device receives requests from a user with full name **user@huawei.com**.
- The device searches for a route to the LNS based on the VPN instance, such as **VPN1**. The device can initiate an L2TP connection only after an available route is found.
- Triggered based on the interface name. User requests are added to an MP bundle.

  In MMP scenarios, the access server functions as both the LAC and LNS.

After the LAC receives call requests from remote users, it performs the following operations:

- Triggered based on the domain name, VPN attribute, or full user name.

  If the call initiator is a VPDN user, the LAC sends L2TP connection requests to LNSs according to the sequence in which the LNSs were configured. If the LAC receives a response packet from the LNS, this LNS will function as the remote end of the L2TP tunnel. If the LAC receives no response from the LNS, the LAC sends an L2TP connection request to another LNS.

 Copyright © Huawei Technologies Co., Ltd.

- Initiates L2TP connection requests based on the interface name.

  After receiving ISDN requests from users, the access server where no MP bundle is configured initiates an L2TP tunnel setup request to the LNSs and searches for an MP bundle. After receiving a response from the first LNS, the access server uses the LNS as the remote end of the L2TP tunnel and adds user requests to the MP bundle. If the access server does not receive responses from any LNS, it creates an MP bundle and adds user requests to the MP bundle so that users can connect to the ISDN.

Prerequisites

The **multichassis-mp enable** command has been executed to enable MMP when the LAC initiates L2TP connection requests based on the interface name.

Example

Determine VPDN users based on the domain name **huawei.com** with the IP address of the LNS in the headquarters as 10.1.2.3.

```
<Huawei> system-view
[Huawei] l2tp-group 1
[Huawei-l2tp1] start l2tp ip 10.1.2.3 domain huawei.com
```

Determine VPDN users based on the domain name **huawei.com** with the domain name of the LNS in the headquarters as **www.huawei.com**.

```
<Huawei> system-view
[Huawei] l2tp-group 1
[Huawei-l2tp1] start l2tp host www.huawei.com domain huawei.com
```

Find a route to the LNS in the routing table of **VPN1** and establish an L2TP connection to the LNS in the headquarters with the IP address 10.1.2.3.

```
<Huawei> system-view
[Huawei] l2tp-group 1
[Huawei-l2tp1] start l2tp ip 10.1.2.3 vpn-instance vpn1 fullusername huawei
```

In an MMP scenario, initiate L2TP connection requests to other access servers according to Serial1/0/0.

```
<Huawei> system-view
[Huawei] l2tp-group 1
[Huawei-l2tp1] multichassis-mp enable
[Huawei-l2tp1] start l2tp ip 10.1.2.3 interface serial 1/0/0
```

12.1.17 tunnel authentication

Function

The **tunnel authentication** command enables L2TP tunnel authentication.

The **undo tunnel authentication** command disables L2TP tunnel authentication.

By default, tunnel authentication is enabled.

Format

tunnel authentication

undo tunnel authentication

 Copyright © Huawei Technologies Co., Ltd.

Parameters

None

Views

L2TP group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To ensure data security, L2TP tunnel authentication is enabled by default. In case of network connectivity test or receiving a connection request sent by an unknown remote end, disable L2TP tunnel authentication. It is recommended that you enable L2TP tunnel authentication.

The tunnel authentication request can be initiated by the LAC or the LNS. As soon as one end is enabled with tunnel authentication, the identity authentication is performed in the tunnel setup process. The tunnel can be set up only if the passwords of both ends are the same and not empty. Otherwise, the local end automatically disconnects itself from the tunnel. If tunnel authentication is disabled on both ends, the authentication password does not take effect.

Follow-up Procedure

Run the **tunnel password** command to configure an authentication password. Configure the same authentication password on the LAC and LNS.

Precautions

By default, tunnel authentication is enabled, but no authentication password is configured. When the default configuration is used to set up an L2TP tunnel, tunnel authentication fails and the tunnel cannot be set up.

Example

Disable tunnel authentication.

```
<Huawei> system-view
[Huawei] l2tp-group 1
[Huawei-l2tp1] undo tunnel authentication
```

Related Topics

12.1.20 tunnel password

12.1.18 tunnel avp-hidden

Function

The **tunnel avp-hidden** command configures Attribute Value Pair (AVP) data to be transmitted in cipher text.

 Copyright © Huawei Technologies Co., Ltd.

The **undo tunnel avp-hidden** command restores the default transmission mode of AVP data.

By default, AVP data is transmitted in plain text.

Format

tunnel avp-hidden

undo tunnel avp-hidden

Parameters

None

Views

L2TP group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

AVP data carries some parameters of the L2TP protocol. For the purpose of security, run this command to configure AVP data to be transmitted in cipher text.

Prerequisites

The following operations have been performed:

1. Run the **l2tp-group** command to create an L2TP group and enter the L2TP group view.
2. Run the **tunnel authentication** command to enable tunnel authentication function. By default, tunnel authentication is enabled.
3. Run the **tunnel password** command to configure the authentication password.

Precautions

If AVP data is transmitted in plain text, the leakage of the user name and password occurs when L2TP packets are intercepted.

When you configure the AVP parameter encryption, enable tunnel authentication on the LAC and LNS, and configure the same authentication password on the two ends.

Example

Configure AVP data to be transmitted in cipher text.

```
<Huawei> system-view
[Huawei] l2tp-group 1
[Huawei-l2tp-1] tunnel authentication
```

 Copyright © Huawei Technologies Co., Ltd.

```
[Huawei-l2tp-1] tunnel password cipher huawei
[Huawei-l2tp-1] tunnel avp-hidden
```

12.1.19 tunnel name

Function

The **tunnel name** command specifies the local name of a tunnel.

The **undo tunnel name** command restores the default tunnel name.

By default, the local name of a tunnel is the device name.

Format

tunnel name *tunnel-name*

undo tunnel name

Parameters

Parameter	Description	Value
tunnel-name	Specifies the name of the local end of a tunnel.	The value is a string of 1 to 30 case-sensitive characters.

Views

L2TP group view

Default Level

2: Configuration level

Usage Guidelines

When you create an L2TP group, the local name of a tunnel is initialized to be the device name. Run the **tunnel name** command to specify another name as the local name. When the configured local tunnel name is the same as the initial host name of the device, the configured local tunnel name will take effect but will not be displayed during the query of configuration.

You can create multiple L2TP groups and establish multiple L2TP tunnels on a device. Specify a tunnel name for each tunnel to differentiate the tunnels. The tunnel name of the LAC end must be specified for the LNS to accept a connection request. It is recommended that you configure the tunnel name on the LAC end.

Example

Set the local tunnel name to **huawei**.

```
<Huawei> system-view
[Huawei] l2tp-group 1
[Huawei-l2tp-1] tunnel name huawei
```

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

12.1.1 allow l2tp

12.1.20 tunnel password

Function

The **tunnel password** command specifies a password for tunnel authentication.

The **undo tunnel password** command deletes the password.

By default, tunnel authentication is enabled, but no authentication password is configured.

Format

tunnel password { **simple** | **cipher** } *password*

undo tunnel password

Parameters

Parameter	Description	Value
simple	Indicates the password in plain text. **NOTICE** If **simple** is selected, the password is saved in the configuration file in plain text. This brings security risks. It is recommended that you select **cipher** to save the password in cipher text.	-
cipher	Indicates the password in cipher text. The password is displayed in cipher text.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
password	Specifies the password for tunnel authentication.	The password is a string of case-sensitive characters. The password cannot contain command line characters such as spaces and question marks (?). • If **simple** is specified, the password must be in plain text and contain 1 to 16 characters. • If **cipher** is specified, the password can be either in cipher or plain text, depending on what is entered. The password in plain text contains 1 to 16 characters, such as 1234567. The password in cipher mode must be a string of 24/32/48 bytes, for example, _(TT8F]Y\5SQ=^Q`MAF4<1!!.

Views

L2TP group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can decide whether to enable tunnel authentication before creating the tunnel connection. After tunnel authentication is enabled, run the **tunnel password** command to configure an authentication password. To ensure tunnel security, it is recommended that you enable tunnel authentication.

Prerequisites

The **l2tp-group** command has been executed to create an L2TP group and enter the L2TP group view.

Tunnel authentication has been enabled by running the **tunnel authentication** command. By default, tunnel authentication is enabled.

Precautions

If tunnel authentication is enabled on the LAC or the LNS, it must also be enabled on the other end. Configure the same authentication password on the LAC and LNS.

Example

Set the password for tunnel authentication to **huawei** in cipher text.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> system-view
[Huawei] l2tp-group 1
[Huawei-l2tp-1] tunnel password cipher huawei
```

Related Topics

12.1.17 tunnel authentication

12.1.21 tunnel timer hello

Function

The **tunnel timer hello** command sets the interval for sending Hello packets.

The **undo tunnel timer hello** command restores the interval to the default value.

By default, Hello packets are sent every 60s.

Format

tunnel timer hello *interval*

undo tunnel timer hello

Parameters

Parameter	Description	Value
interval	Specifies the interval for sending Hello packets.	The value is an integer that ranges from 0 to 1000, in seconds. If the value is 0, no Hello packet is sent.

Views

L2TP group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

L2TP uses Hello packets to check tunnel connectivity. The LAC and LNS periodically send Hello packets to each other. If no response packet is received within a specified period, they retransmit Hello packets. If Hello packets are retransmitted for five times but no response packet is received, the L2TP tunnel is disconnected.

When the network is unstable, set a shorter interval for sending Hello packets to detect tunnel status. When the network is stable, set the interval to a longer value. Different intervals can be set on the LNS and LAC.

Configuration Impact

 Copyright © Huawei Technologies Co., Ltd.

Hello packets are sent periodically, which increases network burdens. If the interval is set to a smaller value, network burdens increase.

Example

Set the interval for sending Hello packets to 99s.

```
<Huawei> system-view
[Huawei] l2tp-group 1
[Huawei-l2tp-1] tunnel timer hello 99
```

Related Topics

12.1.9 l2tp-group

12.2 L2TPv3 Configuration Commands

12.2.1 encapsulation l2tpv3

Function

The **encapsulation l2tpv3** command sets the tunnel type to static L2TPv3.

The **undo encapsulation l2tpv3** command deletes the specified tunnel type.

By default, the tunnel type is not specified.

Format

encapsulation l2tpv3 [**static**]

undo encapsulation l2tpv3

Parameters

Parameter	Description	Value
static	Sets the tunnel type to static L2TPv3.	-

Views

Tunnel interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If you want the device to directly forward data without packet negotiation, run the **encapsulation l2tpv3** command to set the tunnel type to static L2TPv3.

 Copyright © Huawei Technologies Co., Ltd.

Prerequisites

The L2TPv3 function has been enabled globally using the **l2tpv3 enable** command on the LCCE. A tunnel protocol has been configured on tunnel interfaces using the **tunnel-protocol** command.

Precautions

The **encapsulation l2tpv3** and **svpn-proposal** commands cannot be configured simultaneously. A tunnel can be bound only to one protocol.

If you run the **undo encapsulation l2tpv3** command, cookie and session of the tunnel, the tunnel source address and the tunnel destination address, as well as the binding between a tunnel and an AC configured using the **link-bridge** command.

Example

Set the tunnel type to static L2TPv3.

```
<Huawei> system-view
[Huawei] l2tpv3 enable
[Huawei] interface tunnel 0/0/1
[Huawei-Tunnel0/0/1] tunnel-protocol svpn
[Huawei-Tunnel0/0/1] encapsulation l2tpv3
```

Related Topics

12.2.2 l2tpv3 enable

12.3.21 tunnel-protocol

12.2.2 l2tpv3 enable

Function

The **l2tpv3 enable** command enables the L2TPv3 function globally.

The **undo l2tpv3 enable** command disables the L2TPv3 function.

By default, the L2TPv3 function is disabled.

Format

l2tpv3 enable

undo l2tpv3 enable

Parameters

None

Views

System view

 Copyright © Huawei Technologies Co., Ltd.

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If an enterprise wants Layer 2 data to be transparently transmitted on a Layer 3 network without changing the IP network, the L2TPv3 service can be deployed to implement communication between branches or between the headquarters and branches.

Precautions

The L2TPv3 function takes effect only after you run the **l2tpv3 enable** command.

Example

Enable the L2TPv3 function globally.

```
<Huawei> system-view
[Huawei] l2tpv3 enable
```

12.2.3 l2tpv3 local cookie

Function

The **l2tpv3 local cookie** command configures the local cookie key.

The **undo l2tpv3 local cookie** command deletes the local cookie key.

By default, the local cookie key is not configured.

Format

l2tpv3 local cookie { **key cipher** *cipher* | **length 4 plain lower-value** *local-lower-value1* | **length 8 plain lower-value** *local-lower-value2* **upper-value** *local-high-value* }

undo l2tpv3 local cookie

Parameters

Parameter	Description	Value
key cipher *cipher*	Specifies the cookie in cipher text. The local cookie is saved in cipher text. **NOTE** If the parameter is not specified, the cookie is saved in plain text which is not secure. You are advised to select **key cipher** to save the cookie in cipher text.	The value is a string of 1 to 8 case-sensitive bytes without spaces. If the cookie is in cipher text, the key is a string of 1 to 8 bytes and the encrypted password contains 48 bytes. If the cookie is in plain text, the plain-text password contains 4 or 8 bytes.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
length 4 plain lower-value *local-lower-value1*	Specifies a 4-byte cookie in plain text.	The value is a decimal integer that ranges from 0 to 4294967295.
length 8 plain lower-value *local-lower-value2*	Specifies the rightmost four bytes in the 8-byte key.	The value is a decimal integer that ranges from 0 to 4294967295.
upper-value *local-high-value*	Specifies the leftmost four bytes in the 8-byte key.	The value is a decimal integer that ranges from 0 to 4294967295.

Views

Tunnel interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Before establishing a tunnel, you need to create tunnel interfaces. Ensure that parameters of a local tunnel interface are complete and match the parameters configured on the remote device. The **l2tpv3 local cookie** command is used to configure the local cookie key.

Prerequisites

- The L2TPv3 function has been enabled globally using the **l2tpv3 enable** command.
- A tunnel protocol has been configured on tunnel interfaces using the **tunnel-protocol** command.
- The tunnel type has been set to static L2TPv3 using the **encapsulation l2tpv3** command.

Precautions

The **l2tpv3 local cookie** configured on the local device must be the same as the **l2tpv3 remote cookie** configured on the remote device. Traffic can be forwarded through a tunnel when they are the same. If they are different, traffic cannot be forwarded even though a tunnel is established.

Example

Set the local cookie key to **abc** in cipher text.

```
<Huawei> system-view
[Huawei] l2tpv3 enable
[Huawei] interface tunnel 0/0/1
[Huawei-Tunnel0/0/1] tunnel-protocol svpn
```

 Copyright © Huawei Technologies Co., Ltd.

```
[Huawei-Tunnel0/0/1] encapsulation l2tpv3
[Huawei-Tunnel0/0/1] l2tpv3 local cookie key ciper abc
```

Related Topics

12.2.5 l2tpv3 remote cookie

12.2.4 l2tpv3 local session-id

Function

The **l2tpv3 local session-id** command configures the local session ID.

The **undo l2tpv3 local session-id** command deletes the local session ID.

By default, the local session ID is not configured.

Format

l2tpv3 local session-id *local-session-id*

undo l2tpv3 local session-id

Parameters

Parameter	Description	Value
local-session-id	Specifies the local session ID.	The value is a decimal integer that ranges from 1 to 4294967295.

Views

Tunnel interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Before establishing a tunnel, you need to create tunnel interfaces. Ensure that parameters of a local tunnel interface are complete and match the parameters configured on the remote device. The **l2tpv3 local session-id** command is used to configure the local session ID.

Prerequisites

- The L2TPv3 function has been enabled globally using the **l2tpv3 enable** command.
- A tunnel protocol has been configured on tunnel interfaces using the **tunnel-protocol** command.
- The tunnel type has been set to static L2TPv3 using the **encapsulation l2tpv3** command.

Copyright © Huawei Technologies Co., Ltd.

Precautions

- The local session IDs are different for different tunnel interfaces.
- The *local-session-id* configured on the local device must be the same as the *remote session-id* configured on the remote device. Traffic can be forwarded through a tunnel when they are the same. If they are different, traffic cannot be forwarded even though a tunnel is established.

Example

Set the local session ID to 2.

```
<Huawei> system-view
[Huawei] l2tpv3 enable
[Huawei] interface tunnel 0/0/1
[Huawei-Tunnel0/0/1] tunnel-protocol svpn
[Huawei-Tunnel0/0/1] encapsulation l2tpv3
[Huawei-Tunnel0/0/1] l2tpv3 local session-id 2
```

Related Topics

12.2.6 l2tpv3 remote session-id

12.2.5 l2tpv3 remote cookie

Function

The **l2tpv3 remote cookie** command configures the remote cookie key.

The **undo l2tpv3 remote cookie** command deletes the remote cookie key.

By default, the remote cookie key is not configured.

Format

l2tpv3 remote cookie { **key cipher** *cipher* | **length 4 plain lower-value** *remote-lower-value1* | **length 8 plain lower-value** *remote-lower-value2* **upper-value** *remote-high-value* }

undo l2tpv3 remote cookie

Parameters

Parameter	Description	Value
key cipher *cipher*	Specifies the cookie in cipher text. The remote cookie is saved in cipher text. **NOTE** If the parameter is not specified, the cookie is saved in plain text which is not secure. You are advised to select **key cipher** to save the cookie in cipher text.	The value is a string of 1 to 8 case-sensitive bytes without spaces. If the cookie is in cipher text, the key is a string of 1 to 8 bytes and the encrypted password contains 48 bytes. If the cookie is in plain text, the plain-text password contains 4 or 8 bytes.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
length 4 plain lower-value *remote-lower-value1*	Specifies a 4-byte key in plain text.	The value is a decimal integer that ranges from 0 to 4294967295.
length 8 plain lower-value *remote-lower-value2*	Specifies the rightmost four bytes in the 8-byte key.	The value is a decimal integer that ranges from 0 to 4294967295.
upper-value *remote-high-value*	Specifies the leftmost four bytes in the 8-byte key.	The value is a decimal integer that ranges from 0 to 4294967295.

Views

Tunnel interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Before establishing a tunnel, you need to create tunnel interfaces. Ensure that parameters of a local tunnel interface are complete and match the parameters configured on the remote device. The **l2tpv3 remote cookie** command is used to configure the remote cookie key.

Prerequisites

- The L2TPv3 function has been enabled globally using the **l2tpv3 enable** command.
- A tunnel protocol has been configured on tunnel interfaces using the **tunnel-protocol** command.
- The tunnel type has been set to static L2TPv3 using the **encapsulation l2tpv3** command.

Precautions

The **l2tpv3 remote cookie** configured on the local device must be the same as the **l2tpv3 local cookie** configured on the remote device. Traffic can be forwarded through a tunnel when they are the same. If they are different, traffic cannot be forwarded even though a tunnel is established.

Example

Set the remote cookie key to **abc** in cipher text.

```
<Huawei> system-view
[Huawei] l2tpv3 enable
[Huawei] interface tunnel 0/0/1
[Huawei-Tunnel0/0/1] tunnel-protocol svpn
```

 Copyright © Huawei Technologies Co., Ltd.

```
[Huawei-Tunnel0/0/1] encapsulation l2tpv3
[Huawei-Tunnel0/0/1] l2tpv3 remote cookie key ciper abc
```

Related Topics

12.2.3 l2tpv3 local cookie

12.2.6 l2tpv3 remote session-id

Function

The **l2tpv3 remote session-id** command configures the remote session ID.

The **undo l2tpv3 remote session-id** command deletes the remote session ID.

By default, the remote session ID is not specified.

Format

l2tpv3 remote session-id *remote-session-id*

undo l2tpv3 remote session-id

Parameters

Parameter	Description	Value
remote-session-id	Specifies the remote session ID.	The value is a decimal integer that ranges from 1 to 4294967295.

Views

Tunnel interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Before establishing a tunnel, you need to create tunnel interfaces. Ensure that parameters of a local tunnel interface are complete and match the parameters configured on the remote device. The **l2tpv3 remote session-id** command is used to configure the remote session ID.

Prerequisites

- The L2TPv3 function has been enabled globally using the **l2tpv3 enable** command.
- A tunnel protocol has been configured on tunnel interfaces using the **tunnel-protocol** command.
- The tunnel type has been set to static L2TPv3 using the **encapsulation l2tpv3** command.

Copyright © Huawei Technologies Co., Ltd.

Precautions

The *remote session-id* configured on the local device must be the same as the *local-session-id* configured on the remote device. Traffic can be forwarded through a tunnel when they are the same. If they are different, traffic cannot be forwarded even though a tunnel is established.

Example

Set the remote session ID to 2.

```
<Huawei> system-view
[Huawei] l2tpv3 enable
[Huawei] interface tunnel 0/0/1
[Huawei-Tunnel0/0/1] tunnel-protocol svpn
[Huawei-Tunnel0/0/1] encapsulation l2tpv3
[Huawei-Tunnel0/0/1] l2tpv3 remote session-id 2
```

Related Topics

12.2.4 l2tpv3 local session-id

12.2.7 link-bridge

Function

The **link-bridge** command binds an AC interface to a tunnel interface.

The **undo link-bridge** command unbinds an AC interface from a tunnel interface.

By default, an AC interface is not bound to a tunnel interface.

Format

link-bridge tunnel *slot-number* [**vc-id** *vc-id*] { **tagged** | **raw** }

undo link-bridge tunnel *slot-number*

Parameters

Parameter	Description	Value
tunnel *slot-number*	Specifies a tunnel interface bound to an AC interface.	-
tagged	Reserves the service-delimiting tag (SD-tag) of a packet. This parameter can be set only if the AC is an Ethernet link.	-
raw	Deletes the SD-tag of a packet. This parameter can be set only if the AC is an Ethernet link.	-

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
vc-id *vc-id*	Specifies a vc-id.	The value is an integer that ranges from 1 to 4294967295.

Views

AC interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The LCCE devices can transparently transmit only Layer 3 packets when they are connected through an IP network. After Layer 2 packets enter an AC interface on an LCCE device, you can run the **link-bridge** command to bind the AC interface to a tunnel interface. After that, the AC interface encapsulates the Layer 2 packets based on parameters for the tunnel interface and transparently transmits the packets over the IP network based on routing information.

Prerequisites

- The L2TPv3 function has been enabled globally using the **l2tpv3 enable** command.
- A tunnel protocol has been configured on tunnel interfaces using the **tunnel-protocol** command.
- The tunnel type has been set to static L2TPv3 using the **encapsulation l2tpv3** command.

Precautions

- The link bridge function can be configured only on the Layer 3 interface.
- An AC interface can be bound only to one tunnel interface.
- After you run the **link-bridge** command to bind an AC interface to a tunnel interface, the physical status of the interfaces become Standby. After the tunnel is established, the Standby status is changed to Up.

Example

Bind Ethernet0/0/1 and Tunnel0/0/1 in tagged mode.

```
<Huawei> system-view
[Huawei] l2tpv3 enable
[Huawei] interface tunnel 0/0/1
[Huawei-Tunnel0/0/1] tunnel-protocol svpn
[Huawei-Tunnel0/0/1] encapsulation l2tpv3
[Huawei-Tunnel0/0/1] quit
[Huawei] interface ethernet0/0/1
[Huawei-Ethernet0/0/1] link-bridge tunnel 0/0/1 tagged
```

 Copyright © Huawei Technologies Co., Ltd.

12.2.8 tunnel-destination

Function

The **tunnel-destination** command configures a destination address for a tunnel interface.

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

By default, no destination address is configured for a tunnel interface.

Format

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

undo tunnel-destination

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance*	Specifies the name of the VPN instance that the destination address of a tunnel belongs to. **NOTE** You are advised to use the existing VPN instance; otherwise, a tunnel cannot be established.	The value is a string of 1 to 31 case-sensitive characters without spaces. If the string is enclosed in double quotation marks ("), the string can contain spaces.
dest-ip-address	Specifies the destination address for a tunnel.	The value is in dotted decimal notation.

Views

Tunnel interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Before establishing a tunnel, you need to create tunnel interfaces. After creating the tunnel interfaces, run the **tunnel-destination** command to configure destination addresses for the tunnel interfaces.

Prerequisites

- The L2TPv3 function has been enabled globally using the **l2tpv3 enable** command.
- A tunnel protocol has been configured on tunnel interfaces using the **tunnel-protocol** command.

 Copyright © Huawei Technologies Co., Ltd.

- The tunnel type has been set to static L2TPv3 using the **encapsulation l2tpv3** command.

Precautions

- The destination IP address of the local device must be a reachable IP address and be the same as the IP address of the PW interface on the remote device (the source IP address of the remote device).
- The source IP addresses, destination IP addresses, and VPN instances for different tunnel interfaces cannot be exactly the same.
- If you want to set **tunnel-destination** to **vpn-instance**, run the **ip vpn-instance** command to create a VPN instance first. A tunnel cannot be established if a VPN instance that does not exist is used.

Example

Set the destination address for Tunnel0/0/1.

```
<Huawei> system-view
[Huawei] l2tpv3 enable
[Huawei] interface tunnel 0/0/1
[Huawei-Tunnel 0/0/1] tunnel-protocol svpn
[Huawei-Tunnel 0/0/1] encapsulation l2tpv3
[Huawei-Tunnel 0/0/1] tunnel-destination 10.1.1.2
```

Set the destination address for Tunnel0/0/1 to 10.1.1.1 of vpn1.

```
<Huawei> system-view
[Huawei] l2tpv3 enable
[Huawei] interface tunnel 0/0/1
[Huawei-Tunnel0/0/1] tunnel-protocol svpn
[Huawei-Tunnel0/0/1] encapsulation l2tpv3
[Huawei-Tunnel0/0/1] tunnel-destination vpn-instance vpn1 10.1.1.1
```

Related Topics

12.2.9 tunnel-source

12.2.9 tunnel-source

Function

The **tunnel-source** command configures a source address for a tunnel interface.

The **undo tunnel-source** command deletes the source address of a tunnel interface.

By default, no source address is configured for a tunnel interface.

Format

tunnel-source [*source-ip-address* | *interface-type interface-number*]

undo tunnel-source

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
source-ip-address	Specifies the source IP address for a tunnel interface.	The value is in dotted decimal notation.
interface-type interface-number	Specifies the interface type for a tunnel interface. • *interface-type* specifies the interface type. • *interface-number* specifies the interface number.	Only the Ethernet, GigabitEthernet, and VLANIF interfaces are supported.

Views

Tunnel interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Before establishing a tunnel, you need to create tunnel interfaces. After creating the tunnel interfaces, run the **tunnel-source** command to configure source addresses for the tunnel interfaces.

Prerequisites

- The L2TPv3 function has been enabled globally using the **l2tpv3 enable** command.
- A tunnel protocol has been configured on tunnel interfaces using the **tunnel-protocol** command.
- The tunnel type has been set to static L2TPv3 using the **encapsulation l2tpv3** command.

Precautions

- The source IP address of a tunnel interface must be the same as the IP address of the PW interface on the local device. The IP address can be directly configured or be obtained from the Layer 3 interface for which an IP address has been configured.
- The source IP address of the local device must be the same as the destination IP address of the remote device.
- The source IP addresses, destination IP addresses, and VPN instances for different tunnel interfaces cannot be exactly the same.

Example

Set the source address for Tunnel0/0/1.

```
<Huawei> system-view
[Huawei] l2tpv3 enable
```

 Copyright © Huawei Technologies Co., Ltd.

```
[Huawei] interface tunnel 0/0/1
[Huawei-Tunnel 0/0/1] tunnel-protocol svpn
[Huawei-Tunnel 0/0/1] encapsulation l2tpv3
[Huawei-Tunnel 0/0/1] tunnel-source 10.1.1.1
```

Set the source address of Tunnel0/0/1 to the IP address of Ethernet0/0/1.

```
<Huawei> system-view
[Huawei] l2tpv3 enable
[Huawei] interface tunnel 0/0/1
[Huawei-Tunnel0/0/1] tunnel-protocol svpn
[Huawei-Tunnel0/0/1] encapsulation l2tpv3
[Huawei-Tunnel0/0/1] tunnel-source ethernet0/0/1
```

Related Topics

12.2.8 tunnel-destination

12.3 GRE Configuration Commands

12.3.1 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, the description of a tunnel interface is "HUAWEI, AR Series, Tunnel *interface-number* Interface".

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

 Copyright © Huawei Technologies Co., Ltd.

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 0/0/1.

```
<Huawei> system-view
[Huawei] interface tunnel 0/0/1
[Huawei-Tunnel0/0/1] description This is a tunnel from 10.1.1.1 to 10.2.2.2
```

Delete the description of Tunnel 0/0/1.

```
<Huawei> system-view
[Huawei] interface tunnel 0/0/1
[Huawei-Tunnel0/0/1] undo description
```

Related Topics

12.3.10 interface tunnel

12.3.3 display interface tunnel

12.3.2 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 tunnel or IPSec tunnel, you can specify **vpn-instance** *vpn-instance-name*.	The value is the name of an existing VPN instance.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
dest-ip-address	Specifies the destination IP address of a tunnel interface.	The value is in dotted decimal notation.

Views

Tunnel interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When configuring a GRE, IPv4 over IPv6, IPSec, MPLS TE, 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, IPSec, MPLS TE, IPv4 over IPv6, or IPv6 over IPv4 of manual mode using the **tunnel-protocol** command.

Precautions

Two or more GRE tunnel interfaces in a system can have the same source address and same destination address. The system uses GRE keys to identify these GRE tunnel interfaces. Normally, two tunnel interfaces in a system cannot have the same encapsulation mode, source address, and destination address.

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

On the IPSec, IPv6 over IPv4, IPv4 over IPv6, or GRE tunnel, the destination address of the local tunnel interface is the source address of the remote tunnel interface by the **source** command, and the source address of the local tunnel interface is the destination address of the remote tunnel interface.

Example

Set the destination address of the GRE tunnel Tunnel 0/0/1 to 10.1.1.1.

```
<Huawei> system-view
[Huawei] interface tunnel 0/0/1
[Huawei-Tunnel0/0/1] tunnel-protocol gre
[Huawei-Tunnel0/0/1] destination 10.1.1.1
```

 Copyright © Huawei Technologies Co., Ltd.

Set the destination address of the GRE tunnel Tunnel 0/0/0 to 10.1.1.1 that belongs to vpn1.

```
<Huawei> system-view
[Huawei] interface tunnel 0/0/0
[Huawei-Tunnel0/0/0] tunnel-protocol gre
[Huawei-Tunnel0/0/0] destination vpn-instance vpn1 10.1.1.1
```

Related Topics

12.3.10 interface tunnel

12.3.18 source

12.3.21 tunnel-protocol

12.3.3 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

Copyright © Huawei Technologies Co., Ltd.

Default Level

1: Monitoring level

Usage Guidelines

None

Example

Display the details of the tunnel interface.

```
<Huawei> display interface tunnel 0/0/2
Tunnel0/0/2 current state : UP
Line protocol current state : UP
Description:HUAWEI, AR Series, Tunnel0/0/2 Interface
Route Port,The Maximum Transmit Unit is 1500
Internet protocol processing : disabled
Encapsulation is TUNNEL, loopback not set
Tunnel source 10.10.10.1 (GigabitEthernet0/0/1), destination 10.1.1.1
Tunnel protocol/transport GRE/IP, key disabled
keepalive disabled
Checksumming of packets disabled
Current system time: 2012-08-09 18:53:47
    300 seconds input rate 0 bits/sec, 0 packets/sec
    300 seconds output rate 0 bits/sec, 0 packets/sec
    15 seconds input rate 0 bits/sec, 0 packets/sec
    15 seconds output rate 0 bits/sec, 0 packets/sec
    0 packets input,  0 bytes
    0 input error
    0 packets output,  0 bytes
    0 output error
    Input bandwidth utilization  : 0%
    Output bandwidth utilization : 0%
```

Table 12-8 Description of the display interface tunnel command output

Item	Description
Tunnel0/0/2 current state	Physical layer status of the Tunnel0/0/2 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 of the Tunnel0/0/2 interface: ● UP: The link layer protocol of the tunnel interface works normally. ● DOWN: The link layer protocol of the tunnel interface is abnormal.
Description	Description of the tunnel interface.
Route Port,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.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Internet protocol processing: disabled	IP protocol is disabled.
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 10.10.10.1 (GigabitEthernet0/0/1)	The source address of the tunnel is 10.10.10.1. That is, the IP address of the GigabitEthernet 0/0/1 interface sending packets at the source side is 10.10.10.1.
destination	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. ● IPSec: indicates tunnel mode of IPSec to protect data stream. ● MPLS: encapsulates packets into MPLS packets. ● IPv6 over IPv4: encapsulates IPv6 packets into IPv4 packets. ● IPv4 over IPv6: encapsulates IPv4 packets into IPv6 packets. ● SVPN: encapsulates packets into SVPN 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 disabled	The keepalive function of GRE is not enabled.
Checksumming of packets disabled	The check sum function of GRE is not enabled.
300 seconds input rate 0 bits/sec, 0 packets/sec	Rate of bits and packets received on the interface in the last 300 seconds. **NOTE** If the tunnel encapsulation protocol is SVPN, this field is not supported.
300 seconds output rate 0 bits/sec, 0 packets/sec	Rate of bits and packets sent through the interface in the last 300 seconds. **NOTE** If the tunnel encapsulation protocol is SVPN, this field is not supported.

Copyright © Huawei Technologies Co., Ltd.

Item	Description
15 seconds input rate 0 bits/sec, 0 packets/sec	Rate of bits and packets received on the interface during the last query period.
15 seconds output rate 0 bits/sec, 0 packets/sec	Rate of bits and packets sent through the interface during the last query period.
0 packets input, 0 bytes 0 input error	Total packets and bytes received on the interface and the total number of defective packets.
0 packets output, 0 bytes 0 output error	Total packets and bytes sent through the interface and the total number of defective packets.
Input bandwidth utilization	Input bandwidth usage.
Output bandwidth utilization	Output bandwidth usage.

Related Topics

12.3.11 keepalive

12.3.4 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

Copyright © Huawei Technologies Co., Ltd.

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 0/0/1.

```
<Huawei> system-view
[Huawei] interface tunnel 0/0/1
[Huawei-Tunnel0/0/1] tunnel-protocol gre
[Huawei-Tunnel0/0/1] keepalive
[Huawei-Tunnel0/0/1] 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 12-9 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.

Copyright © Huawei Technologies Co., Ltd.

Related Topics

12.3.11 keepalive

12.3.17 reset keepalive packets count

12.3.5 display tunnel-info

Function

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

NOTE

The AR100&AR120&AR150&AR160&AR200 series do not support this command.

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 interface boards.	-

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 detail 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 router.

 Copyright © Huawei Technologies Co., Ltd.

Example

View information about the GRE tunnel.

```
<Huawei> display tunnel-info tunnel-id 10003
Tunnel ID:                0x10003
Tunnel Token:             3
Type:                     gre
Destination:              10.1.1.1
Out Slot:                 0
Instance ID:              0
Interface:                Tunnel0/0/1
```

Table 12-10 Description of the display tunnel-info 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, 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 router sends packets.
Instance ID	VPN instance ID (0 indicates that a tunnel is a public network tunnel).
Interface	Local tunnel interface.

Display all tunnel information.

```
<Huawei> display tunnel-info all
* -> Allocated VC Token
Tunnel ID          Type               Destination          Token
------------------------------------------------------------------------------
0x1800800          lsp                3.3.3.3              0
0x1800801          lsp                2.2.2.2              1
0x41804bb8         lsp                192.168.2.0          3000
```

Display tunnel statistics.

```
<Huawei> display tunnel-info statistics
LSP/32bit LSP :                3/3
GRE :                          0
CRLSP :                        2
LOCAL IFNET :                  0
MPLS LOCAL IFNET :             0
VPN QOS LSP :                  0
Reserved :                     0
```

 Copyright © Huawei Technologies Co., Ltd.

Table 12-11 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.

Display tunnel statistics in the order of interface boards.

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

Table 12-12 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.

Copyright © Huawei Technologies Co., Ltd.

12.3.6 gre checksum

Function

The **gre checksum** command enables the end-to-end checksum function between both ends of a GRE tunnel.

The **undo gre checksum** command disables the end-to-end checksum function.

By default, the checksum function is disabled on the GRE tunnel.

Format

gre checksum

undo gre checksum

Parameters

None

Views

Tunnel interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can configure an end-to-end check between both ends of a GRE tunnel to improve the GRE tunnel security. This mechanism prevents the device from incorrectly identifying and receiving invalid packets.

You can configure the checksum function on the two ends of the tunnel as required to determine whether to trigger the checksum function.

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

After this command is executed, the integrity of packets can be checked.

If the checksum function is configured on the local end:

- The local end calculates the checksum according to the GRE header and payload.
- The local end sends a packet containing the checksum to the remote end.

 Copyright © Huawei Technologies Co., Ltd.

- The remote end calculates the checksum based on the packet and then compares the result with the checksum contained in the packet.
  - If the two checksum values are the same, the packet is processed.
  - If the two checksum values are different, the packet is discarded.

If the checksum function is enabled on the local end and disabled on the remote end, the local end does not perform checksum on received packets, but performs checksum on locally transmitted packets. If the checksum function is disabled on the local end and enabled on the remote end, the local end performs checksum on received packets, but does not perform checksum on locally transmitted packets.

Example

Enable checksum on the GRE Tunnel0/0/1 on the local device.

```
<Huawei> system-view
[Huawei] interface tunnel 0/0/1
[Huawei-Tunnel0/0/1] tunnel-protocol gre
[Huawei-Tunnel0/0/1] gre checksum
```

Related Topics

12.3.10 interface tunnel

12.3.21 tunnel-protocol

12.3.7 gre df-bit

Function

The **gre df-bit** command specifies the don't fragment (DF) flag bit for GRE packets.

By default, the DF flag bit for GRE packets uses the clear mode.

Format

gre df-bit { **clear** | **set** | **copy** }

Parameters

Parameter	Description	Value
clear	Sets the DF flag bit to 0, indicating that packets can be fragmented.	-
set	Sets the DF flag bit to 1, indicating that packets cannot be fragmented.	-
copy	Uses the DF flag bit of original packets.	-

 Copyright © Huawei Technologies Co., Ltd.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After original packets are encapsulated using GRE, the packet length may exceed the maximum transmission unit (MTU) allowed by the device outbound interface. In this case, you need to fragment the packets by running the **gre df-bit clear** command to prevent packet loss.

Precautions

If you run the **gre df-bit** command multiple times, only the latest configuration takes effect.

Example

Set the DF flag bit for GRE packets to clear.

```
<Huawei> system-view
[Huawei] gre df-bit clear
```

12.3.8 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.

Format

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

undo gre key

 Copyright © Huawei Technologies Co., Ltd.

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 bits.

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 0/0/1
[Huawei-Tunnel0/0/1] tunnel-protocol gre
[Huawei-Tunnel0/0/1] gre key cipher 123
```

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

12.3.10 interface tunnel
12.3.21 tunnel-protocol

12.3.9 gre map virtual-ethernet forward-broadcast disable

Function

The **gre map virtual-ethernet forward-broadcast disable** command disables a VE interface from forwarding broadcast, multicast, and unknown unicast packets to devices in the same VLAN.

The **undo gre map virtual-ethernet forward-broadcast disable** command enables a VE interface to forward broadcast, multicast, and unknown unicast packets to devices in the same VLAN.

By default, a VE interface can forward broadcast, multicast, and unknown unicast packets to devices in the same VLAN.

Format

gre map virtual-ethernet forward-broadcast disable

undo gre map virtual-ethernet forward-broadcast disable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

If branch CPE fails to obtain the MAC address of the HQ CPE, it will send broadcast, multicast, and unknown unicast packets to the VE interface bound to the tunnel interface of the HQ CPE. The VE interface then forwards the packets to other CPEs in the same VLAN. This consumes large network bandwidth, increases the workload of the HQ CPE, and may lead to drop of normal packets. To prevent this problem, you can configure the **gre map virtual-ethernet forward-broadcast disable** command on the HQ CPE to disable the VE interface from forwarding broadcast, multicast, and unknown unicast packets to other CPEs in the same VLAN.

Example

Disable a VE interface from forwarding broadcast, multicast, and unknown unicast packets to devices in the same VLAN.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> system-view
[Huawei] gre map virtual-ethernet forward-broadcast disable
```

12.3.10 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*

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
interface-number	Specifies the number of the tunnel interface with format "slot/subslot/number".	The slot, subslot, or interface number is an integer. The value range of the slot or subslot number varies according to the device type. The value of the interface number ranges. • AR100&AR120&AR150&AR160&AR200 series: 0 to 255 • AR1200 series, AR2201-48FE, AR2202-48FE, AR2204, AR2204E, AR2204E-D: 0 to 255 • AR2220, AR2220E: 0 to 1023 • AR2204XE, AR2204XE-DC, AR2240 (using SRU40, SRU60, or SRU80), AR2240C, AR3200 (using SRU40, SRU60, or SRU80) series: 0 to 2047 • AR2240 (using SRU200, or SRU200E, or SRU400), AR3200 (using SRU200, or SRU200E, or SRU400) series: 0 to 4095 • AR3600 (using SRUX5) series: 0 to 4095

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

 Copyright © Huawei Technologies Co., Ltd.

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
- IPSec
- 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

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, IPSec, IPv4 over IPv6, or IPv6 over IPv4 tunnel, run the **source** and **destination** commands.

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

If a tunnel is being used, services transmitted over the tunnel will be affected after the tunnel interface is deleted. Exercise caution when running the **undo interface tunnel** command.

Example

Create a tunnel interface.

```
<Huawei> system-view
[Huawei] interface tunnel 0/0/1
[Huawei-Tunnel0/0/1]
```

12.3.11 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.

 Copyright © Huawei Technologies Co., Ltd.

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.

 Copyright © Huawei Technologies Co., Ltd.

Precautions

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

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 0/0/1
[Huawei-Tunnel0/0/1] tunnel-protocol gre
[Huawei-Tunnel0/0/1] keepalive
```

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

```
<Huawei> system-view
[Huawei] interface tunnel 0/0/1
[Huawei-Tunnel0/0/1] tunnel-protocol gre
[Huawei-Tunnel0/0/1] keepalive period 12 retry-times 4
```

Related Topics

12.3.4 display keepalive packets count

12.3.17 reset keepalive packets count

12.3.12 link-bridge

Function

The **link-bridge** command binds an inbound interface to an outbound interface, so that packets received from the specified inbound interface can only be sent through the specified outbound interface.

The **undo link-bridge** command deletes the binding between inbound and outbound interfaces.

By default, inbound and outbound interfaces are not bound.

Format

link-bridge *tag-id* **interface** *interface-type interface-number* **out-interface** *interface-type interface-number* [**untagged** | **tagged** *vlan-id*]

undo link-bridge *tag-id*

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
tag-id	Indicates the tag ID of a link bridge.	The value is an integer that ranges from 1 to 65535.
interface *interface-type interface-number*	Indicates the inbound interface of the link bridge. • *interface-type* specifies the interface type. • *interface-number* specifies the interface number.	For FR, HDLC, or PPP packets, the inbound interface of a link bridge can only be a serial interface. For Ethernet packets, the inbound interface of a link bridge can only be an Ethernet, a GE, a XGE, Ethernet sub-interface, GE sub-interface, XGE sub-interface, or a VLANIF.
out-interface *interface-type interface-number*	Indicates the outbound interface of the link bridge. • *interface-type* specifies the interface type. • *interface-number* specifies the interface number.	Currently, the outbound interface of a link bridge can only be a tunnel interface.
untagged	Indicates that Ethernet packets do not carry tags.	-
tagged *vlan-id*	Specifies that the AR adds a VLAN tag to Ethernet packets before sending them over a tunnel.	The value is an integer that ranges from 1 to 4094.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Customers want to use GRE to transparently transmit FR, HDLC, PPP, or Ethernet packets over networks of a different network layer protocol, such as the IPv4 network. To transmit FR, HDLC, PPP, or Ethernet packets over a GRE tunnel, they need to configure the link bridge function to bind a serial, an Ethernet, a GE, a XGE, or a VLANIF interface with a tunnel interface, so that packets received from the serial, Ethernet, GE, XGE, or VLANIF interface can be directly sent out from the tunnel interface bound to it.

Copyright © Huawei Technologies Co., Ltd.

Prerequisites

A serial, Ethernet, GE, XGE, or VLANIF interface is available and a tunnel interface has been configured using the **interface** command.

Precautions

- After you configure this command, the protocol status of the inbound interface which is a serial interface turns Down and network-layer configurations on the inbound interface do not take effect. The inbound interface only functions as a bridge.
- After link bridge is bound to an interface, the interface does not support QoS. The inbound interface to which link bridge is bound supports traffic policy, traffic policing, traffic statistics collection, and mapping between 802.1p and DSCP priorities.
- Two link bridges must be configured with different tag IDs. The tag ID of a link bridge must be globally unique. If the tag ID of two link bridges is the same, an error message is displayed.
- Only one link bridge can be configured on a physical interface. If two link bridges are configured on the same physical interface, an error message is displayed.
- Only one link bridge can be configured on a tunnel interface. If two link bridges are configured on the same tunnel interface, an error message is displayed.
- If you specify the untagged mode, Ethernet packets transmitted over a GRE tunnel do not contain VLAN tags; otherwise, packets contain VLAN tags. You can determine whether to configure the untagged mode based on your actual networking to ensure normal traffic transmission over a tunnel. The following table describes the packet transmission rules.

Interface Type	Traffic Flow	Default Processing on Ethernet Packet	With Tag	Without Tag (Untagged)
Layer 2 Ethernet interface	From an Ethernet interface to a tunnel interface	The interface transparently transmits the packet.	The interface adds an outer tag to the packet before sending the packet.	If the packet contains a tag, the interface removes the tag before sending the packet.

 Copyright © Huawei Technologies Co., Ltd.

Interface Type	Traffic Flow	Default Processing on Ethernet Packet	With Tag	Without Tag (Untagged)
	From a tunnel interface to an Ethernet interface	The interface transparently transmits the packet.	If the tag differs from the specified one, the interface discards the packet. Otherwise, the interface removes the outer tag before sending the packet.	The interface transparently transmits the packet.
Layer 3 Ethernet interface	From an Ethernet interface to a tunnel interface	The interface transparently transmits the packet.	The interface adds an outer tag to the packet before sending the packet.	If the packet contains a tag, the interface removes the tag before sending the packet.
	From a tunnel interface to an Ethernet interface	The interface transparently transmits the packet.	If the tag differs from the specified one, the interface discards the packet. Otherwise, the interface removes the outer tag before sending the packet.	The interface transparently transmits the packet.

Copyright © Huawei Technologies Co., Ltd.

Interface Type	Traffic Flow	Default Processing on Ethernet Packet	With Tag	Without Tag (Untagged)
VLANIF interface	From a VLANIF interface to a tunnel interface	If the VLAN ID in the packet is the same as the PVID, the interface removes the tag; otherwise, the interface transparently transmits the packet.	The interface adds an outer tag to the packet before sending the packet.	If the packet contains a tag, the interface removes the tag before sending the packet.
	From a tunnel interface to a VLANIF interface	The device checks whether the VLAN ID in the packet is the same as that of the VLANIF interface. If so, the interface sends the packet; otherwise, the interface discards the packet.	If the tag differs from the specified one, the interface discards the packet. Otherwise, the interface removes the outer tag before sending the packet.	The interface adds the VLAN ID of the VLANIF interface to the packet before sending the packet.
Ethernet sub-interface	From an Ethernet sub-interface to a tunnel interface	The interface transparently transmits the packet.	The interface adds an outer tag to the packet before sending the packet.	If the packet contains a tag, the interface removes the tag before sending the packet.

Copyright © Huawei Technologies Co., Ltd.

Interface Type	Traffic Flow	Default Processing on Ethernet Packet	With Tag	Without Tag (Untagged)
	From a tunnel interface to an Ethernet sub-interface	The device checks whether the VLAN ID in the packet is the same as that of the Dot1q or QinQ sub-interface. If so, the interface sends the packet; otherwise, the interface discards the packet.	If the tag differs from the specified one, the interface discards the packet. Otherwise, the interface removes the outer tag before sending the packet.	The interface adds the VLAN ID of the Dot1q or QinQ sub-interface to the packet before sending the packet.

Example

Configure the link bridge function when the inbound interface is a serial interface.

```
<Huawei> system-view
[Huawei] link-bridge 2 interface serial 1/0/0 out-interface tunnel 0/0/1
```

Configure the link bridge function when the inbound interface is a GE interface.

```
<Huawei> system-view
[Huawei] link-bridge 2 interface gigabitethernet 1/0/0 out-interface tunnel 0/0/1
```

12.3.13 map interface virtual-ethernet

Function

The **map interface virtual-ethernet** command binds a Layer 2 virtual Ethernet (VE) interface to a physical Ethernet interface or tunnel interface.

The **undo map interface virtual-ethernet** command deletes the binding relationship.

By default, no Layer 2 VE interface is bound to a physical Ethernet interface or tunnel interface.

Format

map interface virtual-ethernet *ve-number*

undo map interface virtual-ethernet *ve-number*

Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
ve-number	Specifies a VE interface number. The value is in slot number/card ID/ sequence number format.	The VE interface number must already exist.

Views

Ethernet interface view, GE interface view, XGE interface view, 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. Ethernet over GRE can be configured to transparently transmit Ethernet packets over a GRE tunnel. After you run the **map interface virtual-ethernet** command to bind Layer 2 VE interfaces to the LAN-side physical Ethernet interface and WAN-side tunnel interface of a device, Ethernet packets received from the LAN-side interface are forwarded by the VE interfaces to the WAN-side tunnel interface. The WAN-side tunnel interface encapsulates the packets using GRE and transparently transmits the packets over a 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 or mGRE by using the **tunnel-protocol gre** [**p2mp**] command in the tunnel interface view.

Precautions

- One VE interface can be bound to only one physical Ethernet interface or tunnel interface.
- The physical Ethernet interface and VE interface added to the same VLAN cannot communicate with each other.
- After a VE interface is bound to a physical Ethernet interface, other services on the Ethernet interface become invalid. After a VE interface is bound to a tunnel interface, the MTU value configured by using the **mtu** command does not take effect for Layer 2 traffic.
- This command can be configured only in the Layer 3 physical Ethernet interface view and tunnel interface view.

 Copyright © Huawei Technologies Co., Ltd.

Example

Bind VE0/0/1 to GE0/0/2.

```
<Huawei> system-view
[Huawei] interface virtual-ethernet 0/0/1
[Huawei-Virtual-Ethernet0/0/1] portswitch
[Huawei-Virtual-Ethernet0/0/1] quit
[Huawei] interface gigabitethernet 0/0/2
[Huawei-GigabitEthernet0/0/2] map interface virtual-ethernet 0/0/1
```

Bind VE0/0/2 to Tunnel0/0/2.

```
<Huawei> system-view
[Huawei] interface virtual-ethernet 0/0/2
[Huawei-Virtual-Ethernet0/0/2] portswitch
[Huawei-Virtual-Ethernet0/0/2] quit
[Huawei] interface tunnel 0/0/2
[Huawei-Tunnel0/0/2] tunnel-protocol gre
[Huawei-Tunnel0/0/2] map interface virtual-ethernet 0/0/2
```

Related Topics

5.20.12 interface virtual-ethernet

12.3.15 portswitch (VE interface view)

12.3.10 interface tunnel

12.3.14 mtu (tunnel interface view)

Function

The **mtu** command sets the Maximum Transmission Unit (MTU) of a tunnel interface.

The **undo mtu** command restores the default value.

By default, the MTU is 1500 bytes on a tunnel interface.

Format

mtu *mtu*

undo mtu

Parameters

Parameter	Description	Value
mtu	Specifies the MTU of a tunnel interface.	An integer ranging from 128 to 9202, in bytes.

Views

Tunnel interface view

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

Usage Scenario

The size of data frames is limited at the network layer. Any time the IP layer receives an IP packet to be sent, it checks to which local interface the packet needs to be sent and obtains the MTU configured on the interface. Then the IP layer compares the MTU with the packet length. If the packet length is longer than the MTU, the IP layer fragments the packet into smaller packets, which are shorter than or equal to the MTU.

If unfragmentation is configured, some packets may be discarded during data transmission at the IP layer. To ensure jumbo packets are not dropped during transmission, you need to configure forcible fragmentation. In this case, you can run the **mtu** command to set the size of a fragment.

Precautions

Set the MTU for a tunnel interface based on actual networking. The default value is recommended. If a small MTU is used but the packet size is large, packets may be divided into many fragments. Then the packets are discarded by QoS queues. If a large MTU is used, packets may be transmitted at a low rate.

If IPv6 is run on a tunnel interface and the MTU set using the **mtu** command on the interface is smaller than 1280, IPv6 works abnormally on this interface. To prevent this problem, set the MTU of a tunnel interface to a value greater than or equal to 1280 if IPv6 runs on the tunnel interface.

After running the **mtu** command, run the **shutdown** and then **undo shutdown** commands on the interface. The set MTU then can take effect.

On a network with IPv4 over IPv6 tunnels, if a tunnel interface is Down, the MTU value of the tunnel interface 64000 does not take effect. After the tunnel interface goes Up, the system dynamically refreshes the MTU value of the tunnel interface based on the Path_MTU of the tunnel and IPv6 MTU of the tunnel outbound interface. If the Path_MTU does not exist, the system adopts the MTU of the tunnel outbound interface as the MTU of the tunnel interface.

On a network with Ethernet over GRE tunnels, the MTU configured on a tunnel interface takes effect for Layer 3 traffic but not Layer 2 traffic.

The **mtu** *mtu* command configuration on a TE tunnel interface takes effect for packets sent by hosts only in the following scenarios:

- In an L3VPN over TE scenario, if the length of a packet that a host sends exceeds the configured MTU value, the packet is fragmented based on the MTU value at the IP layer before being forwarded.
- In a TE tunnel scenario, the length of a tunnel detection packet must be less than the configured MTU value.

Example

Set the MTU of Tunnel 0/0/1 to 1492.

```
<Huawei> system-view
[Huawei] interface tunnel 0/0/1
[Huawei-Tunnel0/0/1] mtu 1492
[Huawei-Tunnel0/0/1] shutdown
[Huawei-Tunnel0/0/1] undo shutdown
```

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

12.3.3 display interface tunnel

12.3.15 portswitch (VE interface view)

Function

The **portswitch** command changes the working mode of a virtual Ethernet (VE) interface from Layer 3 mode to Layer 2 mode.

The **undo portswitch** command changes the working mode of a VE interface from Layer 2 mode to Layer 3 mode.

By default, a VE interface works in Layer 3 mode.

Format

portswitch

undo portswitch

Parameters

None.

Views

VE interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

By default, a VE interface on the device works in Layer 3 mode. To enable Layer 2 forwarding on the VE interface, run the **portswitch** command to change the working mode to Layer 2 mode.

Precautions

- The command cannot be executed on an interface that has any other configurations except attributes. Delete these configurations before you run this command.
- After changing the working mode of a VE interface, wait at least 30 seconds if you want to change the working mode again.

Example

Change VE0/0/1 to Layer 2 mode.

```
<Huawei> system-view
[Huawei] interface virtual-ethernet 0/0/1
[Huawei-Virtual-Ethernet0/0/1] portswitch
```

 Copyright © Huawei Technologies Co., Ltd.

12.3.16 qos pre-classify

Function

The **qos pre-classify** command enables pre-extraction of original IP packets.

The **undo qos pre-classify** command disables pre-extraction of original IP packets.

By default, pre-extraction of original IP packets is disabled.

Format

qos pre-classify

undo qos pre-classify

Parameters

None

Views

Tunnel interface view, Efficient VPN policy view, Manual IPSec policy view, IPSec policy view, IPSec policy template view, IPSec profile view, GDOI policy view, BD view, VBDIF interface view, VPN instance view, Virtual template interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In tunnel mode, QoS parameters such as the packet header and protocol type in original packets are hidden after IP packets are encapsulated through GRE, VXLAN, L2TP, and IPSec. Although GRE, VXLAN, L2TP, and IPSec uses the DSCP field in original packets as the DSCP field in the IP packet header, some QoS solutions require quintuple information. The encryption device can pre-extract quintuple information including the source address, destination address, protocol type, source port number, and destination port number to facilitate refined QoS management on GRE, VXLAN, L2TP, and IPSec packets.

In an A2A VPN solution, the device uses the IP header of original packets as the IP header for encapsulated A2A VPN packets. Therefore, you do not need to configure this command if the device classifies packets based on the source address, destination address, or protocol type only.

Follow-up Procedure

After pre-extraction of original IP packets is enabled, run the **if-match acl** { *acl-number* | *acl-name* } command in the traffic classifier view to configure a matching rule based on the ACL.

 Copyright © Huawei Technologies Co., Ltd.

Example

Enable pre-extraction of original IP packets in the IPSec policy view.

```
<Huawei> system-view
[Huawei] ipsec policy policy1 10 isakmp
[Huawei-ipsec-policy-isakmp-policy1-10] qos pre-classify
```

Related Topics

12.6.104 ipsec policy (interface view)

12.6.106 ipsec policy-template

12.6.107 ipsec profile (interface view)

12.6.98 ipsec efficient-vpn (system view)

12.3.17 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

 Copyright © Huawei Technologies Co., Ltd.

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

Example

Reset the Keepalive packet statistics of GRE tunnel interface 0/0/1.

```
<Huawei> system-view
[Huawei] interface tunnel 0/0/1
[Huawei-Tunnel0/0/1] tunnel-protocol gre
[Huawei-Tunnel0/0/1] reset keepalive packets count
 Info: Succeeded in resetting tunnel keepalive packets count.
```

Related Topics

12.3.11 keepalive

12.3.4 display keepalive packets count

12.3.18 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 { [**vpn-instance** *vpn-instance-name*] *source-ip-address* | *interface-type interface-number* }

undo source

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Specifies the name of the VPN instance that the source address of a tunnel belongs to. **NOTE** You can specify the parameter only when the encapsulation mode of a tunnel interface is set to IPSec or mGRE.	The value is the name of an existing VPN instance.

 Copyright © Huawei Technologies Co., Ltd.

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.	-

Views

Tunnel interface view, Tunnel-Template interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When configuring a tunnel, you must 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, IPSec, 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.

IPv6 over IPv4, IPv4 over IPv6, and GRE tunnels are bidirectional tunnels. The source address of the local tunnel interface is the destination address of the remote tunnel interface by the **destination** command, and the destination address of the local tunnel interface is the source address of the remote tunnel interface.

Two or more tunnel interfaces that use the same encapsulation protocol cannot be configured with the same source and destination addresses. Two or more GRE tunnel interfaces in a system can have the same source address and same destination address. The system uses GRE keys to identify these GRE tunnel interfaces. When two or more tunnel interfaces on a P2MP tunnel are configured

 Copyright © Huawei Technologies Co., Ltd.

with the same source address, run the **gre key** command to set the key number of each tunnel interface.

You can also specify VPN instance parameters while specifying the source address for an IPSec tunnel or an mGRE tunnel in IPSec/mGRE over VPN scenarios.

Example

Set the tunnel type of Tunnel0/0/1 to IPv6 over IPv4 manual tunnel and configure the source IP address of Tunnel0/0/1 as 10.1.1.1.

```
<Huawei> system-view
[Huawei] interface tunnel 0/0/1
[Huawei-Tunnel0/0/1] tunnel-protocol ipv6-ipv4
[Huawei-Tunnel0/0/1] source 10.1.1.1
```

Configure Tunnel0/0/2 of mGRE and use Loopback0 address as the interface address.

```
<Huawei> system-view
[Huawei] interface loopback 0
[Huawei-LoopBack0] ip address 10.2.1.1 32
[Huawei-LoopBack0] quit
[Huawei] interface tunnel 0/0/2
[Huawei-Tunnel0/0/2] tunnel-protocol gre p2mp
[Huawei-Tunnel0/0/2] source loopback 0
```

12.3.19 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 { **inbound** | **outbound** }

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

Parameters

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

Views

Tunnel interface view

 Copyright © Huawei Technologies Co., Ltd.

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.

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 0/0/1
[Huawei-Tunnel0/0/1] statistic enable inbound
```

Related Topics

12.3.3 display interface tunnel

12.3.20 tunnel route-via

Function

The **tunnel route-via** command specifies the routing outbound interface for a GRE tunnel or mGRE tunnel.

The **undo tunnel route-via** command restores the default configuration.

By default, a GRE tunnel or mGRE tunnel does not have a routing outbound interface.

Format

tunnel route-via *interface-type interface-number* { **mandatory** | **preferred** }

undo tunnel route-via *interface-type interface-number* { **mandatory** | **preferred** }

Parameters

Parameter	Description	Value
interface-type interface-number	Specifies the type and number of an interface.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
mandatory	Configures traffic to be strictly forwarded through the specified routing outbound interface.	-
preferred	Configures traffic to be preferentially forwarded through the specified routing outbound interface.	-

Views

Tunnel interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

GRE packets are forwarded based on routing tables. If there are multiple equal-cost routes to the destination address, GRE packets are shared among these routes. In some situations, the actual routing outbound interface of GRE packets transmitted over a GRE tunnel may be the routing outbound interface for another GRE tunnel. If Unicast Reverse Path Forwarding (URPF) is enabled on the next hop device, this device checks the source addresses of these GRE packets to identify their outbound interface and then determines whether the outbound interface for these packets are the same as the actual interface that receives these packets. After the device finds that the outbound interface for these packets is different from the actual interface that receives these packets, the device drops these packets. To solve this problem, run the **tunnel route-via** command to specify the routing outbound interface for each GRE tunnel.

If multiple equal-cost routes exist between a Spoke or Hub site and the GRE tunnel destination address for an mGRE tunnel but you want GRE packets to be forwarded through a specified physical outbound interface, run the **tunnel route-via** command in the mGRE tunnel interface view to specify the routing outbound interface.

Prerequisites

The **tunnel-protocol gre** command has been run in the tunnel interface view.

Configuration Impact

If you configure **mandatory** when running the **tunnel route-via** command, traffic is strictly forwarded through the specified routing outbound interface. Specifically, if the available routing outbound interfaces for GRE packets transmitted over a GRE tunnel do not include the routing outbound interface specified for the tunnel, packets cannot be forwarded. The mGRE tunnel status is not affected. If you configure **preferred** when running the **tunnel route-via** command, traffic is preferentially forwarded through the specified routing outbound interface. Specifically, if the available routing outbound interfaces for GRE packets transmitted over a GRE or mGRE tunnel do not include the routing outbound interface specified for the tunnel, packets can still be forwarded through available routing outbound interfaces.

 Copyright © Huawei Technologies Co., Ltd.

Example

Specify the routing outbound interface for a GRE tunnel and configure traffic to be strictly forwarded through the specified interface.

```
<Huawei> system-view
[Huawei] interface Tunnel 0/0/1
[Huawei-Tunnel0/0/1] tunnel-protocol gre
[Huawei-Tunnel0/0/1] tunnel route-via GigabitEthernet 0/0/1 mandatory
```

Related Topics

12.3.10 interface tunnel

12.3.21 tunnel-protocol

12.3.21 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** [**p2mp**] | **ipsec** | **ipv6-ipv4** [**6to4** | **auto-tunnel** | **isatap**] | **ipv4-ipv6** | **mpls te** | **svpn** [**p2p** | **p2mp**] | **none** }

undo tunnel-protocol

Parameters

Parameter	Description	Value
gre	Indicates that the GRE tunnel protocol is configured on a tunnel interface.	-
gre p2mp	Indicates that the mGRE tunnel protocol is configured on a tunnel interface. If this parameter is not used, the tunnel protocol configured on a tunnel interface is a traditional point-to-point GRE.	-
ipsec	Indicates that the IPSec tunnel protocol is configured on a tunnel interface.	-
ipv4-ipv6	Indicates that the IPv4 to IPv6 tunnel protocol is configured on a tunnel interface.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
ipv6-ipv4	Configures the tunnel protocol of the tunnel interface as ipv6-ipv4 and uses a manual IPv6 over IPv4 tunnel.	-
ipv6-ipv4 6to4	Indicates that the IPv6 to IPv4 tunnel protocol is configured on a tunnel interface using 6to4.	-
ipv6-ipv4 auto-tunnel	Configures the tunnel protocol of the tunnel interface as ipv6-ipv4 and uses an automatic IPv6 over IPv4 tunnel.	-
ipv6-ipv4 isatap	Indicates that the IPv6 to IPv4 tunnel protocol is configured on a tunnel interface using isatap.	-
mpls te	Indicates that the MPLS TE tunnel protocol is configured on a tunnel interface. **NOTE** The AR100&AR120&AR150&AR160&AR200 does not support this parameter.	-
svpn [**p2p** | **p2mp**]	Indicates that the SVPN tunnel protocol is configured on a tunnel interface. • **p2p**: indicates the P2P SVPN tunnel protocol. • **p2mp**: indicates the P2MP SVPN tunnel protocol.	-
none	Indicates that no tunnel protocol is configured on a tunnel interface.	-

Views

Tunnel interface view, Tunnel-Template interface view

NOTE

The tunnel template interface view supports the **ipsec** and **none** parameters only.

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:

 Copyright © Huawei Technologies Co., Ltd.

- 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. When the **p2mp** parameter is specified following **gre**, you can set the tunnel encapsulation mode to P2MP GRE. The destination address of a P2MP GRE tunnel does not need to be manually configured. Instead, the destination address of this tunnel can either be defined by a protocol (for example, NHRP in a DSVPN scenario) or be dynamically learned.
- IPSec: protects the security of data transmitted on the Internet by establishing tunnels using the IPSec protocol.
- 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.
- SVPN: binds multiple WAN access lines to provide high bandwidth and highly reliable networks for customers.
  - When the SVPN mode is set to Hub-Spoke, specify **p2p** on the Spoke and **p2mp** on the hub when configuring a tunnel protocol.
  - When the SVPN mode is set to Lone Ranger, you must not specify **p2p** or **p2mp**.

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. When an SVPN proposal is bound to a tunnel interface, you cannot modify the tunnel encapsulation mode.

Example

Set the tunnel encapsulation mode of Tunnel0/0/2 to mGRE.

```
<Huawei> system-view
[Huawei] interface tunnel 0/0/2
[Huawei-Tunnel0/0/2] tunnel-protocol gre p2mp
```

Set the tunnel encapsulation mode of Tunnel0/0/2 to GRE.

```
<Huawei> system-view
[Huawei] interface tunnel 0/0/2
[Huawei-Tunnel0/0/2] tunnel-protocol gre
```

Related Topics

12.3.10 interface tunnel

 Copyright © Huawei Technologies Co., Ltd.

12.4 SVPN Configuration Commands

NOTE

The feature is just for beta test, and is not for commercial use. If the feature is required in the test, contact Huawei technical support personnel.

12.4.1 authentication

Function

The **authentication** command configures the user name and password for authentication in Hub-Spoke mode.

The **undo authentication** command cancels the user name and password.

By default, no user name or password is configured.

Format

authentication user-name *user-name* **password cipher** *cipher-string*

undo authentication

Parameters

Parameter	Description	Value
user-name *user-name*	Specifies a user name for authentication.	The value is a string of 1 to 32 case-sensitive characters without spaces.
password cipher *cipher-string*	Specifies the authentication password in cipher text.	The value is a string of case-sensitive characters without spaces. It can contain 1 to 16 characters in plain text or 32or 48 characters in cipher text.

Views

SVPN proposal view

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

To improve security in Hub-Spoke mode, two communicating parties authenticate each other before establishing an SVPN tunnel between them. An SVPN tunnel can be established only after the two parties pass authentication.

Example

Set the authentication user name and password to **Huawei** and **Huawei@1234**.

```
<Huawei> system-view
[Huawei] svpn-proposal p1
[Huawei-svpn-proposal-p1] authentication user-name Huawei password cipher Huawei@1234
```

12.4.2 cmi-method (service view)

Function

The **cmi-method** command configures a composite measure indicator (CMI) calculation formula for the service flow forwarding path.

The **undo cmi-method** command restores the default configuration.

By default, the CMI calculation formula is CMI = 9000 - (D + J + L), where, D presents the delay; J presents the jitter; L represents the packet loss rate.

Format

cmi-method *cmi-method-formula*

undo cmi-method

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
cmi-method-formula	Specifies the CMI calculation formula. • The CMI calculation formula is CMI = 9000 - *cmi-method*. You can define how *cmi-method* is calculated based on service requirements, and the default value is D + J + L. • In the CMI calculation formula, if there is a coefficient before D, J, or L, the product of D, J, or L and the coefficient must be smaller than or equal to 5000, 3000, and 1000 respectively. If the product is larger than the maximum values (5000, 3000, and 1000), the maximum values are used. For example, when the formula CMI = 9000 - (10 x D + 10 x J + 10 x L) is used, and the D, J, and L are 1000 ms, 100 ms, and 10‰ respectively, the CMI is calculated as follows: CMI = 9000 - (5000 + 1000 + 100) = 2900. This is because 10 x D is 10000, which exceeds the maximum value 5000 and can only be calculated as 5000.	The value is a string of 1 to 20 characters. The value contains only digits, plus sign (+), asterisk (*), slash (/), and letters (D, d, L, l, J, or j). Only the plus operator (+) can be used among parameters D, J, and L. These parameters can be multiplied or divided by a positive integer. For example: • 10 x D • D x 10 + J/10 • D x 100 + J x 10 + L/10 **NOTE** D or d indicates the delay; J or j indicates the jitter; and L or l indicates the packet loss rate.

Views

Service view

 Copyright © Huawei Technologies Co., Ltd.

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can run this command to customize the CMI calculation formula based on service requirements. SVPN determines link quality based on the CMI value and selects an optimal link to forward service data.

Precautions

After an SVPN proposal is bound to an SVPN tunnel interface, you need to unbind the SVPN proposal from the interface if you want to modify the CMI calculation formula for the service flow forwarding path.

Example

Set the CMI calculation formula for the service flow forwarding path to CMI = 9000 - (D + J).

```
<Huawei> system-view
[Huawei] svpn-proposal p1
[Huawei-svpn-proposal-p1] service s1 id 1
[Huawei-svpn-proposal-p1-service-s1] cmi-method d+j
```

Related Topics

12.4.3 cmi-threshold (service view)

12.4.3 cmi-threshold (service view)

Function

The **cmi-threshold** command configures a composite measure indicator (CMI) threshold for the service flow forwarding path.

The **undo cmi-threshold** command restores the default configuration.

By default, the CMI, delay, jitter, and packet loss rate thresholds are 0, 5000 ms, 3000 ms, and 1000‰ respectively.

Format

cmi-threshold { **cmi** *cmi-threshold-value* | **delay** *delay-threshold-value* | **jitter** *jitter-threshold-value* | **loss** *loss-threshold-value* } *

undo cmi-threshold

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
cmi *cmi-threshold-value*	Specifies a CMI threshold for a service flow forwarding path.	The value is an integer that ranges from 0 to 9000.
delay *delay-threshold-value*	Specifies a delay threshold for a service flow forwarding path.	The value is an integer that ranges from 0 to 5000, in milliseconds.
jitter *jitter-threshold-value*	Specifies a jitter threshold for a service flow forwarding path.	The value is an integer that ranges from 0 to 3000, in milliseconds.
loss *loss-threshold-value*	Specifies a packet loss rate threshold for a service flow forwarding path.	The value is an integer that ranges from 0 to 1000, in ‰.

Views

Service view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

- CMI is the composite measure indicator of a link. Many services have requirements for link delay, jitter, and packet loss rate. Therefore, users need to configure the correct CMI calculation formula according to service requirements and use the **cmi-threshold** command set the CMI threshold. When the calculated CMI value is lower than the configured CMI threshold, SVPN determines that the link CMI does not meet service requirements.
- The service delay threshold is the maximum service delay allowed by services on a link. If services require a short delay, this threshold needs to be set.
- The service jitter threshold is the maximum service jitter allowed by services on a link. If services require a low jitter, this threshold needs to be set.
- The packet loss rate threshold is the maximum packet loss rate allowed by services on a link. If services require a low packet loss rate, this threshold needs to be set.

If either of the following occurs, the path does not meet the requirement.

- The CMI value calculated using the CMI calculation formula is smaller than the configured CMI threshold.
- The path delay is larger than the configured delay threshold.

 Copyright © Huawei Technologies Co., Ltd.

- The path jitter is larger than the configured delay threshold.
- The packet loss rate value of a path is larger than the configured packet loss rate threshold.

Precautions

After an SVPN proposal is bound to an SVPN tunnel interface, you need to unbind the SVPN proposal from the interface if you want to modify the CMI threshold for the service traffic forwarding path.

If you run the **cmi-threshold** command multiple times, only the latest configuration takes effect.

Example

Set the CMI threshold for an SVPN service flow forwarding path to 7000.

```
<Huawei> system-view
[Huawei] svpn-proposal p1
[Huawei-svpn-proposal-p1] service s1 id 1
[Huawei-svpn-proposal-p1-service-s1] cmi-threshold cmi 7000
```

Related Topics

12.4.2 cmi-method (service view)

12.4.4 encapsulation (SVPN proposal view)

Function

The **encapsulation** command configures the encapsulation type for SVPN packets.

The **undo encapsulation** command restores the default configuration.

By default, the encapsulation type of SVPN packets is NULL.

Format

encapsulation gre

undo encapsulation

Parameters

Parameter	Description	Value
gre	Specifies the GRE encapsulation type for packets.	-

Views

SVPN proposal view

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

You do not need to set the encapsulation type for SVPN packets to GRE when the device works in Lone Ranger mode. If the encapsulation type is set to GRE, you need to configure the SVPN function on the peer device and configure the peer device to work in Lone Ranger mode. Otherwise, service flows cannot be transmitted between the two devices.

In Hub-Spoke mode, you can use either of the following methods to set the encapsulation type for SVPN packets to GRE:

- Run the **encapsulation** command to set the encapsulation type for SVPN packets to GRE. Packets on all service flow forwarding paths in the SVPN proposal use the GRE encapsulation type. If you want to set the GRE encapsulation type for packets on some service flow forwarding paths, use the following method.
- Specify the **encapsulation gre** parameter when you run the **source (SVPN proposal view)** command to configure a forwarding path for the service flow. In this way, the encapsulation type for packets on the specified forwarding path is set to GRE.

Example

Set the encapsulation type for SVPN packets to GRE.

```
<Huawei> system-view
[Huawei] svpn-proposal p1
[Huawei-svpn-proposal-p1] encapsulation gre
```

Related Topics

12.4.6 svpn-proposal (system view)

12.4.5 destination (SVPN proposal view)

Function

The **destination** command configures the destination address for a service flow forwarding path.

The **undo destination** command deletes the destination address of a service flow forwarding path.

By default, no destination address is configured for a service flow forwarding path.

Format

destination *dest-ip-address*

undo destination

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
dest-ip-address	Specifies a destination address for a service flow forwarding path.	The value is in dotted decimal notation.

Views

SVPN proposal view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After an SVPN proposal is created, you need to configure service flow forwarding paths for the SVPN proposal to direct packet forwarding. You can use the following methods to configure a service flow forwarding path.

- Run the **source** { [**vpn-instance** *vpn-instance-name*] *source-ip-address* | *interface-type interface-number* } **destination** *dest-ip-address* { **bandwidth** { { **up** *bw-value* | **down** *bw-value* } * | *bw-value* } | **encapsulation gre** | **track nqa** *admin-name test-name* } * command to configure the source address/ interface and destination address for a service flow forwarding path.
- Run the **source** { [**vpn-instance** *vpn-instance-name*] *source-ip-address* | *interface-type interface-number* } { **bandwidth** { { **up** *bw-value* | **down** *bw-value* } * | *bw-value* } | **encapsulation gre** | **track nqa** *admin-name test-name* } * or **source** { [**vpn-instance** *vpn-instance-name*] *source-ip-address* | *interface-type interface-number* } command to configure the source address or source interface for a service flow forwarding path, and then run the **destination** *dest-ip-address* command to configure the destination address for the path.

Precautions

If you configure a service flow forwarding path using the **source (service view)** command without **destination** *dest-ip-address* specified or the **source (SVPN proposal view)** command, you must run the this command to configure the destination address for the path. Otherwise, the path cannot be used to forward SVPN packets.

Example

Set the destination address of a service flow forwarding path to 2.2.2.9.

```
<Huawei> system-view
[Huawei] svpn-proposal p1
[Huawei-svpn-proposal-p1] destination 2.2.2.9
```

Related Topics

12.4.6 svpn-proposal (system view)

 Copyright © Huawei Technologies Co., Ltd.

12.4.14 source (SVPN proposal view)
12.4.15 source (service view)

12.4.6 svpn-proposal (system view)

Function

The **svpn-proposal** command creates an SVPN proposal and enters the SVPN proposal view.

The **undo svpn-proposal** command deletes an SVPN proposal.

By default, no SVPN proposal is created on the device.

Format

svpn-proposal *svpn-proposal-name*

undo svpn-proposal *svpn-proposal-name*

Parameters

Parameter	Description	Value
svpn-proposal-name	Specifies the name of an SVPN proposal.	The value is a string of 1 to 31 case-sensitive characters without spaces or hyphens (-). 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

SVPN binds multiple WAN access lines to provide high bandwidth and highly reliable networks for customers. When the SVPN function is required, you can run this command to create an SVPN proposal.

Precautions

After you run the **undo svpn-proposal** command to delete an SVPN proposal, all configurations in the SVPN proposal are deleted.

Follow-up Procedure

After creating an SVPN proposal, you need to perform a series of configurations for the SVPN proposal. The mandatory operations are as follows:

 Copyright © Huawei Technologies Co., Ltd.

- Creating an SVPN service: Only after you run the **service (SVPN proposal view)** command to create an SVPN service, you can set other parameters for the service. The parameters include the forwarding path and scheduling mode for a service flow, and the packet matching mode.
- Binding an SVPN proposal to an SVPN tunnel interface: Run the **svpn-proposal (tunnel interface view)** command to bind an SVPN proposal to an SVPN tunnel interface. After the SVPN proposal is bound to a tunnel interface, packets received by this interface are forwarded along the path for SVPN service packets.

Example

Create an SVPN proposal **p1**.

```
<Huawei> system-view
[Huawei] svpn-proposal p1
[Huawei-svpn-proposal-p1]
```

Related Topics

12.4.7 svpn-proposal (tunnel interface view)

12.4.7 svpn-proposal (tunnel interface view)

Function

The **svpn-proposal** command binds an SVPN proposal to an SVPN tunnel interface.

The **undo svpn-proposal** command unbinds an SVPN proposal from an SVPN tunnel interface.

By default, no SVPN proposal is bound to a tunnel interface.

Format

svpn-proposal *svpn-proposal-name*

undo svpn-proposal *svpn-proposal-name*

Parameters

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

Views

Tunnel interface view

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

Usage Scenario

After an SVPN proposal is created, you need to bind the SVPN proposal to an SVPN tunnel interface. After the SVPN proposal is bound to a tunnel interface, packets received by this interface are forwarded along the path for SVPN service packets.

Prerequisite

An SVPN proposal has been created by using the **svpn-proposal (system view)** command and the tunnel protocol type has been set to SVPN by using the **tunnel-protocol svpn** [**p2p** | **p2mp**] command.

Precautions

One SVPN proposal can be bound to only one tunnel interface. If you want to bind the SVPN proposal to another tunnel interface, unbind the SVPN proposal from the previous tunnel interface first.

All configurations in the SVPN proposal that has been bound to an SVPN tunnel interface cannot be modified. To modify the configurations, unbind the SVPN proposal from the tunnel interface.

Example

Bind the SVPN proposal **p1** to Tunnel0/0/1.

```
<Huawei> system-view
[Huawei] acl 3000
[Huawei-acl-adv-3000] rule 5 permit ip
[Huawei-acl-adv-3000] quit
[Huawei] svpn-proposal p1
[Huawei-svpn-proposal-p1] encapsulation gre
[Huawei-svpn-proposal-p1] source 1.1.1.9 destination 2.2.2.9 bandwidth 1024
[Huawei-svpn-proposal-p1] service s1 id 1
[Huawei-svpn-proposal-p1-service-s1] schedule-type overflow
[Huawei-svpn-proposal-p1-service-s1] match acl 3000
[Huawei-svpn-proposal-p1-service-s1] source 1.1.1.9
[Huawei-svpn-proposal-p1-service-s1] quit
[Huawei-svpn-proposal-p1] quit
[Huawei] interface tunnel 0/0/1
[Huawei-Tunnel0/0/1] tunnel-protocol svpn p2p
[Huawei-Tunnel0/0/1] svpn-proposal p1
```

Related Topics

12.4.6 svpn-proposal (system view)

12.4.8 svpn-zone

Function

The **svpn-zone** command configures an SVPN zone for a tunnel interface.

The **undo svpn-zone** command restores the default configuration.

By default, a tunnel interface belongs to SVPN zone 0.

 Copyright © Huawei Technologies Co., Ltd.

Format

svpn-zone *zone-number*

undo svpn-zone

Parameters

Parameter	Description	Value
zone-number	Specifies an SVPN zone.	The value is an integer that ranges from 1 to 1000. The default value is 0.

Views

Tunnel interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When multiple SVPN tunnel interfaces are configured on a device in an SVPN scenario, you need to run this command to configure different SVPN zones for these interfaces to ensure proper data forwarding.

Prerequisite

The tunnel protocol type has been set to SVPN by using the **tunnel-protocol** command.

Precautions

After an SVPN proposal is bound to a tunnel interface, you cannot modify the SVPN zone of the interface. To modify the SVPN zone of the interface, unbind the SVPN proposal from the interface first.

The SVPN zones of SVPN tunnel interfaces on a device must differ from one another, regardless of whether the device works in Lone Ranger or Hub-Spoke mode. If the device works in Hub-Spoke mode, the Hub and Spoke devices must be configured with the same SVPN zone. If the device works in Lone Ranger mode and uses the GRE encapsulation type, the connected devices must be configured with the same SVPN zone.

Example

Set the SVPN zone of Tunnel0/0/1 to 1.

```
<Huawei> system-view
[Huawei] interface tunnel 0/0/1
[Huawei-Tunnel0/0/1] tunnel-protocol svpn
[Huawei-Tunnel0/0/1] svpn-zone 1
```

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

12.4.6 svpn-proposal (system view)

12.4.9 match (service view)

Function

The **match** command configures an ACL rule or an application protocol type for matching service flows.

The **undo match** command deletes an ACL rule or an application protocol type for matching service flows.

By default, service flows do not match any rule.

Format

match { **acl** *acl-number* | **application** *protocol-name* }

undo match { **acl** *acl-number* | **application** *protocol-name* }

Parameters

Parameter	Description	Value
acl *acl-number*	Indicates that the device matches service flows by ACL rule.	The value is an integer that ranges from 2000 to 3999.
application *protocol-name*	Indicates that the device matches service flows by application protocol type.	The value is a character string without spaces and varies with the feature library.

Views

Service view

Default Level

2: Configuration level

Usage Guidelines

SVPN distinguishes different service flows by matching ACL rules or application protocol types.

If no matching ACL rule or application protocol type is configured for SVPN service flows, all the service flows sent to the SVPN tunnel interface can be forwarded. SVPN randomly selects an available forwarding path.

Example

Distinguish the service flow **s1** by matching the ACL rule 3000.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> system-view
[Huawei] acl number 3000
[Huawei-acl-adv-3000] rule 5 permit ip
[Huawei-acl-adv-3000] quit
[Huawei] svpn-proposal p1
[Huawei-svpn-proposal-p1] service s1 id 1
[Huawei-svpn-proposal-p1-service-s1] match acl 3000
```

Related Topics

12.4.13 service (SVPN proposal view)

12.4.10 recovery-delay

Function

The **recovery-delay** command configures the delay for switching a service flow between forwarding paths when the scheduling mode is Priority.

The **undo recovery-delay** command restores the default configuration.

By default, the delay for switching a service flow between forwarding paths is 5s.

Format

recovery-delay *delay-time*

undo recovery-delay

Parameters

Parameter	Description	Value
delay-time	Specifies the switching delay.	The value is an integer that ranges from 0 to 30000, in seconds. The default value is 5s.

Views

SVPN proposal view

Default Level

2: Configuration level

Usage Guidelines

In an SVPN scenario, when the scheduling mode is set to Priority, the device usually switches a service flow to the optimal path in 5seconds when it detects that a better path is available. When a network is unstable, the service flow may be frequently switched between different paths, resulting in data loss. You can run this command to set an appropriate switching delay.

Example

Set the delay for switching service flow between forwarding paths to 60s.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> system-view
[Huawei] svpn-proposal p1
[Huawei-svpn-proposal-p1] recovery-delay 60
```

Related Topics

12.4.6 svpn-proposal (system view)

12.4.11 reorder-window

Function

The **reorder-window** command configures the size of the receive or transmit buffer for SVPN packets.

The **undo reorder-window** command restores the default configuration.

By default, the size of the receive or transmit buffer for SVPN packets is 64.

Format

reorder-window *window-size*

undo reorder-window

Parameters

Parameter	Description	Value
window-size	Specifies the size of the receive or transmit buffer for SVPN packets.	The value is an integer, which can be 32, 64, or 128.

Views

SVPN proposal view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When SVPN binds multiple WAN access lines and the scheduling mode for a service flow is set to Overflow, packets in the service flow may be forwarded through multiple paths. As a result, the receiver end may receive mis-sequencing packets, leading to communication quality deterioration. You can run this command to adjust the size of the receive or transmit buffer for SVPN packets to reduce packet mis-sequencing.

Precautions

You are advised to specify the *window-size* parameter under the supervision of the technical support personnel.

 Copyright © Huawei Technologies Co., Ltd.

Example

Set the size of the receive or transmit buffer for SVPN packets to 128.

```
<Huawei> system-view
[Huawei] svpn-proposal p1
[Huawei-svpn-proposal-p1] reorder-window 128
```

Related Topics

12.4.6 svpn-proposal (system view)

12.4.12 schedule-type (service view)

Function

The **schedule-type** command configures a mode for scheduling a service flow to one or more forwarding paths.

The **undo schedule-type** command deletes the mode for scheduling a service flow to one or more forwarding paths.

By default, no mode is configured for scheduling a service flow.

Format

schedule-type { **overflow** | **priority** }

undo schedule-type

Parameters

Parameter	Description	Value
overflow	Indicates that a service flow is scheduled based on the path bandwidth.	-
priority	Indicates that a service flow is scheduled based on the path priority.	-

Views

Service view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To configure the SVPN function, the device needs to distinguish different types of service flows. Multiple forwarding paths may be available for one type of service flow. You can run this command to configure a mode for scheduling a service flow to one or more forwarding paths.

 Copyright © Huawei Technologies Co., Ltd.

- Overflow mode: The device schedules the service flow based on the path bandwidth. Packets of one service flow can be transmitted over different paths. If the bandwidth of the first available path is occupied, packets are scheduled to a second available path, and so on.

  You can run the **source index (service view)** command to manually sequence the paths.
- Priority mode: The device schedules the service flow based on the path priority. Packets of one service flow can be transmitted over only one optimal path. When selecting the optimal path, the device calculates forwarding paths that meet the criteria using link detection (associated NQA instances or the default link quality measurement method) and then selects the first available path from these paths.

  Multiple forwarding paths may meet the link quality criteria. To select the first available path from these paths, run the **source index (service view)** command to manually sequence the paths.

Precautions

Ensure that the **schedule-type** command is configured in the service view before you bind an SVPN proposal to an SVPN tunnel interface. After an SVPN proposal is bound to an SVPN tunnel interface, you need to unbind the SVPN proposal from the interface if you want to modify the mode for scheduling a service flow.

Example

Set the mode for scheduling a service flow to Overflow.

```
<Huawei> system-view
[Huawei] svpn-proposal p1
[Huawei-svpn-proposal-p1] service s1 id 1
[Huawei-svpn-proposal-p1-service-s1] schedule-type overflow
```

Related Topics

12.4.13 service (SVPN proposal view)

12.4.13 service (SVPN proposal view)

Function

The **service** command creates an SVPN service and displays the service view.

The **undo service** command deletes an SVPN service.

By default, no SVPN service is created.

Format

service *service-name* [**id** *service-id*]

undo service *service-name*

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
service-name	Specifies the name of an SVPN service.	The value is a string of 1 to 31 case-sensitive characters without spaces or hyphens (-). The total length of the names of the SVPN service and SVPN proposal must be within 56 case-sensitive characters.
id *service-id*	Specifies the ID of an SVPN service.	The value is an integer that ranges from 1 to 8.

Views

SVPN proposal view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After an SVPN service is created, you can configure other parameters for the SVPN service to implement the SVPN function. The parameters include the forwarding path and scheduling mode for a service flow, and the packet matching mode.

Precautions

You must specify the **id** parameter when you create an SVPN service for the first time. The SVPN service ID is unique in an SVPN proposal and the created service ID cannot be modified.

After an SVPN service is created, you do not need to specify the **id** parameter in the service view.

If the device works in Hub-Spoke mode, the Hub and Spoke devices must be configured with the same *service-id*.

Example

Create an SVPN service named **s1** with the ID 1.

```
<Huawei> system-view
[Huawei] svpn-proposal p1
[Huawei-svpn-proposal-p1] service s1 id 1
[Huawei-svpn-proposal-p1-service-s1]
```

Related Topics

12.4.6 svpn-proposal (system view)

 Copyright © Huawei Technologies Co., Ltd.

12.4.14 source (SVPN proposal view)

Function

The **source** command configures one or more forwarding paths for a service flow.

The **undo source** command deletes the forwarding paths of a service flow.

By default, no forwarding path is configured for a service flow.

Format

source { [**vpn-instance** *vpn-instance-name*] *source-ip-address* | *interface-type interface-number* } [**destination** *dest-ip-address*] { { **bandwidth** { { **up** *bw-value* | **down** *bw-value* } * | *bw-value* } | **encapsulation gre** | **track nqa** *admin-name test-name* } *

undo source { [**vpn-instance** *vpn-instance-name*] *source-ip-address* | *interface-type interface-number* }

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Specifies the name of the VPN instance to which the specified source address belongs.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
source-ip-address	Specifies a source address for a service flow forwarding path.	The value is in dotted decimal notation.
interface-type interface-number	Specifies the type and number of the source interface for a service flow forwarding path. • *interface-type* specifies the interface type. • *interface-number* specifies the interface number.	-
destination *dest-ip-address*	Specifies a destination address for a service flow forwarding path.	The value is in dotted decimal notation.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
bandwidth { { **up** *bw-value* | **down** *bw-value* } * | *bw-value* }	Specifies the link bandwidth of a forwarding path. • **up**: indicates the uplink bandwidth. • **down**: indicates the downlink bandwidth. • If neither **up** or **down** is specified, this parameter indicates the uplink bandwidth and downlink bandwidth. **NOTE** If this parameter is not specified, the bandwidth of the forwarding path is equal to the actual physical bandwidth of the source interface.	The value is an integer that ranges from 0 to 4000000000, in kbit/s.
encapsulation gre	Specifies the GRE encapsulation type for packets on a forwarding path.	-
track nqa *admin-name test-name*	Specifies the name of the administrator of the NQA test instance and the name of the test instance associated with a service flow forwarding path. **NOTE** If this parameter is not specified, the default link quality measurement method is used to calculate the delay and packet loss rate of the forwarding path.	The value of *admin-name* or *test-name* is a string of 1 to 32 case-sensitive characters without spaces.

Views

SVPN proposal view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After an SVPN proposal is created, you need to configure service flow forwarding paths for the SVPN proposal to direct packet forwarding. You can use the following methods to configure a service flow forwarding path.

- Run the **source** { [**vpn-instance** *vpn-instance-name*] *source-ip-address* \| *interface-type interface-number* } **destination** *dest-ip-address* { **bandwidth** { { **up** *bw-value* \| **down** *bw-value* } * \| *bw-value* } \| **encapsulation gre** \| **track**

 Copyright © Huawei Technologies Co., Ltd.

nqa *admin-name test-name* } * command to configure the source address/interface and destination address for a service flow forwarding path.

- Run the **source** { [**vpn-instance** *vpn-instance-name*] *source-ip-address* | *interface-type interface-number* } { **bandwidth** { { **up** *bw-value* | **down** *bw-value* } * | *bw-value* } | **encapsulation gre** | **track nqa** *admin-name test-name* } * or **source** { [**vpn-instance** *vpn-instance-name*] *source-ip-address* | *interface-type interface-number* } command to configure the source address or source interface for a service flow forwarding path, and then run the **destination** *dest-ip-address* command to configure the destination address for the path.

After multiple forwarding paths are configured using this command, SVPN supports the following modes for scheduling service flows:

- Overflow mode: The device schedules the service flow based on the path bandwidth. Packets of one service flow can be transmitted over different paths. If the bandwidth of the first available path is occupied, packets are scheduled to a second available path, and so on. You can run the **source index (service view)** command to manually sequence the paths.

  When the Overflow mode is used:

  - You can specify **bandwidth** to configure the bandwidth for a forwarding path. If **bandwidth** is not specified, the actual physical bandwidth of the source interface is used. In practice, SVPN adjusts the bandwidth of the forwarding paths based on the packet loss rate calculated using link detection (associated the default link quality measurement method) in real time to provide a better service.
  - If the link detection result shows that the delay of a second available path is much larger than the delay of the first available path, SVPN does not use this path but searches for another path that meets the link quality requirement.
- Priority mode: The device schedules the service flow based on the path priority. Packets of one service flow can be transmitted over only one optimal path. When this mode is used, SVPN can select a path using either of the following methods:

  - Associate with NQA instances by specifying **track nqa** to calculate forwarding paths that meet the criteria and then select the first available path from these paths.
  - Use the default link quality measurement method to calculate forwarding paths that meet the criteria and then select the first available path from these paths.

  Multiple forwarding paths may meet the link quality criteria. To select the first available path from these paths, run the **source index (service view)** command to manually sequence the paths.

  NOTE

  When this mode is used, the **bandwidth** parameter does not take effect even if it is specified for service flow forwarding path.

Precautions

- A maximum of eight forwarding paths can be created for an SVPN proposal. You can run this command to configure one or more forwarding paths or run

 Copyright © Huawei Technologies Co., Ltd.

the **source (service view)** command to configure a new forwarding path for the SVPN service.

- If you run this command multiple times, the latest configuration for the following parameters overrides the previous configuration. The parameters that are overridden include **destination** *dest-ip-address*, **bandwidth** { { **up** *bw-value* | **down** *bw-value* } * | *bw-value* }, and **track nqa** *admin-name test-name*.
- Generally, the GRE encapsulation type is not required when you configure forwarding paths for a device working in Lone Ranger mode. If the encapsulation type is set to GRE, you need to configure the SVPN function on the peer device and configure the peer device to work in Lone Ranger mode. Otherwise, service flows cannot be transmitted between the two devices. In Hub-Spoke mode, you can use either of the following methods to set the encapsulation type for SVPN packets to GRE:
  - Set the encapsulation type to GRE by specifying the **encapsulation gre** parameter in this command.
  - Run the **encapsulation (SVPN proposal view)** command to set the encapsulation type for SVPN packets to GRE. Packets on all service flow forwarding paths in the SVPN proposal use the GRE encapsulation type. If you want to set the GRE encapsulation type for packets on some service flow forwarding paths, use the first method.
- When you delete a forwarding path that has been referenced by the SVPN service, the forwarding path still exists in the service view as a newly created path.

Example

Configure a forwarding path for the SVPN proposal **p1**, whose source address, destination address, and bandwidth are 1.1.1.9, 2.2.2.9, and 1024 kbit/s respectively.

```
<Huawei> system-view
[Huawei] svpn-proposal p1
[Huawei-svpn-proposal-p1] source 1.1.1.9 destination 2.2.2.9 bandwidth 1024
```

Related Topics

12.4.16 source index (service view)

12.4.15 source (service view)

Function

The **source** command configures one or more service flow forwarding paths for the SVPN service.

The **undo source** command deletes one or more service flow forwarding paths for the SVPN service.

By default, no service flow forwarding path is configured for the SVPN service.

 Copyright © Huawei Technologies Co., Ltd.

Format

source { [**vpn-instance** *vpn-instance-name*] *source-ip-address* | *interface-type interface-number* }

undo source { [**vpn-instance** *vpn-instance-name*] *source-ip-address* | *interface-type interface-number* }

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Specifies the name of the VPN instance to which the specified source address belongs.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
source-ip-address	Specifies a source address for a service flow forwarding path.	The value is in dotted decimal notation.
interface-type interface-number	Specifies the type and number of the source interface for a service flow forwarding path. • *interface-type* specifies the interface type. • *interface-number* specifies the interface number.	-

Views

Service view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After service flow forwarding paths are configured for an SVPN proposal, you can run this command to apply an existing forwarding path to the SVPN service. You can also run this command and the **destination (SVPN proposal view)** command to create a service flow forwarding path for the SVPN service.

Precautions

If you run this command to create a service flow forwarding path, the path uses the default link quality measurement method, actual physical bandwidth of the source interface, and packet encapsulation type configured for the SVPN proposal.

 Copyright © Huawei Technologies Co., Ltd.

Currently, a maximum of eight forwarding paths can be configured for a service flow.

Example

Apply the existing forwarding path with the source address 1.1.1.9, destination address 2.2.2.9, and packet encapsulation type GRE to the SVPN service s1.

```
<Huawei> system-view
[Huawei] svpn-proposal p1
[Huawei-svpn-proposal-p1] source 1.1.1.9 destination 2.2.2.9 encapsulation gre
[Huawei-svpn-proposal-p1] service s1 id 1
[Huawei-svpn-proposal-p1-service-s1] source 1.1.1.9
```

Related Topics

12.4.14 source (SVPN proposal view)

12.4.5 destination (SVPN proposal view)

12.4.16 source index (service view)

Function

The **source index** command adjusts the sequence of forwarding paths for a service flow in the SVPN service.

By default, forwarding paths are sequenced according to the configuration time.

Format

source { [**vpn-instance** *vpn-instance-name*] *source-ip-address* | *interface-type interface-number* } **index** *path-index*

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Specifies the name of the VPN instance to which the specified source address belongs.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
source-ip-address	Specifies a source address for a service flow forwarding path.	The value is in dotted decimal notation.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
interface-type interface-number	Specifies the type and number of the source interface for a service flow forwarding path. • *interface-type* specifies the interface type. • *interface-number* specifies the interface number.	-
path-index	Specifies an index for a service flow forwarding path. **NOTE** The index cannot be larger than the total number of forwarding paths currently configured.	The value is an integer that ranges from 1 to 8.

Views

Service view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After forwarding paths are configured for an SVPN service flow, you can run this command to adjust the sequence of the forwarding paths.

Prerequisite

Before adjusting the sequence of the forwarding paths for a service flow, you need to run the **source (SVPN proposal view)** command to create a forwarding path and the **source (service view)** command to reference this forwarding path, or run the **source (service view)** command to create a forwarding path.

Precautions

After an SVPN proposal is bound to an SVPN tunnel interface, you need to unbind the SVPN proposal from the interface if you want to adjust the sequence of the forwarding paths.

When you adjust the sequence of the forwarding paths, the specified **source** related parameters must be the same as those of the forwarding path to be adjusted.

Example

Set the index of the forwarding path with the source addresses of 1.1.1.9 to 2.

```
<Huawei> system-view
[Huawei] svpn-proposal p1
```

 Copyright © Huawei Technologies Co., Ltd.

```
[Huawei-svpn-proposal-p1] destination 2.2.2.9
[Huawei-svpn-proposal-p1] service s1 id 1
[Huawei-svpn-proposal-p1-service-s1] source 1.1.1.9
[Huawei-svpn-proposal-p1-service-s1] source 3.3.3.9
[Huawei-svpn-proposal-p1-service-s1] source 4.4.4.9
[Huawei-svpn-proposal-p1-service-s1] source 1.1.1.9 index 2
[Huawei-svpn-proposal-p1-service-s1] display this
#
 service s1 id 1
  source 3.3.3.9
  source 1.1.1.9
  source 4.4.4.9
#
return
```

Related Topics

12.4.14 source (SVPN proposal view)

12.4.15 source (service view)

12.4.17 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** [**p2mp**] | **ipsec** | **ipv6-ipv4** [**6to4** | **auto-tunnel** | **isatap**] | **ipv4-ipv6** | **mpls te** | **svpn** [**p2p** | **p2mp**] | **none** }

undo tunnel-protocol

Parameters

Parameter	Description	Value
gre	Indicates that the GRE tunnel protocol is configured on a tunnel interface.	-
gre p2mp	Indicates that the mGRE tunnel protocol is configured on a tunnel interface. If this parameter is not used, the tunnel protocol configured on a tunnel interface is a traditional point-to-point GRE.	-
ipsec	Indicates that the IPSec tunnel protocol is configured on a tunnel interface.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
ipv4-ipv6	Indicates that the IPv4 to IPv6 tunnel protocol is configured on a tunnel interface.	-
ipv6-ipv4	Configures the tunnel protocol of the tunnel interface as ipv6-ipv4 and uses a manual IPv6 over IPv4 tunnel.	-
ipv6-ipv4 6to4	Indicates that the IPv6 to IPv4 tunnel protocol is configured on a tunnel interface using 6to4.	-
ipv6-ipv4 auto-tunnel	Configures the tunnel protocol of the tunnel interface as ipv6-ipv4 and uses an automatic IPv6 over IPv4 tunnel.	-
ipv6-ipv4 isatap	Indicates that the IPv6 to IPv4 tunnel protocol is configured on a tunnel interface using isatap.	-
mpls te	Indicates that the MPLS TE tunnel protocol is configured on a tunnel interface. **NOTE** The AR100&AR120&AR150&AR160&AR200 does not support this parameter.	-
svpn [**p2p** | **p2mp**]	Indicates that the SVPN tunnel protocol is configured on a tunnel interface. • **p2p**: indicates the P2P SVPN tunnel protocol. • **p2mp**: indicates the P2MP SVPN tunnel protocol.	-
none	Indicates that no tunnel protocol is configured on a tunnel interface.	-

Views

Tunnel interface view, Tunnel-Template interface view

NOTE

The tunnel template interface view supports the **ipsec** and **none** parameters only.

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.

 Copyright © Huawei Technologies Co., Ltd.

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. When the **p2mp** parameter is specified following **gre**, you can set the tunnel encapsulation mode to P2MP GRE. The destination address of a P2MP GRE tunnel does not need to be manually configured. Instead, the destination address of this tunnel can either be defined by a protocol (for example, NHRP in a DSVPN scenario) or be dynamically learned.
- IPSec: protects the security of data transmitted on the Internet by establishing tunnels using the IPSec protocol.
- 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.
- SVPN: binds multiple WAN access lines to provide high bandwidth and highly reliable networks for customers.
  - When the SVPN mode is set to Hub-Spoke, specify **p2p** on the Spoke and **p2mp** on the hub when configuring a tunnel protocol.
  - When the SVPN mode is set to Lone Ranger, you must not specify **p2p** or **p2mp**.

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. When an SVPN proposal is bound to a tunnel interface, you cannot modify the tunnel encapsulation mode.

Example

Set the tunnel encapsulation mode of Tunnel0/0/2 to mGRE.

```
<Huawei> system-view
[Huawei] interface tunnel 0/0/2
[Huawei-Tunnel0/0/2] tunnel-protocol gre p2mp
```

Set the tunnel encapsulation mode of Tunnel0/0/2 to GRE.

```
<Huawei> system-view
[Huawei] interface tunnel 0/0/2
[Huawei-Tunnel0/0/2] tunnel-protocol gre
```

Related Topics

12.3.10 interface tunnel

 Copyright © Huawei Technologies Co., Ltd.

12.5 DSVPN Configuration Commands

12.5.1 display nhrp peer

Function

The **display nhrp peer** command displays NHRP peer entries.

Format

display nhrp peer { **interface tunnel** *interface-number* [**dynamic** | **static** | *ip-address*] | *ip-address* }

display nhrp peer { **dynamic** | **static** } [*ip-address*]

display nhrp peer all

Parameters

Parameter	Description	Value
interface tunnel *interface-number*	Displays NHRP peer entries on the specified interface. *interface-number* specifies the interface number.	The interface number must already exist.
dynamic	Displays dynamic NHRP peer entries.	-
static	Displays static NHRP peer entries.	-
ip-address	Displays NHRP peer entry information based on the subnet IP address of the NHRP peer.	The value is in dotted decimal notation.
all	Displays all NHRP peer entries.	-

Views

All views

Default Level

1: Monitoring level

Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

To determine whether a spoke has successfully registered, run the **display nhrp peer** command on the Hub to check whether NHRP peer entries of the spoke are generated. When a communication fault occurs between two spokes, run the **display nhrp peer** command on a spoke to check whether NHRP peer entries of the destination spoke are generated.

Example

Display all NHRP peer entries.

```
<Huawei> display nhrp peer all
--------------------------------------------------------------------------------
Protocol-addr   Mask  NBMA-addr       NextHop-addr    Type           Flag
--------------------------------------------------------------------------------
1.2.1.2         32    2.2.1.1         1.2.1.2         registered     up|unique
--------------------------------------------------------------------------------
Tunnel interface: Tunnel0/0/0
Created time    : 19:00:27
Expire time     : 01:59:34
--------------------------------------------------------------------------------
Protocol-addr   Mask  NBMA-addr       NextHop-addr    Type           Flag
--------------------------------------------------------------------------------
1.2.1.1         32    3.2.1.1         1.2.1.1         registered     up|no-unique
--------------------------------------------------------------------------------
Tunnel interface: Tunnel0/0/0
Created time    : 17:12:23
Expire time     : 01:59:54

Number of nhrp peers: 2
```

Table 12-13 Description of the **display nhrp peer all** command output

Item	Description
Protocol-addr	Subnet address or tunnel interface address of the NHRP peer.
Mask	Subnet address mask or tunnel interface address mask of the NHRP peer.
NBMA-addr	Public address of the NHRP peer, which corresponds to the source tunnel interface address of the NHRP peer.
NextHop-addr	Address of the next hop pointing to the protocol address.

Copyright © Huawei Technologies Co., Ltd.

Item	Description
Type	Type of the NHRP peer table. • hub: indicates a static entry with the **register** parameter. • static: indicates a static entry without the **register** parameter. • local: indicates an entry whose peer is itself. • registered: indicates a dynamically generated branch registration entry. • remote: indicates a dynamically generated entry in which the remote address is a tunnel interface address. • remote-network: indicates a dynamically generated entry in which the remote address is a subnet address. If branches save only summarized routes to the headquarters, the source branch can dynamically learn the subnet address of the destination branch.
Flag	NHRP peer entry status: • up: indicates that the NHRP peer entry is Up. • down: indicates that the NHRP peer entry is Down. • unique: indicates that conflicting NHRP peer entries are not overwritten during NHRP registration. • no-unique: indicates that conflicting NHRP peer entries are overwritten during NHRP registration. **NOTE** up/down and unique/no-unique can be displayed simultaneously.
Tunnel interface	Tunnel interface number.
Before NAT NBMA-addr	NBMA address before NAT is implemented.
Created time	Time when an NHRP peer entry is created.
Expire time	Time when an NHRP peer entry expires.
Number of nhrp peers	Total number of NHRP peer entries generated currently.

12.5.2 display nhrp peer maximum-history

Function

The **display nhrp peer maximum-history** command displays historical statistics on NHRP peer entries and sites.

 Copyright © Huawei Technologies Co., Ltd.

Format

display nhrp peer maximum-history

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run this command to view history statistics on NHRP peer entries and sites.

Example

Display history statistics on NHRP peer entries and sites.

```
<Huawei> display nhrp peer maximum-history
 ------------------------------------------------------------------------------
 Total peers                          :    0
 Maximum of total peers in history          :    0
 Begin time of total peers                  :    2016-10-18 20:22:30
 Maximum time of total peers                :    2016-10-18 20:22:30

 Total sites                          :    0
 Maximum of total sites in history          :    0
 Begin time of total sites                  :    2016-10-18 20:22:30
 Maximum time of total sites                :    2016-10-18 20:22:30
 ------------------------------------------------------------------------------
```

Table 12-14 Description of the **display nhrp peer maximum-history** command output

Item	Description
Total peers	Total number of NHRP peer entries.
Maximum of total peers in history	Maximum number of NHRP peer entries in the history.
Begin time of total peers	Time when collection of statistics on NHRP peer entries begins.
Maximum time of total peers	Time when the number of NHRP peer entries reaches the maximum value.
Total sites	Total number of sites.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Maximum of total sites in history	Maximum number of sites in the history.
Begin time of total sites	Time when collection of site statistics begins.
Maximum time of total sites	Time when the number of sites reaches the maximum value.

12.5.3 display nhrp statistics

Function

The **display nhrp statistics** command displays NHRP packet statistics.

Format

display nhrp statistics interface tunnel *interface-number*

Parameters

Parameter	Description	Value
interface tunnel *interface-number*	Displays NHRP packet statistics on the specified interface.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

This command displays NHRP packet statistics to help locate DSVPN-related faults.

Example

Display NHRP packet statistics on the interface tunnel 0/0/0.

```
<Huawei> display nhrp statistics interface tunnel 0/0/0
RegisterRequestSendSuccess       :0
RegisterRequestSendFail          :0
RegisterRequestCorrectRecv       :1024
```


Copyright © Huawei Technologies Co., Ltd.

```
RegisterRequestErrRecv            :0
RegisterRequestTransf             :0
RegisterReplySendSuccess          :1024
RegisterReplySendFail             :0
RegisterReplyCorrectRecv          :0
RegisterReplyErrRecv              :0
RegisterReplyTransf               :0
ResolutionRequestSendSuccess      :0
ResolutionRequestSendFail         :0
ResolutionRequestCorrectRecv      :0
ResolutionRequestErrRecv          :0
ResolutionRequestTransf           :0
ResolutionReplySendSuccess        :0
ResolutionReplySendFail           :0
ResolutionReplyCorrectRecv        :0
ResolutionReplyErrRecv            :0
ResolutionReplyTransf             :0
PurgeRequestSendSuccess           :0
PurgeRequestSendFail              :0
PurgeRequestCorrectRecv           :0
PurgeRequestErrRecv               :0
PurgeRequestTransf                :0
PurgeReplySendSuccess             :0
PurgeReplySendFail                :0
PurgeReplyCorrectRecv             :0
PurgeReplyErrRecv                 :0
PurgeReplyTransf                  :0
RedirectIndicationSendSuccess     :0
RedirectIndicationSendFail        :0
RedirectIndicationCorrectRecv     :0
RedirectIndicationErrRecv         :0
RedirectIndicationTransf          :0
ErrIndicationSendSuccess          :0
ErrIndicationSendFail             :0
ErrIndicationCorrectRecv          :0
ErrIndicationErrRecv              :0
ErrIndicationTransf               :0
AuthenticationFail                :0
LoopdetectFail                    :0
```

Table 12-15 Description of the **display nhrp statistics** command output

Item	Description
RegisterRequest-SendSuccess	Number of NHRP Registration Request packets that are sent successfully.
RegisterRequest-SendFail	Number of NHRP Registration Request packets that fail to be sent.
RegisterRequestCor-rectRecv	Number of NHRP Registration Request packets that are received successfully.
RegisterRequestErr-Recv	Number of NHRP Registration Request packets that fail to be received.
RegisterRequest-Transf	Number of NHRP Registration Request packets that are forwarded.
RegisterReplySend-Success	Number of NHRP Registration Reply packets that are sent successfully.
RegisterReplySend-Fail	Number of NHRP Registration Reply packets that fail to be sent.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
RegisterReplyCorrectRecv	Number of NHRP Registration Reply packets that are received successfully.
RegisterReplyErrRecv	Number of NHRP Registration Reply packets that fail to be received.
RegisterReplyTransf	Number of NHRP Registration Reply packets that are forwarded.
ResolutionRequestSendSuccess	Number of NHRP Resolution Request packets that are sent successfully.
ResolutionRequestSendFail	Number of NHRP Resolution Request packets that fail to be sent.
ResolutionRequestCorrectRecv	Number of NHRP Resolution Request packets that are received successfully.
ResolutionRequestErrRecv	Number of NHRP Resolution Request packets that fail to be received.
ResolutionRequestTransf	Number of NHRP Resolution Request packets that are forwarded.
ResolutionReplySendSuccess	Number of NHRP Resolution Reply packets that are sent successfully.
ResolutionReplySendFail	Number of NHRP Resolution Reply packets that fail to be sent.
ResolutionReplyCorrectRecv	Number of NHRP Resolution Reply packets that are received successfully.
ResolutionReplyErrRecv	Number of NHRP Resolution Reply packets that fail to be received.
ResolutionReplyTransf	Number of NHRP Resolution Reply packets that are forwarded.
PurgeRequestSendSuccess	Number of NHRP Purge Request packets that are sent successfully.
PurgeRequestSendFail	Number of NHRP Purge Request packets that fail to be sent.
PurgeRequestCorrectRecv	Number of NHRP Purge Request packets that are received successfully.
PurgeRequestErrRecv	Number of NHRP Purge Request packets that fail to be received.
PurgeRequestTransf	Number of NHRP Purge Request packets that are forwarded.
PurgeReplySendSuccess	Number of NHRP Purge Reply packets that are sent successfully.

Copyright © Huawei Technologies Co., Ltd.

Item	Description
PurgeReplySendFail	Number of NHRP Purge Reply packets that fail to be sent.
PurgeReplyCorrectRecv	Number of NHRP Purge Reply packets that are received successfully.
PurgeReplyErrRecv	Number of NHRP Purge Reply packets that fail to be received.
PurgeReplyTransf	Number of NHRP Purge Reply packets that are forwarded.
RedirectIndicationSendSuccess	Number of NHRP Redirect Indication packets that are sent successfully.
RedirectIndicationSendFail	Number of NHRP Redirect Indication packets that fail to be sent.
RedirectIndicationCorrectRecv	Number of NHRP Redirect Indication packets that are received successfully.
RedirectIndicationErrRecv	Number of NHRP Redirect Indication packets that fail to be received.
RedirectIndicationTransf	Number of NHRP Redirect Indication packets that are forwarded.
ErrIndicationSendSuccess	Number of NHRP Error Indication packets that are sent successfully.
ErrIndicationSendFail	Number of NHRP Error Indication packets that fail to be sent.
ErrIndicationCorrectRecv	Number of NHRP Error Indication packets that are received successfully.
ErrIndicationErrRecv	Number of NHRP Error Indication packets that fail to be received.
ErrIndicationTransf	Number of NHRP Error Indication packets that are forwarded.
AuthenticationFail	Number of packets that fail to be authenticated.
LoopdetectFail	Number of loopback packets.

Related Topics

12.5.15 reset nhrp statistics

 Copyright © Huawei Technologies Co., Ltd.

12.5.4 nhrp authentication

Function

The **nhrp authentication** command configures an NHRP authentication string.

The **undo nhrp authentication** command deletes an NHRP authentication string.

By default, no NHRP authentication string is configured.

Format

nhrp authentication { **simple** *string* | **cipher** *cipher-string* }

undo nhrp authentication

Parameters

Parameter	Description	Value
simple	Indicates the plain text password. You can enter a plain text password. When you want to view the configuration file, the password is displayed in plain text mode. **NOTICE** If **simple** is selected, the password is saved in the configuration file in plain text. This brings security risks. It is recommended that you select **cipher** to save the password in cipher text.	-
string	Specifies the NHRP authentication string.	The value is a string of 1 to 8 case-sensitive characters. The value can contain special characters except the question mark (?) and space. **NOTE** To improve security, it is recommended that the NHRP authentication string contains at least two types of lowercase letters, uppercase letters, digits, and special characters, and contains at least 6 characters.
cipher	Indicates the cipher text password. You can enter a plain or cipher text password. When you want to view the configuration file, the password is displayed in cipher text mode.	-

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
cipher-string	Specifies the NHRP authentication string. The value is a string of encrypted or unencrypted characters.	An unencrypted password is a string of 1 to 8 case-sensitive characters, and an encrypted password is a string of 48 case-sensitive characters. The value can contain special characters except the question mark (?) and space. **NOTE** To improve security, it is recommended that the NHRP authentication string contains at least two types of lowercase letters, uppercase letters, digits, and special characters, and contains at least 6 characters.

Views

Tunnel interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

This command configures the NHRP authentication string on a spoke and the hub. This command enables the hub to reject the illegal registration of a spoke.

Prerequisites

The following operations have been performed:

1. Run the **interface tunnel** command to create a tunnel interface and display the tunnel interface view.
2. Run the **tunnel-protocol gre p2mp** command to set the tunnel encapsulation mode to mGRE.

Configuration Impact

After this command is executed on a spoke and the hub, the spoke sends an NHRP Registration Request packet to the hub, and the hub decides whether to process this packet based on the NHRP authentication string in the packet. If this NHRP authentication string is different from that configured on the hub, the hub does not process this packet. If the two NHRP authentication strings are the same, the hub processes this packet.

Precautions

If the NHRP authentication string is configured on the spoke but not on the hub, the NHRP authentication string cannot be used for authentication.

 Copyright © Huawei Technologies Co., Ltd.

Example

Set the NHRP authentication string to huawei@1 in cipher text.

```
<Huawei> system-view
[Huawei] interface tunnel 0/0/0
[Huawei-Tunnel0/0/0] tunnel-protocol gre p2mp
[Huawei-Tunnel0/0/0] nhrp authentication cipher huawei@1
```

Related Topics

12.3.10 interface tunnel

12.3.21 tunnel-protocol

12.5.5 nhrp entry

12.5.5 nhrp entry

Function

The **nhrp entry** command adds static NHRP peer entries to the local NHRP mapping table.

The **undo nhrp entry** command deletes static NHRP peer entries from the local NHRP mapping table.

By default, no static NHRP peer entry is added to the local NHRP mapping table.

Format

nhrp entry *protocol-address* { *dns-name* | *nbma-address* } [**register** [**preference** *preference-value*]] [**track apn** *apn-name*]

undo nhrp entry *protocol-address* { *dns-name* | *nbma-address* } [**register** [**preference** *preference-value*]] [**track apn** *apn-name*]

Parameters

Parameter	Description	Value
protocol-address	Specifies the tunnel interface address of an NHRP peer device.	The value is in dotted decimal notation.
dns-name	Specifies the domain name of the NHRP peer device.	The value is a string of 1 to 255 case-sensitive characters without spaces.
nbma-address	Specifies the NBMA address of the NHRP peer device.	The value is in dotted decimal notation.
register	Configures a spoke to register with the hub to generate NHRP peer entries on the hub.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
preference *preference-value*	Specifies the hub priority. When multiple static NHRP peer entries are configured on a branch device and NHRP fails to determine the hub based on the next hop in private routes, the device selects an active hub based on the hub priority.	The value is an integer that ranges from 1 to 255. The default value is 60. A smaller value indicates a higher priority.
track apn	Binds NHRP peer information with the APN profile.	-
apn-name	Specifies the APN profile name.	The value is the name of an existing APN profile.

Views

Tunnel interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

This command configures mapping between the tunnel interface address of the NHRP peer device (the hub) and the NBMA address or mapping between the tunnel interface address and the host name.

When the spoke registers with the hub, the hub generates mapping between the tunnel interface address of the spoke and the NBMA address, so that the spoke and the hub communicate with each other through a VPN tunnel.

In a LTE scenario, you can bind NHRP peer information with the APN profile configured on the cellular interface if the source interface of the mGRE tunnel is a cellular interface. The NHRP peer information takes effect when the associated APN profile is in use. This flexibly controls mGRE tunnel setup.

Prerequisites

The following operations have been performed:

1. Run the **interface tunnel** command to create a tunnel interface and display the tunnel interface view.
2. Run the **tunnel-protocol gre p2mp** command to set the tunnel encapsulation mode to mGRE.

Configuration Impact

After this command is executed on the spoke, a local NHRP peer entry is generated and takes effect regardless of whether the hub receives Registration

 Copyright © Huawei Technologies Co., Ltd.

Request packets or not. If the spoke forwards packets based on this entry but the hub cannot receive the packets, a black hole is generated.

Precautions

The Domain Name Server (DNS) provides static mappings between domain names and IP addresses. When IP addresses change, DNS cannot dynamically update mappings. Therefore, administrators should configure the **nhrp peer** or **shutdown** and **undo shutdown** command to specify the next mGRE interface.

If NHRP peer information is associated with the APN profile, whether the NHRP peer entry takes effect depends on the APN status. If the APN is valid, the NHRP peer entry takes effect; otherwise, the configuration is saved but the NHRP peer entry does not take effect.

Example

Configure mapping between tunnel interface address 10.10.10.10 and NBMA address 1.1.1.1.

```
<Huawei> system-view
[Huawei] interface tunnel 0/0/0
[Huawei-Tunnel0/0/0] tunnel-protocol gre p2mp
[Huawei-Tunnel0/0/0] nhrp entry 10.10.10.10 1.1.1.1
```

Configure mapping between the static address 10.10.10.10 and domain name **www.huawei.com**, and set the hub priority to 40.

```
<Huawei> system-view
[Huawei] interface tunnel 0/0/0
[Huawei-Tunnel0/0/0] tunnel-protocol gre p2mp
[Huawei-Tunnel0/0/0] nhrp entry 10.10.10.10 www.huawei.com register preference 40
```

Related Topics

12.3.10 interface tunnel

12.3.21 tunnel-protocol

12.5.6 nhrp entry holdtime

Function

The **nhrp entry holdtime** command sets the aging time of NHRP peer entries.

The **undo nhrp entry holdtime** command restores the aging time of NHRP peer entries to the default value.

By default, the aging time of NHRP peer entries is 7200 seconds.

Format

nhrp entry holdtime seconds *seconds*

undo nhrp entry holdtime seconds

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
seconds *seconds*	Specifies the aging time of NHRP peer entries.	The value is an integer that ranges from 5 to 31845, in seconds. It is recommended that the aging time of NHRP peer entries be larger than 120s.

Views

Tunnel interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

This command sets the aging time. The aging time is notified by the local device to the remote end so that the remote end can learn how long local NHRP peer entries can be retained. When a network exception occurs, the remote end deletes local NHRP peer entries based on the configured aging time. After the network recovers, a spoke registers with the hub to generate new NHRP peer entries.

Prerequisites

The following operations have been performed:

1. Run the **interface tunnel** command to create a tunnel interface and display the tunnel interface view.
2. Run the **tunnel-protocol gre p2mp** command to set the tunnel encapsulation mode to mGRE.

Configuration Impact

When you run this command to change the aging time of NHRP peer entries:

- If the value is too large, the device cannot delete NHRP peer entries in time.
- If the value is too small, a smaller interval for sending Registration packets must be configured on the peer device. This results in frequent sending of Registration packets, wasting network resources.

Precautions

The value of *seconds* must be larger than the value configured using the **nhrp registration interval** command so that the hub can receive re-registration packets from a spoke within the entry hold time.

 Copyright © Huawei Technologies Co., Ltd.

Example

Set the aging time of NHRP peer entries to 1800 seconds.

```
<Huawei> system-view
[Huawei] interface tunnel 0/0/0
[Huawei-Tunnel0/0/0] tunnel-protocol gre p2mp
[Huawei-Tunnel0/0/0] nhrp entry holdtime seconds 1800
```

Related Topics

12.3.10 interface tunnel

12.3.21 tunnel-protocol

12.5.10 nhrp registration interval

12.5.7 nhrp entry multicast dynamic

Function

The **nhrp entry multicast dynamic** command enables the Hub to add dynamically registered Spokes to the NHRP multicast member table.

The **undo nhrp entry multicast dynamic** command disables the Hub to add dynamically registered Spokes from the NHRP multicast member table.

By default, no dynamically registered Spoke is added to the NHRP multicast member table.

Format

nhrp entry multicast dynamic

undo nhrp entry multicast dynamic

Parameters

None

Views

Tunnel interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the RIP or OSPF protocol is deployed on the DSVPN network, run the **nhrp entry multicast dynamic** command to enable the Hub to add dynamically registered Spokes to the multicast member table. This allows Spokes to learn routes from each other. After receiving routing multicast packets sent from Spokes, the Hub copies these routing multicast packets and forwards them to the

 Copyright © Huawei Technologies Co., Ltd.

destination Spoke based on the NHRP multicast member table. This allows routing multicast packets to be exchanged between Spokes.

Prerequisites

The following operations have been performed:

1. Run the **interface tunnel** command to create a tunnel interface and display the tunnel interface view.
2. Run the **tunnel-protocol gre p2mp** command to set the tunnel encapsulation mode to mGRE.

Configuration Impact

When a network has multiple Spokes and the Hub learns all the routes to these Spokes, the Hub consumes large CPU resources. In this case, you can configure a shortcut mode of DSVPN and the route summarization function to allow Spokes to directly communicate with each other.

Precautions

Run this command on the hub in both the shortcut and non-shortcut mode of DSVPN.

Example

Configure the Spoke registered on Tunnel0/0/0 to be dynamically added to the NHRP multicast member table of the Hub.

```
<Huawei> system-view
[Huawei] interface tunnel 0/0/0
[Huawei-Tunnel0/0/0] tunnel-protocol gre p2mp
[Huawei-Tunnel0/0/0] nhrp entry multicast dynamic
```

Related Topics

12.3.10 interface tunnel

12.3.21 tunnel-protocol

12.5.5 nhrp entry

12.5.8 nhrp network-id

Function

The **nhrp network-id** command specifies the NHRP domain for a local mGRE interface.

The **undo nhrp network-id** command restores the default NHRP domain of the local mGRE interface.

By default, the local mGRE interface belongs to NHRP domain 0.

Format

nhrp network-id *number*

undo nhrp network-id

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
number	Specifies an NHRP domain. This domain takes effect only on the local device.	The value is an integer ranging from 1 to 4294967295.

Views

Tunnel interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **nhrp network-id** command specifies NHRP domains for mGRE interfaces to isolate various mGRE interfaces into different NHRP domains. A VPN tunnel is set up between two devices to forward NHRP packets. The network IDs of the inbound and outbound mGRE interfaces determine whether to set up a tunnel.

Prerequisites

The following operations have been performed:

1. Run the **interface tunnel** command to create a tunnel interface and display the tunnel interface view.
2. Run the **tunnel-protocol gre p2mp** command to set the tunnel encapsulation mode to mGRE.

Configuration Impact

If the inbound and outbound interfaces for NHRP packets are both mGRE interfaces, compare the network IDs of the two interfaces. The configuration impact on different types of NHRP packets is as follows:

- NHRP Registration Request packet and NHRP Registration Reply packet

  The NHRP module does not forward NHRP Registration packets. Therefore, it has no impact on the NHRP registration process.
- NHRP Resolution Request packet

  If the inbound and outbound mGRE interfaces for the NHRP packets have different network IDs, the NHRP module discards the packet and sends an NHRP Resolution Reply packet to the source peer device.
- NHRP Resolution Reply packet, Purge Request packet, Purge Reply packet and Redirect packet

  If the inbound and outbound mGRE interfaces for the NHRP packets have different network IDs, the NHRP module discards the packet.

 Copyright © Huawei Technologies Co., Ltd.

Precautions

After network IDs are changed, the NHRP peer learned by the device is not affected and the existing IPSec tunnel will not be changed.

Example

Set the network ID of an NHRP domain to 100.

```
<Huawei> system-view
[Huawei] interface tunnel 0/0/0
[Huawei-Tunnel0/0/0] tunnel-protocol gre p2mp
[Huawei-Tunnel0/0/0] nhrp network-id 100
```

Related Topics

12.3.10 interface tunnel

12.3.21 tunnel-protocol

12.5.9 nhrp redirect

Function

The **nhrp redirect** command enables the NHRP redirect function.

The **undo nhrp redirect** command disables the NHRP redirect function.

By default, the NHRP redirect function is disabled.

Format

nhrp redirect

undo nhrp redirect

Parameters

None

Views

Tunnel interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In the shortcut scenario, enable the NHRP redirect function on the hub. The hub sends NHRP Redirect packets to the source spoke while forwarding data flows within the NHRP domain. After receiving the NHRP Redirect packets, the source spoke sends NHRP Resolution Request packets and then establishes a tunnel to communicate with the destination spoke.

 Copyright © Huawei Technologies Co., Ltd.

Prerequisites

The following operations have been performed:

1. Run the **interface tunnel** command to create a tunnel interface and display the tunnel interface view.
2. Run the **tunnel-protocol gre p2mp** command to set the tunnel encapsulation mode to mGRE.

Configuration Impact

After you run this command on the hub, it takes effect no matter the NHRP shortcut function is enabled on a spoke or not. When you disable the NHRP shortcut function on spoke, the hub sends an NHRP Redirect packet whenever a data packet is received, this cause the wasting of CPU and network resources. Enabling the NHRP shortcut function on a spoke solves this problem.

Precautions

To allow two branches to directly communicate by establishing a tunnel, you must also enable the **nhrp shortcut** function on spokes.

Example

Enable the NHRP redirect function on Tunnel0/0/0.

```
<Huawei> system-view
[Huawei] interface tunnel 0/0/0
[Huawei-Tunnel0/0/0] tunnel-protocol gre p2mp
[Huawei-Tunnel0/0/0] nhrp redirect
```

Related Topics

12.3.10 interface tunnel

12.3.21 tunnel-protocol

12.5.12 nhrp shortcut

12.5.10 nhrp registration interval

Function

The **nhrp registration interval** command sets the interval at which a spoke registers with the hub.

The **undo nhrp registration interval** command restores the interval to the default value.

By default, a spoke registers with the hub at an interval of 1800 seconds.

Format

nhrp registration interval *seconds*

undo nhrp registration interval

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
seconds	Specifies the interval at which a spoke registers with the hub.	The value is an integer that ranges from 5 to 31845, in seconds. The default value is 1800 seconds.

Views

Tunnel interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the tunnel address and public network address of a spoke change or the NHRP peer entry of the hub ages, the hub may fail to update the NHRP peer entry in time. In this case, run the **nhrp registration interval** command on the spoke to set the interval at which a spoke registers with the hub to a value smaller than the aging time of NHRP peer entries.

Prerequisites

The following operations have been performed:

1. Run the **interface tunnel** command to create a tunnel interface and display the tunnel interface view.
2. Run the **tunnel-protocol gre p2mp** command to set the tunnel encapsulation mode to mGRE.

Configuration Impact

When you run this command to change the interval at which a spoke registers with the hub:

- If the interval is too long, the spoke fails to immediately inform the hub of the latest branch information.
- If the interval is too short, the spoke frequently registers with the hub, wasting network resources.

Precautions

NOTICE

The value of the parameter *seconds* cannot be larger than the aging time of NHRP peer entries configured by using the **nhrp entry holdtime** command.

Copyright © Huawei Technologies Co., Ltd.

Example

Configure a spoke to register with the hub at an interval of 600 seconds.

```
<Huawei> system-view
[Huawei] interface tunnel 0/0/0
[Huawei-Tunnel0/0/0] tunnel-protocol gre p2mp
[Huawei-Tunnel0/0/0] nhrp registration interval 600
```

Related Topics

12.3.10 interface tunnel

12.5.6 nhrp entry holdtime

12.3.21 tunnel-protocol

12.5.11 nhrp registration no-unique

Function

The **nhrp registration no-unique** command configures the device to send NHRP packets that carry the no-unique flag to instruct the remote end to overwrite conflicting NHRP peer entries.

The **undo nhrp registration no-unique** command configures the device to send NHRP packets that do not carry the no-unique flag to instruct the remote end not to overwrite conflicting NHRP peer entries.

By default, the device sends NHRP packets that do not carry the no-unique flag to instruct the remote end not to overwrite conflicting NHRP peer entries.

Format

nhrp registration no-unique

undo nhrp registration no-unique

Parameters

None

Views

Tunnel interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

This command can only be configured on branch devices. When a branch device sends an NHRP Registration Reply packet to a headquarters device, whether this packet carries the no-unique flag determines whether the headquarters device overrides conflicting NHRP peer entries of this branch device.

 Copyright © Huawei Technologies Co., Ltd.

When a branch device performs NHRP registration with a headquarters device, the headquarters device generates an NHRP peer entry for this branch device. If the branch device performs NHRP registration again after its public IP address changes, by default, the NHRP registration packet sent by this branch device does not carry the no-unique flag. After the headquarters device receives this packet, it does not override the conflicting NHRP peer entry of this branch device and rejects this NHRP registration. If the headquarters device needs to save the latest branch device information and overrides the conflicting NHRP peer entry, run the **nhrp registration no-unique** command on the branch device to enable the NHRP registration packet sent by this branch device to carry the no-unique flag.

If a branch device dynamically obtains an IP address, for example, in an LTE scenario, you are advised to run the **nhrp registration no-unique** command on the branch device to send NHRP packets that carry the no-unique flag, instructing the headquarters device to overwrite the conflicting NHRP peer entry. Otherwise, the branch device cannot re-register with the headquarters device successfully.

Prerequisites

The following operations have been performed:

1. Run the **interface tunnel** command to create a tunnel interface and display the tunnel interface view.
2. Run the **tunnel-protocol gre p2mp** command to set the tunnel encapsulation mode to mGRE.

Configuration Impact

The following situations occur when the spoke re-registers with the hub after the public address of the spoke is changed:

- If the **nhrp registration no-unique** command is used on the spoke, the device overrides existing NHRP peer entries with new NHRP peer entries.
- If the **nhrp registration no-unique** command is not configured on a spoke node, new NHRP peer entries will not override existing NHRP peer entries on a hub node and new registration entries will be discarded. New registration entries can successfully register only when old NHRP peer entries are aged out.

Example

Configure the device to send NHRP packets that carry the no-unique flag to instruct the remote end to overwrite conflicting NHRP peer entries.

```
<Huawei> system-view
[Huawei] interface tunnel 0/0/0
[Huawei-Tunnel0/0/0] tunnel-protocol gre p2mp
[Huawei-Tunnel0/0/0] nhrp registration no-unique
```

Related Topics

12.3.10 interface tunnel

12.3.21 tunnel-protocol

 Copyright © Huawei Technologies Co., Ltd.

12.5.12 nhrp shortcut

Function

The **nhrp shortcut** command enables the NHRP shortcut function.

The **undo nhrp shortcut** command disables the NHRP shortcut function.

By default, the NHRP shortcut function is disabled.

Format

nhrp shortcut

undo nhrp shortcut

Parameters

None

Views

Tunnel interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The hub sends NHRP Redirect packets to the source spoke while forwarding data flows within the NHRP domain. Run the **nhrp shortcut** command on the spoke to allow it to send NHRP Resolution Request packets to the destination spoke after it receives NHRP Redirect packets sent from the hub. A tunnel is directly established between two branches.

Prerequisites

The following operations have been performed:

1. Run the **interface tunnel** command to create a tunnel interface and display the tunnel interface view.
2. Run the **tunnel-protocol gre p2mp** command to set the tunnel encapsulation mode to mGRE.

Precautions

The NHRP shortcut function must work with the NHRP redirect function. Therefore, the NHRP redirect function must be enabled on the hub using the **nhrp redirect** command.

Example

Enable the NHRP shortcut function on Tunnel0/0/0.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> system-view
[Huawei] interface tunnel 0/0/0
[Huawei-Tunnel0/0/0] tunnel-protocol gre p2mp
[Huawei-Tunnel0/0/0] nhrp shortcut
```

Related Topics

12.3.10 interface tunnel

12.3.21 tunnel-protocol

12.5.9 nhrp redirect

12.5.13 nhrp tunnel-if-state related

Function

The **nhrp tunnel-if-state related** command associates the mGRE interface status of a Spoke with the Hub status.

The **undo nhrp tunnel-if-state related** command cancels associating the mGRE interface status of a Spoke with the Hub status.

By default, the mGRE interface status of a Spoke is not associated with the Hub status.

Format

nhrp tunnel-if-state related

undo nhrp tunnel-if-state related

Parameters

None

Views

Tunnel interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In a DSVPN scenario, when a Spoke detects that the Hub status goes Down, the Spoke reports an alarm to the NMS to alert network administrators. If the intermediate network experiences a fault, the Spoke detects that the status of all Hubs goes Down; however, network administrators cannot view the network fault on the NMS monitor topology. To solve this problem, associate the mGRE interface status of the Spoke with the Hub status for rapid fault detection on the monitor topology. That is, the mGRE interface becomes Down when the Hub status is Down. Additionally, enable the system to send an email to instruct network

 Copyright © Huawei Technologies Co., Ltd.

administrators to rectify faults in a timely manner when the mGRE interface becomes Down. To associate the mGRE interface status of the Spoke with the Hub status, run the **nhrp tunnel-if-state related** command.

Prerequisites

Before executing this command, perform the following operations:

1. Run the **interface tunnel** command to create a tunnel interface and enter the tunnel interface view.
2. Run the **tunnel-protocol gre p2mp** command to set the encapsulation mode of a tunnel interface to mGRE.

Example

Associate the mGRE interface status of a Spoke with the Hub status.

```
<Huawei> system-view
[Huawei] interface tunnel 0/0/0
[Huawei-Tunnel0/0/0] tunnel-protocol gre p2mp
[Huawei-Tunnel0/0/0] nhrp tunnel-if-state related
```

12.5.14 reset nhrp peer maximum-history

Function

The **reset nhrp peer maximum-history** command clears the history statistics on NHRP peer entries.

Format

reset nhrp peer maximum-history

Parameters

None

Views

User view

Default Level

3: Management level

Usage Guidelines

You can run this command to clear the history statistics on NHRP peer entries.

Example

Clear the history statistics on NHRP peer entries.

```
<Huawei> reset nhrp peer maximum-history
```

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

12.5.2 display nhrp peer maximum-history

12.5.15 reset nhrp statistics

Function

The **reset nhrp statistics** command clears NHRP packet statistics on a specified tunnel interface.

Format

reset nhrp statistics interface tunnel *interface-number*

Parameters

Parameter	Description	Value
interface tunnel *interface-number*	Specifies the interface number.	-

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

This command clears NHRP packet statistics on a specified tunnel interface. This helps you locate DSVPN faults quickly.

Configuration Impact

This command clears NHRP packet statistics on a specified tunnel interface.

Precautions

NOTICE

Statistics cannot be restored after being cleared. Therefore, confirm the action before you run the command.

Example

Clear NHRP packet statistics on Tunnel0/0/0.

Copyright © Huawei Technologies Co., Ltd.

```
<Huawei>reset nhrp statistics interface tunnel 0/0/0
```

Related Topics

12.5.3 display nhrp statistics

12.5.16 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 { [**vpn-instance** *vpn-instance-name*] *source-ip-address* | *interface-type interface-number* }

undo source

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Specifies the name of the VPN instance that the source address of a tunnel belongs to. **NOTE** You can specify the parameter only when the encapsulation mode of a tunnel interface is set to IPSec or mGRE.	The value is the name of an existing VPN instance.
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.	-

Copyright © Huawei Technologies Co., Ltd.

Views

Tunnel interface view, Tunnel-Template interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When configuring a tunnel, you must 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, IPSec, 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.

IPv6 over IPv4, IPv4 over IPv6, and GRE tunnels are bidirectional tunnels. The source address of the local tunnel interface is the destination address of the remote tunnel interface by the **destination** command, and the destination address of the local tunnel interface is the source address of the remote tunnel interface.

Two or more tunnel interfaces that use the same encapsulation protocol cannot be configured with the same source and destination addresses. Two or more GRE tunnel interfaces in a system can have the same source address and same destination address. The system uses GRE keys to identify these GRE tunnel interfaces. When two or more tunnel interfaces on a P2MP tunnel are configured with the same source address, run the **gre key** command to set the key number of each tunnel interface.

You can also specify VPN instance parameters while specifying the source address for an IPSec tunnel or an mGRE tunnel in IPSec/mGRE over VPN scenarios.

Example

Set the tunnel type of Tunnel0/0/1 to IPv6 over IPv4 manual tunnel and configure the source IP address of Tunnel0/0/1 as 10.1.1.1.

```
<Huawei> system-view
[Huawei] interface tunnel 0/0/1
[Huawei-Tunnel0/0/1] tunnel-protocol ipv6-ipv4
[Huawei-Tunnel0/0/1] source 10.1.1.1
```

Configure Tunnel0/0/2 of mGRE and use Loopback0 address as the interface address.

```
<Huawei> system-view
[Huawei] interface loopback 0
[Huawei-LoopBack0] ip address 10.2.1.1 32
[Huawei-LoopBack0] quit
[Huawei] interface tunnel 0/0/2
```

 Copyright © Huawei Technologies Co., Ltd.

```
[Huawei-Tunnel0/0/2] tunnel-protocol gre p2mp
[Huawei-Tunnel0/0/2] source loopback 0
```

12.5.17 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** [**p2mp**] | **ipsec** | **ipv6-ipv4** [**6to4** | **auto-tunnel** | **isatap**] | **ipv4-ipv6** | **mpls te** | **svpn** [**p2p** | **p2mp**] | **none** }

undo tunnel-protocol

Parameters

Parameter	Description	Value
gre	Indicates that the GRE tunnel protocol is configured on a tunnel interface.	-
gre p2mp	Indicates that the mGRE tunnel protocol is configured on a tunnel interface. If this parameter is not used, the tunnel protocol configured on a tunnel interface is a traditional point-to-point GRE.	-
ipsec	Indicates that the IPSec tunnel protocol is configured on a tunnel interface.	-
ipv4-ipv6	Indicates that the IPv4 to IPv6 tunnel protocol is configured on a tunnel interface.	-
ipv6-ipv4	Configures the tunnel protocol of the tunnel interface as ipv6-ipv4 and uses a manual IPv6 over IPv4 tunnel.	-
ipv6-ipv4 6to4	Indicates that the IPv6 to IPv4 tunnel protocol is configured on a tunnel interface using 6to4.	-
ipv6-ipv4 auto-tunnel	Configures the tunnel protocol of the tunnel interface as ipv6-ipv4 and uses an automatic IPv6 over IPv4 tunnel.	-
ipv6-ipv4 isatap	Indicates that the IPv6 to IPv4 tunnel protocol is configured on a tunnel interface using isatap.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
mpls te	Indicates that the MPLS TE tunnel protocol is configured on a tunnel interface. **NOTE** The AR100&AR120&AR150&AR160&AR200 does not support this parameter.	-
svpn [**p2p** | **p2mp**]	Indicates that the SVPN tunnel protocol is configured on a tunnel interface. • **p2p**: indicates the P2P SVPN tunnel protocol. • **p2mp**: indicates the P2MP SVPN tunnel protocol.	-
none	Indicates that no tunnel protocol is configured on a tunnel interface.	-

Views

Tunnel interface view, Tunnel-Template interface view

NOTE

The tunnel template interface view supports the **ipsec** and **none** parameters only.

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. When the **p2mp** parameter is specified following **gre**, you can set the tunnel encapsulation mode to P2MP GRE. The destination address of a P2MP GRE tunnel does not need to be manually configured. Instead, the destination address of this tunnel can either be defined by a protocol (for example, NHRP in a DSVPN scenario) or be dynamically learned.
- IPSec: protects the security of data transmitted on the Internet by establishing tunnels using the IPSec protocol.
- 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.

 Copyright © Huawei Technologies Co., Ltd.

- 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.
- SVPN: binds multiple WAN access lines to provide high bandwidth and highly reliable networks for customers.
  - When the SVPN mode is set to Hub-Spoke, specify **p2p** on the Spoke and **p2mp** on the hub when configuring a tunnel protocol.
  - When the SVPN mode is set to Lone Ranger, you must not specify **p2p** or **p2mp**.

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. When an SVPN proposal is bound to a tunnel interface, you cannot modify the tunnel encapsulation mode.

Example

Set the tunnel encapsulation mode of Tunnel0/0/2 to mGRE.

```
<Huawei> system-view
[Huawei] interface tunnel 0/0/2
[Huawei-Tunnel0/0/2] tunnel-protocol gre p2mp
```

Set the tunnel encapsulation mode of Tunnel0/0/2 to GRE.

```
<Huawei> system-view
[Huawei] interface tunnel 0/0/2
[Huawei-Tunnel0/0/2] tunnel-protocol gre
```

Related Topics

12.3.10 interface tunnel

12.5.18 undo nhrp peer

Function

The **undo nhrp peer** command deletes dynamically negotiated NHRP peer entries.

Format

undo nhrp peer [*protocol-address* [*mask*]]

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
protocol-address [*mask*]	Specifies the network layer protocol address and mask.	-

Views

Tunnel interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

This command deletes dynamically negotiated NHRP peer entries before the entries age out. This prevents the existing NHRP peer entries from affecting the diagnosis result.

Configuration Impact

Dynamically negotiated NHRP peer entries are deleted from the local device and no entry will be generated before the peer device registers with the local device.

Precautions

NOTICE

- Deleting dynamically negotiated NHRP peer entries may result in communication interruption.
- Run this command only on the mGRE interface.

Example

Delete an NHRP peer entry with an IP address 10.10.10.10 and a 24-bit mask.

```
<Huawei> system-view
[Huawei] interface tunnel 0/0/0
[Huawei-Tunnel0/0/0] tunnel-protocol gre p2mp
[Huawei-Tunnel0/0/0] undo nhrp peer 10.10.10.10 24
```

Related Topics

12.5.1 display nhrp peer

12.3.21 tunnel-protocol

12.6 IPSec Configuration Commands

Copyright © Huawei Technologies Co., Ltd.

12.6.1 aaa authorization

Function

The **aaa authorization** command configures AAA RADIUS server authorization.

The **undo aaa authorization** command cancels AAA RADIUS server authorization.

By default, AAA RADIUS server authorization is not configured.

Format

aaa authorization [**domain** *domain-name*]

undo aaa authorization

Parameters

Parameter	Description	Value
domain *domain-name*	Specifies the domain name.	The domain name must already exist.

Views

IKE peer view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the remote device establishes an IKE SA with the server, you can run this command on the server to enable AAA RADIUS server authorization. If the **domain** parameter is specified, the remote device obtains authorization information using the specified **domain**. If the **domain** parameter is not specified, the remote device obtains authorization information using the domain name it sends to the server. The domain name is specified using the **service-scheme** command in the Efficient VPN policy view.

Prerequisite

A domain has been created using the **domain (AAA view)** command.

Precautions

After you configure this command on the server, the **service-scheme** command does not take effect.

Copyright © Huawei Technologies Co., Ltd.

Example

Set the domain name for AAA RADIUS server authorization to **abc**.

```
<Huawei> system-view
[Huawei] aaa
[Huawei-aaa] domain abc
[Huawei-aaa-domain-abc] quit
[Huawei] ike peer p1
[Huawei-ike-peer-p1] aaa authorization domain abc
```

12.6.2 alias

Function

The **alias** command sets an alias of an IPSec policy or IPSec policy template.

The **undo alias** command restores the default alias of an IPSec policy or IPSec policy template.

By default, the alias of an IPSec policy or IPSec policy template is the combination of its name and ID. If the default alias has been used by another IPSec policy or IPSec policy template, the system defines the default alias of the IPSec policy or IPSec policy template by combining the current time with its name and ID.

Format

alias *alias*

undo alias

Parameters

Parameter	Description	Value
alias	Specifies an alias for an IPSec policy or IPSec policy template.	The value is a string of 1 to 127 case-sensitive characters. It can contain special characters, such as !, @, #, $, and %, but cannot contain question marks.

Views

ISAKMP IPSec policy view, IPSec policy template view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

 Copyright © Huawei Technologies Co., Ltd.

In real-world applications, multiple IPSec policies or IPSec policy templates are often configured in an IPSec policy group. In this case, you can use the **alias** command to configure alias to identify these IPSec policies or IPSec policy templates. It is recommended that you configure meaningful alias that are easy to remember.

Precautions

The alias of each IPSec policy or IPSec policy template must be unique. Otherwise, the system displays a configuration failure message.

Example

Configure the alias **huawei** for the IPSec policy **policy1** with the ID of 1.

```
<Huawei> system-view
[Huawei] ipsec policy policy1 1 isakmp
[Huawei-ipsec-policy-isakmp-policy1-1] alias huawei
```

12.6.3 ah authentication-algorithm

Function

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

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

By default, the AH authentication algorithm is SHA2-256.

Format

ah authentication-algorithm { **md5** | **sha1** | **sha2-256** | **sha2-384** | **sha2-512** }

undo ah authentication-algorithm

Parameters

Parameter	Description	Value
md5	Uses the message digest algorithm 5 (MD5) authentication algorithm.	-
sha1	Uses the Secure Hash Algorithm 1 (SHA-1) authentication algorithm.	-
sha2-256	Uses the SHA2-256 authentication algorithm.	-
sha2-384	Uses the SHA2-384 authentication algorithm.	-
sha2-512	Uses the SHA2-512 authentication algorithm.	-
sm3	Uses the SM3 authentication algorithm.The algorithm can be used only in IKEv1 negotiation.When the SM3 algorithm is used, the padding mode of RSA signing cannot be PSS.	-

 Copyright © Huawei Technologies Co., Ltd.

NOTE

AR100&AR120 series, AR161, AR161W, AR161EW, AR161EW-M1, AR161G-L, AR161G-Lc, AR161G-U, AR169, AR169G-L, AR169CVW, AR169CVW-4B4S, AR169W, AR169W-P-M9, AR169RW-P-M9, AR169EW, AR169EGW-L, AR1220C, AR1220-8GE, AR2204-27GE, AR2204E-D-27GE, AR2204-24GE, AR2204-27GE-P, AR2204-48GE-P, AR2204-51GE, AR2204-51GE-P, AR2204-51GE-R, AR2204E, AR2204E-D, AR2204XE, and AR2204XE-DC do not support SHA2-384 and SHA2-512 authentication algorithms.

Views

IPSec proposal view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The AH protocol only authenticates packets and does not provide the encryption function.

Authentication algorithms that can be used in an IPSec proposal include the following (listed in descending order of security level): **sha2-512** > **sha2-384** > **sha2-256** > **sha1** > **md5**.

Prerequisites

ah or **ah-esp** has been specified in the **transform** command.

Precautions

Both ends of an IPSec tunnel must use the same authentication algorithm.

Authentication algorithms **sha2-256**, **sha2-384**, and **sha2-512** are recommended for security purpose. **md5** and **sha1** are not recommended.

Example

Specify the SHA2-256 algorithm for the AH protocol in the IPSec proposal **newprop1**.

```
<Huawei> system-view
[Huawei] ipsec proposal newprop1
[Huawei-ipsec-proposal-newprop1] transform ah
[Huawei-ipsec-proposal-newprop1] ah authentication-algorithm sha2-256
```

Related Topics

12.6.40 display ipsec proposal (All views)

Copyright © Huawei Technologies Co., Ltd.

12.6.4 ah authentication-algorithm (ipsec-proto-protect-proposal view)

Function

The **ah authentication-algorithm** command configures the authentication algorithm for Authentication Header (AH).

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

By default, the authentication algorithm SHA2-256 is used for AH.

Format

ah authentication-algorithm { **md5** | **sha1** | **sha2-256** }

undo ah authentication-algorithm

Parameters

Parameter	Description	Value
md5	Configures MD5 as the authentication algorithm for AH. **NOTE** To ensure high security, do not use the MD5 algorithm as the AH authentication algorithm.	-
sha1	Configures Secure Hash Algorithm-1 (SHA1) as the authentication algorithm for AH. **NOTE** To ensure high security, do not use the SHA1 algorithm as the AH authentication algorithm.	-
sha2-256	Configures SHA2-256 as the authentication algorithm for AH.	-

Views

IPSec proto-protect proposal view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

AH is used to prevent packets from being intercepted or modified and implement data origin authentication during data transmission. AH implements the Hash algorithm on the sending and receiving parties and checks data integrity and authenticity.

 Copyright © Huawei Technologies Co., Ltd.

AH currently supports MD5, SHA-1 and SHA2-256 authentication algorithms.

- MD5: generates a 128-bit message summary for an input message of any length
- SHA-1: generates a 160-bit message summary for an input message of less than 2^{64} bits
- SHA2-256: generates a 256-bit message summary for an input message of less than 2^{64} bits

MD5 is faster than SHA-1, but is less secure.

Prerequisite

The **transform** command has been configured to select AH before the authentication algorithm for AH is configured.

Precautions

The authentication algorithms on both IPSec peers must be identical.

Example

Set the authentication algorithm to SHA-1 for AH.

```
<Huawei> system-view
[Huawei] ipsec proto-protect proposal prop1
[Huawei-ipsec-proto-protect-proposal-prop1] transform ah
[Huawei-ipsec-proto-protect-proposal-prop1] ah authentication-algorithm sha1
```

12.6.5 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.

 Copyright © Huawei Technologies Co., Ltd.

Views

Manual IPSec policy view, ISAKMP IPSec policy view, IPSec policy template view, IPSec profile view, 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 **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 policy poli 10 isakmp
[Huawei-ipsec-policy-isakmp-poli-10] anti-replay window 128
```

Related Topics

12.6.93 ipsec anti-replay window

12.6.34 display ipsec policy (all views)

12.6.36 display ipsec policy-template (all views)

12.6.38 display ipsec profile (all views)

12.6.30 display ipsec efficient-vpn

12.6.6 authentication-algorithm

Function

The **authentication-algorithm** command configures an authentication algorithm for IKEv1 negotiation.

The **undo authentication-algorithm** command restores the default configuration.

 Copyright © Huawei Technologies Co., Ltd.

By default, the SHA2-256 authentication algorithm is used for IKEv1 negotiation.

Format

authentication-algorithm { **md5** | **sha1** | **sha2-256** | **sha2-384** | **sha2-512** }

undo authentication-algorithm

Parameters

Parameter	Description	Value
md5	Uses the message digest algorithm 5 (MD5) authentication algorithm.	-
sha1	Uses the Secure Hash Algorithm 1 (SHA-1) authentication algorithm.	-
sha2-256	Uses the SHA2-256 authentication algorithm.	-
sha2-384	Uses the SHA2-384 authentication algorithm.	-
sha2-512	Uses the SHA2-512 authentication algorithm.	-
sm3	Uses the SM3 authentication algorithm.The algorithm can be used only in IKEv1 negotiation.When the SM3 algorithm is used, the padding mode of RSA signing cannot be PSS.	-

Views

IKE proposal view

Default Level

2: Configuration level

Usage Guidelines

An authentication algorithm is required for IKEv1 negotiation. Authentication algorithms that can be used for IKEv1 negotiation include the following (listed in descending order of security level): **sha2-512** > **sha2-384** > **sha2-256** > **sha1** > **md5**.

NOTE

md5 and **sha1** are not recommended because they cannot provide high security.

Example

Specify the SHA2-384 authentication algorithm for IKE proposal 10.

```
<Huawei> system-view
[Huawei] ike proposal 10
[Huawei-ike-proposal-10] authentication-algorithm sha2-384
```

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

12.6.22 display ike proposal (All views)

12.6.7 authentication-method

Function

The **authentication-method** command specifies the authentication method used in IKE negotiation.

The **undo authentication-method** command restores the default authentication method.

By default, pre-shared key authentication is used in IKE negotiation.

Format

authentication-method { **pre-share** | **rsa-signature** }

undo authentication-method

Parameters

Parameter	Description	Value
pre-share	Uses pre-shared key authentication.	-
rsa-signature	Uses RSA signature authentication.	-

Views

IKE proposal view, Efficient VPN policy view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Identity authentication is a protection mechanism that ensures secure data transmission on an insecure network. This command configures an identity authentication method.

Precautions

The authentication methods in the IKE proposals used by the IKE peer must be the same. Otherwise, IKE negotiation fails.

For IKEv1, the **authentication-method** command does not take effect in the Efficient VPN policy view.

Follow-up Procedure

 Copyright © Huawei Technologies Co., Ltd.

- If **pre-share** is specified, run the **pre-shared-key** command to specify an authentication key.
- If **rsa-signature** is specified, configure a local certificate.

Example

Configure pre-shared key authentication in IKE proposal 10.

```
<Huawei> system-view
[Huawei] ike proposal 10
[Huawei-ike-proposal-10] authentication-method pre-share
```

Configure pre-shared key authentication for Efficient VPN policy **vpn1**.

```
<Huawei> system-view
[Huawei] ipsec efficient-vpn vpn1 mode client
[Huawei-ipsec-efficient-vpn-vpn1] authentication-method pre-share
```

Related Topics

12.6.76 ike proposal
12.6.22 display ike proposal (All views)
12.6.30 display ipsec efficient-vpn
12.6.98 ipsec efficient-vpn (system view)

12.6.8 certificate peer-name

Function

The **certificate peer-name** command enables IKEv1 digital envelope negotiation to use the peer certificate file imported to the PKI.

The **undo certificate peer-name** command disables IKEv1 digital envelope negotiation from using the peer certificate file imported to the PKI.

By default, the system does not use the peer certificate file imported to the PKI for IKEv1 digital envelope negotiation.

Format

certificate peer-name *peer-name*

undo certificate peer-name

Parameters

Parameter	Description	Value
peer-name *peer-name*	Specifies the name of the digital certificate of an IKE peer.	The digital certificate must have been imported to the PKI.

Views

IKE peer view

 Copyright © Huawei Technologies Co., Ltd.

Default Level

2: Configuration level

Usage Guidelines

If the authentication method is digital envelope (**digital-envelope**), you can use the peer digital certificate imported to the PKI. IKEv1 obtains the certificate public key through the peer digital certificate for digital envelope negotiation.

Example

Import the peer digital certificate **aa.pem** and reference it in the IKE peer.

```
<Huawei> system-view
[Huawei] pki import-certificate peer abcd pem filename aa.pem
[Huawei] ike peer a
[Huawei-ike-peer-a] certificate peer-name abcd
```

Related Topics

12.6.7 authentication-method

12.6.9 certificate-check disable

Function

The **certificate-check disable** command disables validity verification on certificates of an IKE peer.

The **undo certificate-check disable** command restores the default configuration.

By default, the device verifies certificates of an IKE peer.

Format

certificate-check disable

undo certificate-check disable

Parameters

None

Views

IKE peer view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

 Copyright © Huawei Technologies Co., Ltd.

When IPSec uses certificate authentication, users cannot update certificates after they become invalid, leading to unavailable certificates and IPSec authentication failure. If users still want to use these invalid certificates, run the **certificate-check disable** command to disable validity verification on certificates of an IKE peer. If users do not want to verify certificates of all IKE peers, run the **12.6.65 ike certificate-check disable** command.

Precautions

Disabling validity verification on certificates will lead to security risks.

Example

Configure the device not to verify certificates of an IKE peer.

```
<Huawei> system-view
[Huawei] ike peer peer1
[Huawei-ike-peer-peer1] certificate-check disable
```

Related Topics

12.6.20 display ike peer (all views)

12.6.10 certificate-request empty-payload enable

Function

The **certificate-request empty-payload enable** command configures a router to send certificate requests with empty payload.

The **undo certificate-request empty-payload enable** command restores the default configuration.

By default, certificate requests sent from a router carries CA information in the payload.

Format

certificate-request empty-payload enable

undo certificate-request empty-payload enable

Parameters

None

Views

IKE peer view

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

Usage Scenario

When a router acting as a gateway in the headquarters uses an IPSec policy configured using a policy template and authenticates branches by digital certificates, you can run the **certificate-request empty-payload enable** command to send certificate requests with empty payload, allowing access from branches using certificates issued by different CAs. The router can then perform certificate authentication based on certificate information provided by each branch.

Precautions

Do not configure this command if access devices cannot process certificate request packets with an empty authentication and authorization field. Otherwise, IKE negotiation fails.

Example

Configure the router to send certificate requests with empty payload.

```
<Huawei> system-view
[Huawei] ike peer a20
[Huawei-ike-peer-a20] certificate-request empty-payload enable
```

12.6.11 config-exchange

Function

The **config-exchange** command enables the device to request or set subnet route information.

The **undo config-exchange** command disables the device from requesting or setting subnet route information.

By default, the device cannot request or set subnet route information.

Format

config-exchange { **request** | **set** { **accept** | **send** } }

undo config-exchange { **request** | **set** [**accept** | **send**] }

Parameters

Parameter	Description	Value
request	Enables the device to request subnet route information from a remote device.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
set { **accept** | **send** }	Enables the device to accept subnet route information from a remote device or send local subnet route information.	-

Views

IKE peer view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A headquarters gateway sets up an IPSec tunnel with a branch gateway in virtual tunnel mode. In this case, you can run the **config-exchange** command to enable the gateways to request or set subnet route information.

1. The **config-exchange request** command can only be used on the initiator to enable it to request subnet information from the responder.
2. The **config-exchange set** { **accept** | **send** } command can be configured on both the initiator and the responder.
   - The **config-exchange set accept** command enables the local device to accept subnet route information sent by the remote device.
   - The **config-exchange set send** command enables the local device to send subnet route information to the remote device.

   If the **config-exchange set send** command is configured on the local device, the **config-exchange set accept** command must be configured on the remote device.

Prerequisites

Before you configure the **config-exchange set send** command to enable the local device to send subnet route information, the following operations must have been completed in the AAA service scheme.

- Run the **route set acl** *acl-number* command to configure local subnet route information.
- Run the **route set interface** command to configure interface addresses to which the IPSec profile is applied.

Precautions

This command is supported by IKEv2 only.

 Copyright © Huawei Technologies Co., Ltd.

If the **config-exchange set accept** command is configured on the local device, the **route accept** command must also be configured before the local device can accept subnet route information sent by the remote device and generate routes.

Example

Enable the IKE peer named **peer1** to accept subnet route information from the remote device.

```
<Huawei> system-view
[Huawei] ike peer peer1
[Huawei-ike-peer-peer1] config-exchange set accept
```

Related Topics

12.6.75 ike peer

12.6.149 route accept

12.6.12 connect track

Function

The **connect track** command configures the device to control IPSec tunnel setup according to the NQA test instance, NQA group, BFD session, or BFD group status.

The **undo connect track** command cancels the configuration.

By default, the device is configured not to control IPSec tunnel setup according to the NQA test instance, NQA group, BFD session, or BFD group status.

Format

connect track { **nqa** *admin-name test-name* | **nqa-group** *nqa-group-name* | **bfd-session** *bfd-session-name* | **bfd-session-group** *bfd-group-name* } { **up** | **down** }

undo connect track { **nqa** | **nqa-group** | **bfd-session** | **bfd-session-group** }

Parameters

Parameter	Description	Value
nqa *admin-name test-name*	Configures the device to control IPSec tunnel setup according to the NQA test instance status. *admin-name* and *test-name* specify the administrator name and name of the NQA test instance respectively.	The administrator name or name of an NQA test instance must have been created.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
nqa-group *nqa-group-name*	Configures the device to control IPSec tunnel setup according to the NQA group status. *nqa-group-name* specifies the name of the NQA group.	The value is a string of 1 to 32 case-sensitive characters without spaces. **NOTE** If the character string is quoted by quotation marks, the character string can contain spaces.
bfd-session *bfd-session-name*	Configures the device to control IPSec tunnel setup according to the BFD session status. *bfd-session-name* specifies the name of the BFD session.	The BFD session name must have been created.
bfd-session-group *bfd-group-name*	Configures the device to control IPSec tunnel setup according to the BFD group status. *bfd-group-name* specifies the name of the BFD group.	The value is a string of 1 to 15 case-sensitive characters without spaces. **NOTE** If the character string is quoted by quotation marks, the character string can contain spaces.
up	Indicates that an IPSec tunnel is set up when the NQA test instance, NQA group, BFD session, or BFD group status is Up.	-
down	Indicates that an IPSec tunnel is set up when the NQA test instance, NQA group, BFD session, or BFD group status is Down.	-

Views

View of the IPSec policy established in ISAKMP mode

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

Usage Scenario

On a live network, to improve network reliability, a branch gateway connects to the headquarters using multiple links. The branch gateway needs to determine on which link an IPSec tunnel is established. You can associate IPSec with NQA or BFD so that the branch gateway controls IPSec tunnel setup according to the NQA test instance, NQA group, BFD session, or BFD group status, which ensures that only one link is available at any time.

Prerequisites

- An NQA test instance has been created using the **nqa** command and the NQA test instance type has been set to ICMP using the **test-type** command if **nqa** *admin-name test-name* is specified.
- A BFD session has been created using the **bfd bind peer-ip** command and the BFD session has been set the local and remote discriminators using the **discriminator** command if **bfd-session** *bfd-session-name* is specified.

Precautions

- The device supports only association between IPSec and the NQA test instance of ICMP.
- The NQA test instance, NQA group, BFD session, and BFD group cannot be configured simultaneously in this scenario. That is, the device controls IPSec tunnel setup using a specified IPSec policy according to one of the NQA test instance, NQA group, BFD session, BFD group, and VRRP group status.
- When **nqa-group** *nqa-group-name* is specified, you do not need to create an NQA group first. However, the configuration takes effect only when the NQA group is created and configured using the **nqa-group** and **nqa (nqa-group view)** commands respectively.
- When **bfd-session-group** *bfd-group-name* is specified, you do not need to create a BFD group first. However, the configuration takes effect only when the BFD group is created and configured using the **bfd-group** and **track bfd** commands respectively.
- **connect track** needs to be used with **disconnect track** to implement link redundancy control.

Example

Configure the device to establish an IPSec tunnel when the NAQ test instance (administrator name **admin** and instance name **test**) status is Up in the view of the IPSec policy **policy1** established in ISAKMP mode.

```
<Huawei> system-view
[Huawei] nqa test-instance admin test
[Huawei-nqa-admin-test] test-type icmp
[Huawei-nqa-admin-test] quit
[Huawei] ipsec policy policy1 100 isakmp
[Huawei-ipsec-policy-isakmp-policy1-100] connect track nqa admin test up
```

Configure the device to establish an IPSec tunnel when the status of the NAQ group **ngroup** is Down in the view of the IPSec policy **policy2** established in ISAKMP mode.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> system-view
[Huawei] ipsec policy policy2 200 isakmp
[Huawei-ipsec-policy-isakmp-policy2-200] connect track nqa-group ngroup down
```

Configure the device to establish an IPSec tunnel when the status of the BFD session **test** is Up in the view of the IPSec policy **policy1** established in ISAKMP mode.

```
<Huawei> system-view
[Huawei] interface ethernet 2/0/0
[Huawei-Ethernet2/0/0] ip address 10.1.1.1 255.255.255.0
[Huawei-Ethernet2/0/0] quit
[Huawei] bfd
[Huawei-bfd] quit
[Huawei] bfd test bind peer-ip 10.1.1.2 interface ethernet 2/0/0
[Huawei-bfd-session-test] discriminator local 10
[Huawei-bfd-session-test] discriminator remote 20
[Huawei-bfd-session-test] quit
[Huawei] ipsec policy policy1 100 isakmp
[Huawei-ipsec-policy-isakmp-policy1-100] connect track bfd-session test up
```

Configure the device to establish an IPSec tunnel when the status of the BFD group **bfd-group1** is Down in the view of the IPSec policy **policy2** established in ISAKMP mode.

```
<Huawei> system-view
[Huawei] ipsec policy policy2 200 isakmp
[Huawei-ipsec-policy-isakmp-policy2-200] connect track bfd-session-group bfd-group1 down
```

12.6.13 description

Function

The **description** command configures the description for an IKE user.

The **undo description** command deletes the description of an IKE user.

By default, the description of an IKE user is not configured.

Format

description *description*

undo description

Parameters

Parameter	Description	Value
description	Specifies the description of an IKE user.	The value is a string of 1 to 63 case-sensitive characters.

Views

IKE user view

 Copyright © Huawei Technologies Co., Ltd.

Default Level

2: Configuration level

Usage Guidelines

To identify IKE users, run the **description** command to configure the description for the IKE users. For example, you can describe branches corresponding to IKE users,

Example

Configure the description for an IKE user.

```
<Huawei> system-view
[Huawei] ike user-table 10
[Huawei-ike-user-table-10] user user1
[Huawei-ike-user-table-10-user1] description user1
```

Related Topics

12.6.27 display ike user-table (all views)

12.6.14 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 { **group1** | **group2** | **group5** | **group14** | **group19** | **group20** | **group21** }

undo dh

Parameters

Parameter	Description	Value
group1	Uses the 768-bit DH group in IKE negotiation phase 1.	-
group2	Uses the 1024-bit DH group in IKE negotiation phase 1.	-
group5	Uses the 1536-bit DH group in IKE negotiation phase 1.	-
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.	-

 Copyright © Huawei Technologies Co., Ltd.

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

Views

IKE proposal view, 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** > **group5** > **group2** > **group1**.
- The **group1**, **group2**, and **group5** have potential security risks. The other DH groups are recommended.

Example

Specify the 2048-bit DH group for IKE proposal 10.

```
<Huawei> system-view
[Huawei] ike proposal 10
[Huawei-ike-proposal-10] dh group14
```

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
```

Related Topics

12.6.22 display ike proposal (All views)

12.6.30 display ipsec efficient-vpn

12.6.15 disconnect track

Function

The **disconnect track** command configures the device to control IPSec tunnel teardown according to the NQA test instance, NQA group, BFD session, or BFD group status.

 Copyright © Huawei Technologies Co., Ltd.

The **undo disconnect track** command cancels the configuration.

By default, the device is configured not to control IPSec tunnel teardown according to the NQA test instance, NQA group, BFD session, or BFD group status.

Format

disconnect track { **nqa** *admin-name test-name* | **nqa-group** *nqa-group-name* | **bfd-session** *bfd-session-name* | **bfd-session-group** *bfd-group-name* } { **up** | **down** }

undo disconnect track { **nqa** | **nqa-group** | **bfd-session** | **bfd-session-group** }

Parameters

Parameter	Description	Value
nqa *admin-name test-name*	Configures the device to control IPSec tunnel teardown according to the NQA test instance status. *admin-name* and *test-name* specify the administrator name and name of the NQA test instance respectively.	The administrator name or name of an NQA test instance must have been created.
nqa-group *nqa-group-name*	Configures the device to control IPSec tunnel teardown according to the NQA group status. *nqa-group-name* specifies the name of the NQA group.	The value is a string of 1 to 32 case-sensitive characters without spaces. **NOTE** If the character string is quoted by quotation marks, the character string can contain spaces.
bfd-session *bfd-session-name*	Configures the device to control IPSec tunnel teardown according to the BFD session status. *bfd-session-name* specifies the name of the BFD session.	The BFD session name must have been created.
bfd-session-group *bfd-group-name*	Configures the device to control IPSec tunnel teardown according to the BFD group status. *bfd-group-name* specifies the name of the BFD group.	The value is a string of 1 to 15 case-sensitive characters without spaces. **NOTE** If the character string is quoted by quotation marks, the character string can contain spaces.

 Copyright © Huawei Technologies Co., Ltd.

up	Indicates that an IPSec tunnel is torn down when the NQA test instance, NQA group, BFD session, or BFD group status is Up.	-
down	Indicates that an IPSec tunnel is torn down when the NQA test instance, NQA group, BFD session, or BFD group status is Down.	-

Views

View of the IPSec policy established in ISAKMP mode

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On a live network, to improve network reliability, a branch gateway connects to the headquarters using multiple links. The link where an IPSec tunnel is established needs to be determined. You can associate IPSec with NQA or BFD so that the branch gateway controls IPSec tunnel teardown according to the NQA test instance, NQA group, BFD session, or BFD group status, which ensures that only one link is available at any time.

Prerequisites

- An NQA test instance has been created using the **nqa** command and the NQA test instance type has been set to ICMP using the **test-type** command if **nqa** *admin-name test-name* is specified.
- A BFD session has been created using the **bfd bind peer-ip** command and the BFD session has been set the local and remote discriminators using the **discriminator** command if **bfd-session** *bfd-session-name* is specified.

Precautions

- The device supports only association between IPSec and the NQA test instance of ICMP.
- When **nqa-group** *nqa-group-name* is specified, you do not need to create an NQA group first. However, the configuration takes effect only when the NQA group is created and configured using the **nqa-group** and **nqa (nqa-group view)** commands respectively.
- When **bfd-session-group** *bfd-group-name* is specified, you do not need to create a BFD group first. However, the configuration takes effect only when

 Copyright © Huawei Technologies Co., Ltd.

the BFD group is created and configured using the **bfd-group** and **track bfd** commands respectively.

- **disconnect track** needs to be used with **connect track** to implement link redundancy control.

Example

Configure the device to terminate an IPSec tunnel when the NAQ test instance (administrator name **admin** and instance name **test**) status is Up in the view of the IPSec policy **policy1** established in ISAKMP mode.

```
<Huawei> system-view
[Huawei] nqa test-instance admin test
[Huawei-nqa-admin-test] test-type icmp
[Huawei-nqa-admin-test] quit
[Huawei] ipsec policy policy1 100 isakmp
[Huawei-ipsec-policy-isakmp-policy1-100] disconnect track nqa admin test up
```

Configure the device to terminate an IPSec tunnel when the status of the NAQ group **ngroup** is Down in the view of the IPSec policy **policy2** established in ISAKMP mode.

```
<Huawei> system-view
[Huawei] ipsec policy policy2 200 isakmp
[Huawei-ipsec-policy-isakmp-policy2-200] disconnect track nqa-group ngroup down
```

Configure the device to terminate an IPSec tunnel when the status of the BFD session **test** is Up in the view of the IPSec policy **policy1** established in ISAKMP mode.

```
<Huawei> system-view
[Huawei] interface ethernet 2/0/0
[Huawei-Ethernet2/0/0] ip address 10.1.1.1 255.255.255.0
[Huawei-Ethernet2/0/0] quit
[Huawei] bfd
[Huawei-bfd] quit
[Huawei] bfd test bind peer-ip 10.1.1.2 interface ethernet 2/0/0
[Huawei-bfd-session-test] discriminator local 10
[Huawei-bfd-session-test] discriminator remote 20
[Huawei-bfd-session-test] quit
[Huawei] ipsec policy policy1 100 isakmp
[Huawei-ipsec-policy-isakmp-policy1-100] disconnect track bfd-session test up
```

Configure the device to terminate an IPSec tunnel when the status of the BFD group **bfd-group1** is Down in the view of the IPSec policy **policy2** established in ISAKMP mode.

```
<Huawei> system-view
[Huawei] ipsec policy policy2 200 isakmp
[Huawei-ipsec-policy-isakmp-policy2-200] disconnect track bfd-session-group bfd-group1 down
```

12.6.16 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*]

 Copyright © Huawei Technologies Co., Ltd.

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
--------------------------------------------------------------------------------
```

 Copyright © Huawei Technologies Co., Ltd.

Table 12-16 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	Remote IP address.
port or Port	Peer UDP port number.

Copyright © Huawei Technologies Co., Ltd.

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. • route limit: The number of injected routes has reached the upper limit.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
	• ip assigned fail: IP address allocation fails. • local address mismatch: The local IP address in IKE negotiation and interface IP address do not match. • 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. • netmask mismatch: The mask does not match the configured mask after the IPSec mask filtering function is enabled. • flow confict: A data flow conflict occurs. • proposal mismatch or use sm in ikev2: IPSec proposals at both ends of the IPSec tunnel do not match or IKEv2 uses the SM algorithm. • ikev2 not support sm in ipsec proposal ikev2: IKEv2 does not support the SM algorithm used in the IPSec proposal. • 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. • proposal mismatch or use sm in ikev2: The received IPSec proposal parameters do not match the local parameters or IKEv2 uses the SM algorithm.
version	IKE version.
Error-time/error-time	Time of IPSec tunnel negotiation failures using IKE.

 Copyright © Huawei Technologies Co., Ltd.

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. • route limit: The number of injected routes has reached the upper limit.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
	• ip assigned fail: IP address allocation fails. • local address mismatch: The local IP address in IKE negotiation and interface IP address do not match. • 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. • netmask mismatch: The mask does not match the configured mask after the IPSec mask filtering function is enabled. • flow confict: A data flow conflict occurs. • proposal mismatch or use sm in ikev2: IPSec proposals at both ends of the IPSec tunnel do not match or IKEv2 uses the SM algorithm. • ikev2 not support sm in ipsec proposal ikev2: IKEv2 does not support the SM algorithm used in the IPSec proposal. • 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. • proposal mismatch or use sm in ikev2: The received IPSec proposal parameters do not match the local parameters or IKEv2 uses the SM algorithm. • 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 cert fail or inband cert validate fail: Failed to process or verify the certificate.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
	• outband cert validate fail(rsa-signature): Certificate verification failed during RSA signature authentication. • hash value not equal(pre-share-key): The hash values are different during pre-shared key authentication. • hash value not equal(digital-envelope): The hash values are different during digital signature authentication. • verify sig data fail(rsa-signature): Failed to verify the signature. • proc auth payload fail(pre-share-key): Failed to process the authentication payload during pre-shared key authentication. • proc auth payload fail(rsa-signature): Failed to process the authentication payload during RSA signature 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. • recv peer auth fail notification(rsa-signature): An authentication failure notification from the peer end is received during RSA signature authentication. • recv peer auth fail notification(digital-envelope): An authentication failure notification from the peer end is received during digital signature authentication. • proc and auth ID payload fail(pre-share-key): The peer ID fails to be authenticated during pre-shared key authentication. • proc and auth ID payload fail(rsa-signature): The peer ID fails to be authenticated during RSA signature authentication. • can not find key by cert: Failed to obtain the key pair corresponding to the certificate. • the cert is not valid: The certificate is invalid. • cert revoked by CRL: The certificate is revoked by the CRL. • unable to get issuer cert: The issuer cannot be found. • ocsp valid fail: Failed to check the certificate online. • cert filter check mismatch: The certificate filtering verification does not match. • no corresponding CRL: No corresponding CRL exists. • inband cert validate fail: Failed to verify the certificate.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
	• receive proposal mismatch or use sm in ikev2: The received IPSec proposal parameters do not match the local parameters or IKEv2 uses the SM algorithm.

12.6.17 display ike global config

Function

The **display ike global config** command displays the global IKE configuration.

Format

display ike global config

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run this command to view the global IKE configuration, such as the local name used in IKE negotiation, interval at which an IKE SA sends a heartbeat packet, timeout interval of heartbeat packets, and interval at which an IKE SA sends an NAT keepalive packet.

Example

Display the global IKE configuration.

```
<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
  IKE sm-encryption-key-length    : disable
  IKE certificate-check           : disable
  IKEv2 prf aes-xcbc-128 compatible: enable
------------------------------------------------------------
```

 Copyright © Huawei Technologies Co., Ltd.

Table 12-17 Description of the **display ike global config** command output

Item	Description
IKE Global Config	Global configuration of IKE.
IKE local-name	Local name used in IKE negotiation. To set the local name used in IKE negotiation, run the **ike local-name** command. If **ike local-name** is not configured on the local end, the name specified by the **sysname** command is used for IKE negotiation.
IKE heartbeat-timer interval	Interval at which an IKE SA sends a heartbeat packet, in seconds. To set the interval at which an IKE SA sends a heartbeat packet, run the **ike heartbeat-timer interval** command.
IKE heartbeat-timer timeout	Timeout interval of heartbeat packets, in seconds. To set the timeout interval of heartbeat packets, run the **ike heartbeat-timer timeout** command.
IKE nat-keepalive-timer interval	Interval at which an IKE SA sends an NAT keepalive packet, in seconds. To set the interval at which an IKE SA sends an NAT keepalive packet, run the **ike nat-keepalive-timer interval** command.
IKE sm-encryption-key-length	Whether IKE negotiation packets carry the SM encryption key length when IKE uses a digital envelope for authentication. • enable • disable
IKE certificate-check	Whether validity verification on certificates of all IKE peers is enabled. • enable • disable To configure this function, run the **12.6.65 ike certificate-check disable** command.
IKEv2 prf aes-xcbc-128 compatible	Whether the IKEv2 PRF AES-XCBC-128 algorithm is a non-standard RFC algorithm: • enable • disable This function is configured using the **12.6.84 ikev2 prf aes-xcbc-128 compatible** command. **NOTE** V200R010C10 and later versions support this parameter.

12.6.18 display ike offline-info

Copyright © Huawei Technologies Co., Ltd.

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 :3
  Ike offline information:
--------------------------------------------------------------------------------
  peer              offline-reason       version     offline-time
--------------------------------------------------------------------------------------------------------
  10.10.10.10         dpd-timeout          v2          2015/08/01  16:05:55
  3.3.3.3             dpd-timeout          v2          2015/08/01  16:05:55
  10.2.2.2            hardware-timeout     v2          2015/08/01  15:05:55
--------------------------------------------------------------------------------------------------------
```

Table 12-18 Description of the **display ike offline-info** command output

Item	Description
Current info Num	Current number of information records.
peer	Peer IP address of a deleted IPSec tunnel.

 Copyright © Huawei Technologies Co., Ltd.

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. • peer address switch: An SA is deleted due to change of the peer address. • hard expiry triggered by port mismatch: A hard timeout occurs due to mismatch NAT port number. • kick old sa with same flow: The old SA is deleted for the same incoming flow. • 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. • nhrp notify: NHRP notifies the device that the SA needs to be deleted. • disconnect track nqa/bfd/vrrp: The IPSec tunnel is torn down based on the NQA test instance, NQA group, VRRP, BFD session, or BFD group status. • 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.
version	IKE version.
offline-time	IPSec tunnel deletion time.

 Copyright © Huawei Technologies Co., Ltd.

12.6.19 display ike identity

Function

The **display ike identity** command displays information about an identity filter set.

Format

display ike identity [**name** *identity-name*]

Parameters

Parameter	Description	Value
name *identity-name*	Specifies the name of the identity filter set.	The value is an existing identity filter name.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run this command to display information about an identity filter set.

Example

Display information about all identity filter sets.

```
<Huawei> display ike identity

Number of identity: 2

IKE identity: identity1
 FQDN       : R1
 DN         : c=cn,st=jiangsu,l=nanjing,o=huawei,ou=vpn,cn=ipsec
 User-FQDN  : liming@huawei.com
 User-FQDN  : zhangsan@huawei.com
 IP address : 1.1.1.0 255.255.255.0
 IP address : 2.2.2.0 255.255.255.0
 IP address : 3.3.3.0 255.255.255.0

IKE identity: 1
 FQDN       : R2
 IP address : 4.1.1.0 255.255.255.0
 IP address : 4.1.2.0 255.255.255.0
```

Display information about the identity filter set named **identity1**.

```
<Huawei> display ike identity name identity1
```

 Copyright © Huawei Technologies Co., Ltd.

```
IKE identity: identity1
 FQDN       : R1
 DN         : c=cn,st=jiangsu,l=nanjing,o=huawei,ou=vpn,cn=ipsec
 User-FQDN  : liming@huawei.com
 User-FQDN  : zhangsan@huawei.com
 IP address : 1.1.1.0 255.255.255.0
 IP address : 2.2.2.0 255.255.255.0
 IP address : 3.3.3.0 255.255.255.0
 IP address : 6.6.6.0 255.255.255.0
```

Table 12-19 Description of the display ike identity command output

Item	Description
IKE identity	Name of the identity filter set. To set this parameter, run the **12.6.70 ike identity** command.
Name	Name of the allowed peer for IKE negotiation. To set this parameter, run the **12.6.62 fqdn** command.
DN	DN of the allowed peer. To set this parameter, run the **12.6.49 dn** command.
User-FQDN	User-FQDN of the allowed peer. To set this parameter, run the **12.6.182 user-fqdn** command.
IP address	IP address of the allowed peer. To set this parameter, run the **12.6.90 ip address** command.

Related Topics

12.6.70 ike identity

12.6.20 display ike peer (all views)

Function

The **display ike peer** command displays the IKE peer configuration.

Format

display ike peer [**brief** | **name** *peer-name*]

Parameters

Parameter	Description	Value
brief	Displays brief information about IKE peers.	-

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
name *peer-name*	Displays detailed information about the IKE peer with a specified name.	The value must be an existing IKE peer name.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The **display ike peer** command output contains the following information:

- Name of the IKE peer
- Negotiation mode
- Authentication key
- IKE proposal
- Type of the local ID
- IP address of the IKE peer
- Name of the IKE peer
- Whether NAT traversal is enabled

Example

Display brief configuration of the IKE peer.

```
<Huawei> display ike peer brief
Current ike peer number: 3

-------------------------------------------------------------------------------
Peer name       Version  Exchange-mode   Proposal   Id-type   RemoteAddr
-------------------------------------------------------------------------------
1               v1v2     main           11         IP
peer1           v1v2     main           12         IP
huawei          v1v2     main           13         IP
```

Table 12-20 Description of the **display ike peer brief** command output

Item	Description
Current ike peer number	Current number of IKE peers that have been configured.
Peer name	Number of an IKE peer. To configure an IKE peer, run the **12.6.75 ike peer** command.

Copyright © Huawei Technologies Co., Ltd.

Item	Description
Version	IKE version of the IKE peer: • v1: IKEv1 is enabled. • v2: IKEv2 is enabled. • v1v2: Both IKEv1 and IKEv2 are enabled. To configure an IKE version, run the **12.6.180 version** command.
Exchange-mode	IKEv1 negotiation mode: • main • aggressive • -: not supported. The value is displayed when the IKE peer uses only IKEv2. To configure a negotiation mode, run the **exchange-mode** command.
Proposal	Name of the referenced IKE proposal. To configure an IKE proposal, run the **ike-proposal** command.
Id-type	Local ID type in IKE negotiation. To set the local ID type, run the **local-id-type** command.
RemoteAddr	IP address of the remote IKE peer. To configure an IP address of the remote IKE peer, run the **12.6.134 remote-address (IKE peer view)** command.

Display configuration of the IKE peer.

```
<Huawei> display ike peer

Number of IKE peers: 1
------------------------------------------
  Peer name                     : 1
  IKE version                   : v1v2
  VPN instance                  : vpn1
  Remote IP                     : 1.1.1.1
  Remote IP                     : 2.2.2.2
  Authentic IP address          : -
  Proposal                      : 1
  Pre-shared-key                : %^%#G7(t:%yFw/PVF>Jsva;"zx]oL!sw-8z\C;I}%%RY%^%#
  Local ID type                 : IP
  Local ID                      : -
  Remote ID type                : any
  Remote ID                     : -
  certificate peer-name         : abc
  PKI realm                     : test
  Inband OCSP                   : Enable
  Inband CRL                    : Disable
  cert-request empty-payload    : Enable
```


Copyright © Huawei Technologies Co., Ltd.

```
  VPN instance bound to the SA          : vpna
  NAT-traversal                      : Enable
  Service-scheme name                   : a
  Re-authentication interval(s)         : 333
  IKE user-table                     : 1
  AAA authorization domain              : a
  DSCP                               : -
  Lifetime-notification-message         : Enable
  DPD                                : Enable
  DPD type                           : on-demand
  DPD retry-limit                    : 3
  DPD retransmit-interval(s)            : 30
  DPD idle-time(s)                   : 60
  DPD msg                            : seq-hash-notify
  RSA encryption-padding                : PKCS1
  RSA signature-padding                 : PKCS1
  ipsec sm4 version                  : standard
  Certificate-check                  : Disable
  Resource acl                       : -
  Local ID Certificate Preference       : Enable
  IKEv2 Local ID Reflect             : Enable
-----------------------------------------------
```

Table 12-21 Description of the **display ike peer** command output

Item	Description
Number of IKE peers	Number of IKE peers that have been configured.
Peer name	Name of an IKE peer. To configure an IKE peer, run the **12.6.75 ike peer** command.
IKE version	IKE version of the IKE peer: • v1: IKEv1 is enabled. • v2: IKEv2 is enabled. • v1v2: Both IKEv1 and IKEv2 are enabled. To configure an IKE version, run the **12.6.180 version** command.
VPN instance	VPN instance name. To configure a VPN instance name, run the **12.6.134 remote-address (IKE peer view)** command.
Remote IP	IP address of the remote IKE peer. To configure an IP address of the remote IKE peer, run the **12.6.134 remote-address (IKE peer view)** command.

Copyright © Huawei Technologies Co., Ltd.

Item	Description
Authentic IP address	IP address used for IKE negotiation authentication before NAT translation. To configure the IP address used for IKE negotiation authentication before NAT translation, run the **12.6.134 remote-address (IKE peer view)** command.
Proposal	Referenced IKE proposal. This parameter is available only when the IKE proposal has been configured using the **12.6.78 ike-proposal** command.
Pre-shared-key	Pre-shared key used for authentication. When an IKE proposal referenced by an IKE peer uses pre-shared key authentication, the pre-shared key is used for identity authentication. To configure a pre-shared key, run the **pre-shared-key** command.
Local ID type	Local ID type in IKE negotiation. To set the local ID type, run the **local-id-type** command.
Local ID	Local ID used in IKE negotiation. To set the local ID used in IKE negotiation, run the **ike local-name** or **12.6.118 local-id** command.
Remote ID type	Remote ID type in IKE negotiation. To set the remote ID type, run the **remote-id-type** command.
Remote ID	Remote ID used in IKE negotiation. To configure the remote ID used in IKE negotiation, run the **12.6.136 remote-id** command.
certificate peer-name	Peer name in the specified certificate.
PKI realm	PKI realm bound to the IKE peer. To bind a PKI realm to an IKE peer, run the **12.6.124 pki realm** command.

Copyright © Huawei Technologies Co., Ltd.

Item	Description
Inband OCSP	Whether IKEv2 is used to transmit Online Certificate Status Protocol (OCSP) requests and responses: • Enable • Disable To this function, run the **inband ocsp** command.
Inband CRL	Whether IKEv2 is used to transmit certificate revocation list (CRL) requests and responses: • Enable • Disable To this function, run the **inband crl** command.
cert-request empty-payload	Whether the certificate request payload is empty: • Enable • Disable To configure the device to send certificate requests with empty payload, run the **12.6.10 certificate-request empty-payload enable** command.
VPN instance bound to the SA	Name of the VPN instance bound to the IPSec tunnel. To bind a VPN instance to an IPSec tunnel, run the **12.6.155 sa binding vpn-instance** command.
NAT-traversal	Whether NAT traversal is enabled: • Enable • Disable To enable NAT traversal, run the **nat traversal** command.
Service-scheme name	AAA scheme referenced by an IKE peer. To configure an AAA scheme, run the **12.6.168 service-scheme** command.
Re-authentication interval(s)	IKEv2 re-authentication interval. To configure an IKEv2 re-authentication interval, run the **12.6.133 re-authentication interval** command.

Copyright © Huawei Technologies Co., Ltd.

Item	Description
IKE user-table	IKE user table referenced by an IKE peer. To configure an IKE user table, run the **12.6.179 user-table** command.
AAA authorization domain	AAA authorization domain referenced by an IKE peer. To configure an AAA authorization domain, run the **12.6.1 aaa authorization** command.
DSCP	DSCP value of IKE packets of an IKE peer. To configure a DSCP value, run the **12.6.53 dscp** command.
Lifetime-notification-message	Whether the device is enabled to send notification messages of the IKE SA lifetime: • Enable • Disable To enable this function, run the **12.6.115 lifetime-notification-message enable** command.
DPD	Whether the DPD function is enabled: • Enable • Disable
DPD type	DPD mode of an IKE peer. • on-demand: DPD is performed on demand. • periodic: DPD is performed periodically. To specify a DPD mode, run the **12.6.52 dpd type** command.
DPD retry-limit	Number of times that an IKE peer can retransmit DPD packets. To specify the number of retransmission times, run the **12.6.50 dpd** command.
DPD retransmit-interval(s)	Interval at which an IKE peer retransmits DPD packets. To configure the retransmission interval, run the **12.6.50 dpd** command.
DPD idle-time(s)	DPD idle time of an IKE peer. To configure a DPD idle time, run the **12.6.50 dpd** command.

Copyright © Huawei Technologies Co., Ltd.

Item	Description
DPD msg	Sequence of the payload in DPD packets. • 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. To configure the sequence of the payload, run the **12.6.51 dpd msg** command.
RSA encryption-padding	Padding mode of RSA encryption.
RSA signature-padding	Padding mode of an RSA signature. To specify the padding mode, run the **12.6.152 rsa signature-padding** command.
ipsec sm4 version	Version of the SM4 algorithm.
Certificate-check	Whether validity verification on certificates of an IKE peer is enabled: • Enable • Disable To disable validity verification on certificates of an IKE peer, run the **12.6.9 certificate-check disable** command.
Resource acl	ACL information to be pushed by the headquarters device to the branch. To configure ACL information, run the **12.6.148 resource acl** command.
Local ID Certificate Preference	Whether to enable the device to preferentially obtain the local ID from a field in a certificate when IKE uses certificate negotiation: • Enable • Disable To enable this function, run the **12.6.119 local-id-preference certificate enable** command.

Copyright © Huawei Technologies Co., Ltd.

Item	Description
IKEv2 Local ID Reflect	Whether the local ID of the responder is used as the remote ID carried in the IKE packets sent by the initiator during IKEv2 negotiation: • Enable • Disable To enable this function, run the **12.6.120 local-id-reflect enable** command.

12.6.21 display ike peer ctrl-plane

Function

The **display ike peer ctrl-plane** command displays the IKE peer configuration on control plane.

Format

display ike peer [**brief** | **name** *peer-name*] **ctrl-plane**

Parameters

Parameter	Description	Value
brief	Displays brief information about the IKE peer.	-
name *peer-name*	Specifies the name of IKE peer.	The value is an existing ike peer name.

Views

User view

Default Level

1: Monitoring level

Usage Guidelines

The output of the **display ike peer ctrl-plane** command is as follows:

- Name of the IKE peer
- Negotiation mode
- Authentication key

Copyright © Huawei Technologies Co., Ltd.

- IKE proposal
- Type of the local ID
- IP address of the peer
- Name of the peer
- Whether NAT traversal is enabled

Example

Display configuration of the IKE peer.

```
<Huawei> display ike peer ctrl-plane
Number of IKE peers: 1
------------------------------------------
  Peer name                       : 1
  IKE version                     : v1v2
  VPN instance                    : vpn1
  Remote IP                       : 1.1.1.1
  Remote IP                       : 2.2.2.2
  Authentic IP address            : -
  Proposal                        : 1
  Pre-shared-key                  : %^%#G7(t:%yFw/PVF>Jsva;"zx]oL!sw-8z\C;I}%%RY%^%#
  Local ID type                   : IP
  Local ID                        : -
  Remote ID type                  : any
  Remote ID                       : -
  certificate peer-name           : abc
  PKI realm                       : test
  Inband OCSP                     : Enable
  Inband CRL                      : Disable
  cert-request empty-payload      : Enable
  VPN instance bound to the SA    : vpna
  NAT-traversal                   : Enable
  Service-scheme name             : a
  Re-authentication interval(s)   : 333
  IKE user-table                  : 1
  AAA authorization domain        : a
  DSCP                            : -
  Lifetime-notification-message   : Enable
  DPD                             : Enable
  DPD type                        : on-demand
  DPD retry-limit                 : 3
  DPD retransmit-interval(s)      : 30
  DPD idle-time(s)                : 60
  DPD msg                         : seq-hash-notify
  RSA encryption-padding          : PKCS1
  RSA signature-padding           : PKCS1
  ipsec sm4 version               : standard
  Certificate-check               : Disable
  Resource acl                    : -
  Local ID Certificate Preference : Enable
  IKEv2 Local ID Reflect          : Enable
------------------------------------------
```

Display brief configuration of the IKE peer.

```
<Huawei> display ike peer brief ctrl-plane
Current ike peer number: 3

------------------------------------------------------------------------------
Peer name       Version  Exchange-mode   Proposal   Id-type   RemoteAddr
------------------------------------------------------------------------------
1               v1v2     main           11         IP
peer1           v1v2     main           12         IP
huawei          v1v2     main           13         IP
```

 Copyright © Huawei Technologies Co., Ltd.

Table 12-22 Description of the **display ike peer ctrl-plane** command output

Item	Description
Number of IKE peers	Number of IKE peers that have been configured.
Peer name	Name of the IKE peer.
IKE version/Version	IKE version of the IKE peer: • v1: IKEv1 is enabled. • v2: IKEv2 is enabled. • v1v2: Both IKEv1 and IKEv2 are enabled.
VPN instance	VPN instance name.
Exchange-mode	IKEv1 negotiation mode: • main • aggressive • -: not supported. The value is displayed when the IKE peer uses only IKEv2.
Remote IP/RemoteAddr	IP address of the remote IKE peer.
Authentic IP address	IP address used for IKE negotiation authentication before NAT translation.
Proposal	Name of the IKE proposal.
Pre-shared-key	Pre-shared key used in pre-shared key authentication.
Local ID type/Id-type	Local ID type in IKE negotiation.
Local ID	Local ID used in IKE negotiation.
Remote ID type	Remote ID type in IKE negotiation.
Remote ID	Remote ID used in IKE negotiation.
certificate peer-name	Peer name in the specified certificate.
PKI realm	PKI domain bound to the IKE peer.
Inband OCSP	Whether the IKEv2 for Online Certificate Status Protocol (OCSP) requests and responses is enabled for the IKE peer.
Inband CRL	Whether IKEv2 for certificate revocation list (CRL) requests and responses is enabled for an IKE peer.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
cert-request empty-payload	Whether the certificate request payload carries CA information.
VPN instance bound to the SA	Name of the VPN instance bound to the IPSec tunnel.
NAT-traversal	Whether NAT traversal is enabled.
Service-scheme name	AAA scheme referenced by an IKE peer.
Re-authentication interval(s)	IKEv2 re-authentication interval.
IKE user-table	IKE user table referenced by an IKE peer.
AAA authorization domain	AAA authorization domain referenced by an IKE peer.
DSCP	DSCP value of IKE packets of an IKE peer.
Lifetime-notification-message	Whether the device is enabled to send notification messages of the IKE SA lifetime.
DPD	Whether the DPD function is enabled.
DPD type	DPD mode of an IKE peer. • on-demand: DPD is performed on demand. • periodic: DPD is performed periodically.
DPD retry-limit	Number of times that an IKE peer can retransmit DPD packets.
DPD retransmit-interval(s)	Interval at which an IKE peer retransmits DPD packets.
DPD idle-time(s)	DPD idle time of an IKE peer.
DPD msg	Sequence of the payload in DPD packets. • seq-hash-notify • seq-notify-hash
RSA encryption-padding	Padding mode of RSA encryption.
RSA signature-padding	Padding mode of a RSA signature.
ipsec sm4 version	Version of the SM4 algorithm.
Certificate-check	Whether validity verification on certificates of an IKE peer is enabled.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Resource acl	ACL information to be pushed by the headquarters device to the branch.
Local ID Certificate Preference	Whether to enable the device to preferentially obtain the local ID from a field in a certificate when IKE uses certificate negotiation. • Enable • Disable To enable this function, run the **12.6.119 local-id-preference certificate enable** command.
IKEv2 Local ID Reflect	Whether the local ID of the responder is used as the remote ID carried in the IKE packets sent by the initiator during IKEv2 negotiation. • Enable • Disable To enable this function, run the **12.6.120 local-id-reflect enable** command.

12.6.22 display ike proposal (All views)

Function

The **display ike proposal** command displays the IKE proposal configuration.

Format

display ike proposal [**number** *proposal-number*]

display ike proposal default

Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
number *proposal-number*	Specifies the number of an IKE proposal. A smaller IKE proposal number indicates a higher priority.	The value is an integer that ranges from 1 to 99.
default	Displays a default IKE proposal information.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

IKE proposals are displayed in ascending order of IKE proposal number.

Example

Display the configuration of all IKE proposals.

```
<Huawei> display ike proposal

Number of IKE Proposals: 2

-------------------------------------------
 IKE Proposal: 1
   Authentication Method      : PRE_SHARED
   Authentication Algorithm   : SHA2-256
   Encryption Algorithm       : AES-256
   Diffie-Hellman Group       : MODP-2048
   SA Duration(Seconds)       : 86400
   Integrity Algorithm        : HMAC-SHA2-256
   Prf Algorithm              : HMAC-SHA2-256
-------------------------------------------
```

 Copyright © Huawei Technologies Co., Ltd.

```
-----------------------------------------
IKE Proposal: Default
  Authentication Method      : PRE_SHARED
  Authentication Algorithm   : SHA2-256
  Encryption Algorithm       : AES-256
  Diffie-Hellman Group       : MODP-1024
  SA Duration(Seconds)       : 86400
  Integrity Algorithm        : HMAC-SHA2-256
  Prf Algorithm              : HMAC-SHA2-256
-----------------------------------------
```

Table 12-23 Description of the **display ike proposal** command output

Item	Description
Number of IKE Proposals	Number of the IKE proposal.
IKE Proposal	IKE proposal number. To configure an IKE proposal, run the **ike proposal** command.
Authentication Method	Authentication method used in the IKE proposal: • PRE_SHARED: pre-shared key authentication • RSA-SIGNATURE: RSA signature authentication To configure an authentication method, run the **authentication-method** command.
Authentication Algorithm	Authentication algorithm used in the IKE proposal: • MD5: uses a 128-bit key. • SHA1: uses a 160-bit key. • SHA2-256: uses a 256-bit key. • SHA2-384: uses a 384-bit key. • SHA2-512: uses a 512-bit key. To configure an authentication algorithm, run the **authentication-algorithm** command. **NOTE** The MD5 and SHA-1 algorithms have potential security risks. The SHA2 algorithm is recommended.
Encryption Algorithm	Encryption algorithm used in the IKE proposal: • 3DES: 168-bit 3DES-CBC encryption algorithm • AES-128: 128-bit AES encryption algorithm • AES-192: 192-bit AES encryption algorithm • AES-256: 256-bit AES encryption algorithm • DES: DES-CBC encryption algorithm To configure an encryption algorithm, run the **encryption-algorithm** command. **NOTICE** The DES and 3DES algorithms have potential security risks. The AES algorithm is recommended.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Diffie-Hellman Group	DH group in the IKE proposal: • MODP-768: 768-bit Diffie-Hellman group • MODP-1024: 1024-bit Diffie-Hellman group • MODP-1536: 1536-bit Diffie-Hellman group • MODP-2048: 2048-bit Diffie-Hellman group • ECP-256: 256-bit ECP Diffie-Hellman group • ECP-384: 384-bit ECP Diffie-Hellman group • ECP-521: 521-bit ECP Diffie-Hellman group To configure a DH group, run the **dh** command.
SA Duration(Seconds)	IKE SA lifetime. To set the IKE SA lifetime, run the **sa duration** command.
Integrity Algorithm	Integrity algorithm in the IKE proposal: • AES-XCBC-96: AES-XCBC-96 algorithm • HMAC-MD5-96: HMAC-MD5-96 algorithm • HMAC-SHA1-96: HMAC-SHA1-96 algorithm • HMAC-SHA2-256: HMAC-SHA2-256 algorithm • HMAC-SHA2-384: HMAC-SHA2-384 algorithm • HMAC-SHA2-512: HMAC-SHA2-512 algorithm Only IKEv2 negotiation requires the integrity algorithm. To configure an integrity algorithm, run the **integrity-algorithm** command. **NOTE** The HMAC-MD5-96 and HMAC-SHA1-96 algorithms have potential security risks. The HMAC-SHA2-256, HMAC-SHA2-384, or HMAC-SHA2-512 algorithm is recommended.
Prf Algorithm	Algorithm used to generate a pseudo random number in the IKE proposal: • AES-XCBC-128: AES-XCBC-128 algorithm • HMAC-MD5: HMAC-MD5 algorithm • HMAC-SHA1: HMAC-SHA1 algorithm • HMAC-SHA2-256: HMAC-SHA2-256 algorithm • HMAC-SHA2-384: HMAC-SHA2-384 algorithm • HMAC-SHA2-512: HMAC-SHA2-512 algorithm Only IKEv2 requires the PRF algorithm. To specify an algorithm used to generate a pseudo random number, run the **prf** command. **NOTE** The HMAC-MD5 and HMAC-SHA1 algorithms have potential security risks. The AES-XCBC-128, HMAC-SHA2-256, HMAC-SHA2-384, or HMAC-SHA2-512 algorithm is recommended.

Copyright © Huawei Technologies Co., Ltd.

Related Topics

12.6.76 ike proposal

12.6.78 ike-proposal

12.6.23 display ike proposal ctrl-plane

Function

The **display ike proposal ctrl-plane** command displays the IKE proposal configuration on control plane.

Format

display ike proposal [**number** *proposal-number*] **ctrl-plane**

Parameters

Parameter	Description	Value
number *proposal-number*	Specifies the number of an IKE proposal. A smaller IKE proposal number indicates a higher priority.	The value is an integer that ranges from 1 to 99.

Views

User view

Default Level

1: Monitoring level

Usage Guidelines

None.

Example

Display the configuration of all IKE proposals.

```
<Huawei> display ike proposal number 10 ctrl-plane
-----------------------------------------
 IKE Proposal: 10
   Authentication Method     : PRE_SHARED
   Authentication Algorithm  : SHA2-256
   Encryption Algorithm      : AES-256
   Diffie-Hellman Group      : MODP-1024
   SA Duration(Seconds)      : 86400
   Integrity Algorithm       : HMAC-SHA2-256
   Prf Algorithm             : HMAC-SHA2-256
-----------------------------------------
```

 Copyright © Huawei Technologies Co., Ltd.

Table 12-24 Description of the **display ike proposal ctrl-plane** command output

Item	Description
IKE Proposal	IKE proposal number.
Authentication Method	Authentication mode in the IKE proposal: • PRE_SHARED: pre-shared key authentication. • RSA-SIGNATURE: RSA signature authentication. • DIGITAL-ENVELOPE: digital envelope authentication.
Authentication Algorithm	Authentication algorithm in the IKE proposal: • MD5: uses a 128-bit key. • SHA1: uses a 160-bit key. • SHA2-256: uses a 256-bit key. • SHA2-384: uses a 384-bit key. • SHA2-512: uses a 512-bit key.
Encryption Algorithm	Encryption algorithm in the IKE proposal: • 3DES: 168-bit 3DES-CBC encryption algorithm. • AES-128: 128-bit AES encryption algorithm. • AES-192: 192-bit AES encryption algorithm. • AES-256: 256-bit AES encryption algorithm. • DES: DES-CBC encryption algorithm.
Diffie-Hellman Group	DH group in the IKE proposal: • MODP-768: 768-bit Diffie-Hellman group. • MODP-1024: 1024-bit Diffie-Hellman group. • MODP-1536: 1536-bit Diffie-Hellman group. • MODP-2048: 2048-bit Diffie-Hellman group. • MODP-3072: 3072-bit Diffie-Hellman group. • MODP-4096: 4096-bit Diffie-Hellman group.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
SA Duration(Seconds)	ISAKMP SA Duration used in the IKE proposal.
Integrity Algorithm	Integrity algorithm in the IKE proposal: • AES-XCBC-96: AES-XCBC-96 algorithm. • HMAC-MD5-96: HMAC-MD5-96 algorithm. • HMAC-SHA1-96: HMAC-SHA1-96 algorithm. • HMAC-SHA2-256: HMAC-SHA2-256 algorithm. • HMAC-SHA2-384: HMAC-SHA2-384 algorithm. • HMAC-SHA2-512: HMAC-SHA2-512 algorithm.
Prf Algorithm	Algorithm used to generate a pseudo random number in the IKE proposal: • AES-XCBC-128: AES-XCBC-128 algorithm. • HMAC-MD5: HMAC-MD5 algorithm. • HMAC-SHA1: HMAC-SHA1 algorithm. • HMAC-SHA2-256: HMAC-SHA2-256 algorithm. • HMAC-SHA2-384: HMAC-SHA2-384 algorithm. • HMAC-SHA2-512: HMAC-SHA2-512 algorithm.

12.6.24 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*

 Copyright © Huawei Technologies Co., Ltd.

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, dn, 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.	-
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
  117477243    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 : 3
```

 Copyright © Huawei Technologies Co., Ltd.

```
-------------------------------------------------------------------------------

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 12-25 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.
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.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
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 information :
-------------------------------------------------
Ike Sa phase   : 2
Establish Time : 2015-09-18 18:58:24
PortCfg Index  : 0xe
IKE Peer Name  : zhe
Connection Id  : 67126707
Version        : v1
Flow VPN       :
Peer VPN       :
-------------------------------------------------
Intiator Cookie         : 0x a7b1c107a7a67b1
Responder Cookie        : 0xf70b111e391f79a9
Local Address           : 10.2.1.1
Remote Address          : 10.1.1.1:4500
PFS                     : dh-group14
Flags                   : RD|ST|S
-------------------------------------------------

-------------------------------------------------
Ike Sa phase   : 1
Establish Time :
PortCfg Index  : 0xe
IKE Peer Name  : zhe
Connection Id  : 67125326
Version        : v1
Exchange Mode  : Main
Flow VPN       :
Peer VPN       :
-------------------------------------------------
Intiator Cookie               : 0x a7b1c107a7a67b1
Responder Cookie              : 0xf70b111e391f79a9
Local Address                 : 10.2.1.1
Remote Address                : 10.1.1.1:4500
Encryption Algorithm          : AES-256
Authentication Algorithm      : SHA2-256
Authentication Method         : Pre-Shared key
DPD Capability                : Yes
DPD Enable                    : Yes
Remaining Duration            : 11168
Reference Counter             : 60
Flags                         : RD|ST|S
Remote Id Type                : IP
```

 Copyright © Huawei Technologies Co., Ltd.

```
Remote Id                   : 10.136.24.108
DH Group                    : group14
NAT Traversal Version       : RFC3947
ModeCfg IP                  : 10.10.1.36
-----------------------------------------------

  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 verbose information :
-----------------------------------------------
Ike Sa phase   : 2
Establish Time : 2015-09-18 18:58:24
PortCfg Index  : 0x4
IKE Peer Name  : ptest
Connection Id  : 117440514
Version        : v2
Flow VPN       :
Peer VPN       :
-----------------------------------------------
Intiator Cookie         : 0x10dbb95cdb031726
Responder Cookie        : 0x4ba2840bddcf74fd
Local Address           : 10.2.1.1
Remote Address          : 10.1.1.1:4500
PFS                     : dh-group14
Flags                   : RD|ST|A
-----------------------------------------------

-----------------------------------------------
Ike Sa phase   : 1
Establish Time : 2015-09-18 18:58:24
PortCfg Index  : 0x4
IKE Peer Name  : ptest
Connection Id  : 117440513
Version        : v2
Flow VPN       :
Peer VPN       :
-----------------------------------------------
Intiator Cookie                 : 0x10dbb95cdb031726
Responder Cookie                : 0x4ba2840bddcf74fd
Local Address                   : 10.2.1.1
Remote Address                  : 10.1.1.1:4500
Encryption Algorithm            : AES-256
Authentication Method           : Pre-Shared key
Integrity Algorithm             : hmac-sha2-256
Prf Algorithm                   : hmac-sha2-256
DPD Capability                  : Yes
DPD Enable                      : Yes
Remaining Duration              : 11168
Reference Counter               : 1
Flags                           : RD|ST|A
Remote Id Type                  : IP
Remote Id                       : 10.136.24.108
DH Group                        : group2
Re-authentication remaining time (sec) : -
ModeCfg IP                      : 10.10.1.36
-----------------------------------------------

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

 Copyright © Huawei Technologies Co., Ltd.

```
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 12-26 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. To configure an IKE peer, run the **12.6.75 ike peer** command.
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. To configure an IKE version, run the **12.6.180 version** command.
Exchange Mode	Negotiation mode of the IKEv1 phase 1. • Main: main mode. • Aggressive: aggressive mode. To configure the negotiation mode, run the **12.6.61 exchange-mode** command.
Flow VPN	VPN to which the data flow belongs, run the **12.6.155 sa binding vpn-instance** command.
Peer VPN	VPN to which the peer belongs, run the **12.6.155 sa binding vpn-instance** command.
Intiator Cookie	Cookie of the initiator.
Responder Cookie	Cookie of the responder.
Local Address	Local IP address of an IPSec tunnel. To configure the local IP address of an IPSec tunnel, run the **12.6.174 tunnel local** command.

Copyright © Huawei Technologies Co., Ltd.

Item	Description
Remote Address	Remote IP address and UDP port number of an IPSec tunnel. To configure the remote IP address of an IPSec tunnel, run the **12.6.175 tunnel remote** command.
Encryption Algorithm	Encryption algorithm in the IKE proposal. To configure an encryption algorithm, run the **12.6.56 encryption-algorithm** command.
Authentication Algorithm	Authentication algorithm in the IKE proposal. To configure an authentication algorithm, run the **12.6.6 authentication-algorithm** command.
Authentication Method	Authentication method in the IKE proposal. To configure an authentication method, run the **12.6.7 authentication-method** command.
Integrity Algorithm	Integrity algorithm used in an IKEv2 proposal. To configure an integrity algorithm, run the **12.6.87 integrity-algorithm** command.
Prf Algorithm	Pseudo-random function (PRF) used in an IKEv2 proposal. To configure a PRF algorithm, run the **12.6.128 prf** command.
DPD Capability	Whether DPD capability is successfully negotiated. • Yes • No
DPD Enable	Whether the DPD function is enabled. • Yes • No To enable this function, run the **12.6.52 dpd type** command.
Remaining Duration	Remaining lifetime of an SA.
Reference Counter	Number of IPSec SAs negotiated by the IKE SA.

Copyright © Huawei Technologies Co., Ltd.

Item	Description
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.
PFS	Perfect Forward Secrecy (PFS) when the local end initiates negotiation. To enable this function, run the **12.6.123 pfs** command.
Remote Id Type	Remote ID type. To configure the remote ID type, run the **12.6.137 remote-id-type** command.
Remote Id	Remote ID for IKE negotiation. To configure the remote ID, run the **12.6.136 remote-id** command.
DH Group	DH group in the IKE proposal. To configure a DH group, run the **dh** command.
NAT Traversal Version	Version of NAT traversal. • draft-ietf-ipsec-nat-t-ike-00 • draft-ietf-ipsec-nat-t-ike-02 • RFC3947

Copyright © Huawei Technologies Co., Ltd.

Item	Description
Re-authentication remaining time (sec)	Remaining time for IKEv2 to initiate re-authentication, in seconds. When the IKEv2 re-authentication interval is set on the device and the device functions as the responder, it does not initiate IKEv2 re-authentication. Therefore, the remaining time for IKEv2 to initiate re-authentication displays - in the command output. You can view the remaining time on the initiator.
ModeCfg IP	IP address allocated through mode configuration.
Number of IKE SA	Total number of IKE SAs and IPSec SAs.

12.6.25 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.

Copyright © Huawei Technologies Co., Ltd.

```
<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
------------------------------------------------------------------------------
```

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
------------------------------------------------------------------------------
```

 Copyright © Huawei Technologies Co., Ltd.

Table 12-27 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.
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.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
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.

12.6.26 display ikev2 statistics

Function

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

Format

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

Parameters

Parameter	Description	Value
eap	Displays EAP statistics on IPSec tunnels negotiated using IKEv2.	-

Copyright © Huawei Technologies Co., Ltd.

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, EAP, and notification message statistics on IPSec tunnels negotiated using IKEv2.

Example

Display EAP statistics on IPSec tunnels negotiated using IKEv2.

```
<Huawei> display ikev2 statistics eap

Ikev2 eap and modecfg statistics:
------------------------------------------------------------------------------
Eap user auth success                                :0
Eap auth timeout                                     :0
Eap auth fail                                        :0
Eap user get authorized IP address                   :0
Eap user go online number                            :0
Eap user go offline number                           :0
Eap user cut message                                 :0
Send ip address allocation request                   :0
Send ip address allocation request timeout           :0
Receive ip address allocation request ack            :0
Receive ip address allocation request nack           :0
Send ip address release request                      :0
Receive ip address release request nack              :0
Fail to process the ip address allocation            :0
Ip address allocated fail to save                    :0
Ip address allocated exist but receive duplicate ip request :0
------------------------------------------------------------------------------
```

 Copyright © Huawei Technologies Co., Ltd.

Table 12-28 Description of the **display ikev2 statistics eap** command output

Item	Description
Ikev2 eap and modecfg statistics	IKEv2 EAP and mode configuration statistics.
Eap user auth success	EAP users pass the authentication successfully.
Eap auth timeout	EAP authentication timed out.
Eap auth fail	EAP authentication failed.
Eap user get authorized IP address	EAP users obtained authorized IP addresses.
Eap user go online number	Number of times EAP users go online.
Eap user go offline number	Number of times EAP users go offline.
Eap user cut message	Number of times EAP users are forced offline.
Send ip address allocation request	The device sends an IP address allocation request message.
Send ip address allocation request timeout	The IP address request message times out.
Receive ip address allocation request ack	The device receives an ACK message for the IP address allocation request.
Receive ip address allocation request nack	The device receives an NACK message for the IP address allocation request.
Send ip address release request	The device sends an IP address release request message.
Receive ip address release request nack	The device receives an NACK message for the IP address release request.
Fail to process the ip address allocation	The device fails to process the reply message for the IP address allocation request.
Ip address allocated fail to save	The allocated IP address is not saved in the SA.
Ip address allocated exist but receive duplicate ip request	The device receives a duplicate IP address request message.

 Copyright © Huawei Technologies Co., Ltd.

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 12-29 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.

 Copyright © Huawei Technologies Co., Ltd.

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.

Copyright © Huawei Technologies Co., Ltd.

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
```

 Copyright © Huawei Technologies Co., Ltd.

```
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
------------------------------------------------------------------------------
```

Table 12-30 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.

 Copyright © Huawei Technologies Co., Ltd.

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_CHILD SA notification	Delete_Old_ChildSa notification message.
DSCP payload	DSCP notification 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    :33          Ike_init response send   :0
Ike_init request recv    :10          Ike_init response recv   :0
Ike_auth request send    :10          Ike_auth response send   :0
Ike_auth request recv    :10          Ike_auth response recv   :0
Create_child req send    :91          Create_child resp send   :147
Create_child req recv    :87          Create_child resp recv   :147
Ike_info request send    :210         Ike_info response send   :31
Ike_info request recv    :0           Ike_info response recv   :31
Del_info request send    :209         Del_info response send   :26
Del_info request recv    :0           Del_info response recv   :31
Dpd_info request send    :4           Dpd_info response send   :0
Dpd_info request recv    :0           Dpd_info response recv   :0
--------------------------------------------------------------------------------
```

 Copyright © Huawei Technologies Co., Ltd.

Table 12-31 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 response send	Number of sent ike_init response packets.
Ike_init request recv	Number of received ike_init request packets.
Ike_init response recv	Number of received ike_init response packets.
Ike_auth request send	Number of sent IKE authentication exchange (ike_auth) request packets.
Ike_auth response send	Number of sent ike_auth response packets.
Ike_auth request recv	Number of received ike_auth request packets.
Ike_auth response recv	Number of received ike_auth response packets.
Create_child req send	Number of sent IPSec SA for sub-tunnel creation (create_child) request packets.
Create_child resp send	Number of sent create_child response packets.
Create_child req recv	Number of received create_child request packets.
Create_child resp recv	Number of received create_child response packets.
Ike_info request send	Number of sent IKE notification exchange (ike_info) request packets.
Ike_info response send	Number of sent ike_info response packets.
Ike_info request recv	Number of received ike_info request packets.
Ike_info response recv	Number of received ike_info response packets.
Del_info request send	Number of sent tunnel information deletion (del_info) request packets.
Del_info response send	Number of sent del_info response packets.
Del_info request recv	Number of received del_info request packets.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Del_info response recv	Number of received del_info response packets.
Dpd_info request send	Number of sent DPD information (dpd_info) request packets.
Dpd_info response send	Number of sent dpd_info response packets.
Dpd_info request recv	Number of received dpd_info request packets.
Dpd_info response recv	Number of received dpd_info response packets.

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
-------------------------------------------------------------------------------
```

Table 12-32 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.

Copyright © Huawei Technologies Co., Ltd.

Item	Description
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.
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.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
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.

12.6.27 display ike user-table (all views)

Function

The **display ike user-table** command displays IKE user table information.

Format

display ike user-table [**number** *user-table-id* [**user-name** *user-name*]]

Parameters

Parameter	Description	Value
number *user-table-id*	Specifies the ID of an IKE user table. If this parameter is not specified, the command displays information about all IKE user tables.	The value must be an existing IKE user table ID.
user-name *user-name*	Specifies a user name.	The value must be a user name.

Views

All views

Default Level

1: Monitoring level

Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

You can run this command to check the user ID type, user ID, pre-shared key, and user description in an IKE user table.

Example

Display information about all IKE user tables.

```
<Huawei> display ike user-table
Number of IKE User-tables: 1

------------------------------------------------------------------------------
 IKE User-table: 10, Number of users: 1
------------------------------------------------------------------------------

  User Name            : user1
  User ID-type         : IP
  User ID              : 1.1.1.1
  Pre-shared-key       : %^%#D,Ul0!:u2RM;giQtp4KDzkbm*)=Y[NYF[N6s)SMQ%^%#
  VPN instance         : vrf1
  Description          : USER1
  Interface-assign     : Tunnel0/0/1
```

Table 12-33 Description of the **display ike user-table** command output

Item	Description
Number of IKE User-tables	Number of IKE user tables.
Number of users	Number of IKE users.
IKE User-table	ID of an IKE user table.
User Name	IKE user name. To configure the IKE user name, run the **12.6.178 user** command.
User ID-type	Remote ID type of the IKE peer. • ANY: The remote ID type of the IKE peer is of any type. • ESN: The remote ID type of the IKE peer is an ESN. • FQDN: The remote ID type of the IKE peer is a name. • IP: The remote ID type of the IKE peer is an IP address. • USER-FQDN: The remote ID type of the IKE peer is a user domain name. To configure the remote ID type of an IKE peer, run the **12.6.63 id-type** command.
User ID	Remote ID of the IKE peer. To configure the remote ID of an IKE peer, run the **12.6.63 id-type** command.

Copyright © Huawei Technologies Co., Ltd.

Item	Description
Pre-shared-key	Pre-shared key. To configure the pre-shared key, run the **12.6.127 pre-shared-key (IKE user view)** command.
VPN instance	Name of the VPN instance. To configure the name of a VPN instance, run the **12.6.181 vpn-instance-traffic (IKE user view)** command.
Description	Description of the IKE user table. To configure the description of an IKE user table, run the **12.6.13 description** command.
Interface-assign	Interface with which an IKE user associates. To specify an interface, run the **12.6.88 interface-assign** command.

12.6.28 display ike user-table ctrl-plane

Function

The **display ike user-table ctrl-plane** command displays IKE user table information on control plane.

Format

display ike user-table [**number** *user-table-id* [**user-name** *user-name*]] **ctrl-plane**

Parameters

Parameter	Description	Value
number *user-table-id*	Specifies the ID of an IKE user table. If the name of an IKE user table is not specified, information about all IKE user tables is displayed.	The ID of an IKE user table must already exist.

Views

User view

Copyright © Huawei Technologies Co., Ltd.

Default Level

1: Monitoring level

Usage Guidelines

You can run this command to check the user ID type, user ID, pre-shared key, and user description in an IKE user table.

Example

Display information about all IKE user tables.

```
<Huawei> display ike user-table ctrl-plane
Number of IKE User-tables: 1

------------------------------------------------------------------------------
 IKE User-table: 10, Number of users: 1
------------------------------------------------------------------------------

  User Name             : user1
  User ID-type          : IP
  User ID               : 1.1.1.1
  Pre-shared-key        : %^%#D,Ul0!:u2RM;giQtp4KDzkbm*)=Y[NYF[N6s)SMQ%^%#
  VPN instance          : vrf1
  Description           : USER1
```

Table 12-34 Description of the **display ike user-table ctrl-plane** command output

Item	Description
Number of IKE User-tables	Number of IKE user tables.
Number of users	Number of IKE users.
IKE User-table	ID of an IKE user table.
User Name	IKE user name.
User ID-type	Remote ID type of the IKE peer.
User ID	Remote ID of the IKE peer.
Pre-shared-key	Pre-shared key.
VPN instance	Name of the VPN instance.
Description	Description of the IKE user table.

12.6.29 display interface tunnel-template

Function

The **display interface tunnel-template** command displays information about a tunnel template interface.

 Copyright © Huawei Technologies Co., Ltd.

Format

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

Parameters

Parameter	Description	Value
interface-number	Specifies the number of a tunnel template.	The number must be an existing tunnel template.
main	Displays information about only a tunnel template interface. If a tunnel template interface has no sub-interface, the information about the tunnel template interface is displayed regardless of whether the **main** parameter is specified.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

None.

Example

Displays information about Tunnel template 0.

```
<Huawei> display interface tunnel-template 0
Tunnel-Template0 current state : UP
Line protocol current state : DOWN
Description:ith
Route Port,The Maximum Transmit Unit is 1500
Internet Address is unnumbered, using address of LoopBack0(1.1.1.1/32)
Encapsulation is TUNNEL, loopback not set
Tunnel protocol IPSEC
Current system time: 2013-10-24 14:58:00
    300 seconds input rate 0 bits/sec, 0 packets/sec
    300 seconds output rate 0 bits/sec, 0 packets/sec
    0 seconds input rate 0 bits/sec, 0 packets/sec
    0 seconds output rate 0 bits/sec, 0 packets/sec
    0 packets input,  0 bytes
    0 input error
```

 Copyright © Huawei Technologies Co., Ltd.

```
0 packets output,  0 bytes
0 output error
Input bandwidth utilization  : --
Output bandwidth utilization : --
```

Table 12-35 Description of the **display interface tunnel-template** command output

Item	Description
Tunnel-Template0 current state	Physical status of the tunnel template interface: • **UP**: The physical status of the tunnel template interface is Up. • **DOWN**: The physical status of the tunnel template interface is Down.
Line protocol current state	Link layer protocol status of the tunnel template interface: • **UP**: The link layer protocol status of the tunnel template interface is Up. • **DOWN**: The link layer protocol of the tunnel template interface is Down or no IP address is assigned to the tunnel template interface.
Description	Description of the tunnel template interface.
Route Port	Indicates that the interface is a Layer 3 interface.
The Maximum Transmit Unit is 1500	MTU of the tunnel template interface. The default MTU is 1500 bytes. If the length of a packet is greater than the MTU, it is fragmented before being sent. If fragmentation is disabled, the packet is discarded.
Internet Address is unnumbered, using address of LoopBack0 (1.1.1.1/32)	Indicates that the interface IP address is borrowed from Loopback 0 (1.1.1.1/32).
Encapsulation is TUNNEL	Indicates that the tunnel template interface encapsulates packets in tunnel mode.
loopback not set	Indicates that the loopback mode is not set for the tunnel-template interface.
Tunnel protocol IPSEC	Indicates that the tunnel encapsulation protocol is IPsec.
Current system time	Current time of the system. If a time zone is configured and the daylight saving time begins, the time is displayed in the format of YYYY/MM/DD HH:MM:SS UTC±HH:MM DST.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
300 seconds input rate 0 bits/sec, 0 packets/sec	Receive bit and packet rates on the tunnel template interface within the first 300 seconds. You can run the **set flow-stat interval** command to change the interval at which traffic statistics are collected. The interval must be an integer multiple of 10 and range from 10 to 600, in seconds.
300 seconds output rate 0 bits/sec, 0 packets/sec	Send bit and packet rates on the tunnel template interface within the first 300 seconds. You can run the **set flow-stat interval** command to change the interval at which traffic statistics are collected. The interval must be an integer multiple of 10 and range from 10 to 600, in seconds.
0 seconds input rate 0 bits/sec, 0 packets/sec	Receive bit and packet rates within the interval between two queries.
0 seconds output rate 0 bits/sec, 0 packets/sec	Send bit and packet rates within the interval between two queries.
0 packets input, 0 bytes	Total numbers of packets and bytes received by the tunnel template interface.
0 input error	Number of error packets received by the tunnel template interface.
0 packets output, 0 bytes	Total numbers of packets and bytes sent by the tunnel template interface.
0 output error	Number of error packets sent by the tunnel template interface.
Input bandwidth utilization	"--" indicates that this item is not supported.
Output bandwidth utilization	"--" indicates that this item is not supported.

Related Topics

12.6.89 interface tunnel-template

12.6.30 display ipsec efficient-vpn

Function

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

 Copyright © Huawei Technologies Co., Ltd.

Format

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

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.
remote	Displays the running status of remote devices. **remote** only takes effect on the server.	-

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**.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> display ipsec efficient-vpn name easyvpn_1
==========================================
IPSec efficient-vpn name: easyvpn_1
Using interface         : GigabitEthernet1/0/0
==========================================
 IPSec Efficient-vpn Name  : easyvpn_1
 IPSec Efficient-vpn Mode  : 3 (1:Client 2:Network 3:Network-plus 4:Network-auto-cfg)
 ACL Number                :
 Auth Method               : 8 (8:PSK 9:RSA)
 VPN name                  :
 Local ID Type             : 1 (1:IP 2:Name 3:User-fqdn 9:DN 11:Key-id)
 IKE Version               : 1 (1:IKEv1 2:IKEv2)
 Remote Address            : 1.1.1.1
 Pre Shared Key            :
 DH Group                  : DH group 14
 PFS Type                  : DH group 14
 Remote Name               :
 PKI Object                :
 Re-auth interval          : 300 seconds
 Anti-replay window size   : 32
 Qos pre-classify          : 0 (0:Disable 1:Enable)
 Qos group                 : -
 Service-scheme name       : scheme
 DPD Msg Type
 Sim-based-username Type   : IMEI
 RSA signature-padding     : PKCS1
 Interface loopback        : LoopBack100
 Interface loopback IP     : 1.2.1.1/25
 Dns server IP             : 2.2.2.2, 2.2.2.3
 Wins server IP            : 3.3.3.2, 3.3.3.3
 Dns default domain name   : mydomain.com.cn
 Auto-update url           :
 Auto-update version       :
 IP pool                   : 10.1.1.0/255.255.255.0
 Resource acl list         : 1
   IP address/mask         : 5.1.1.2/255.255.255.255
   Source port number      : 0
   Destination port number : 0
   Protocol ID             : 0
 Resource acl list         : 2
   IP address/mask         : 6.1.1.0/255.255.255.0
   Source port number      : 0
   Destination port number : 0
   Protocol ID             : 0
```

Table 12-36 Description of the **display ipsec efficient-vpn** command output

Item	Description
IPSec Efficient-vpn Name/ 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.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
IPSec Efficient-vpn Mode/ Efficient-vpn mode	Mode used by the Efficient VPN policy. • 1: client • 2: network • 3: network-plus • 4: network-auto-cfg 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 mode used by the Efficient VPN policy: • 8: pre-shared key authentication • 9: RSA signature authentication To configure an authentication mode, run the **authentication-method** command.
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.
Local ID Type	Local ID type in IKE negotiation, 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	Pre-shared key. To configure a pre-shared key, run the **pre-shared-key** command.

Copyright © Huawei Technologies Co., Ltd.

Item	Description
DH Group	DH group used in IKE negotiation: • DH group 1: 768-bit Diffie-Hellman group is used during IKE negotiation. • DH group 2: 1024-bit Diffie-Hellman group is used during IKE negotiation. • DH group 5: 1536-bit Diffie-Hellman group is used during IKE negotiation. • DH group 14: 2048-bit Diffie-Hellman group is used during IKE negotiation. • DH group 19: 256-bit ECP Diffie-Hellman group is used during IKE negotiation. • DH group 20: 384-bit ECP Diffie-Hellman group is used during IKE negotiation. • DH group 21: 521-bit ECP Diffie-Hellman group is used during IKE negotiation. To specify a DH group, run the **dh** command.
PFS Type	Perfect Forward Secrecy (PFS) used in IKE negotiation: • DH group 1: 768-bit Diffie-Hellman group is used during IKE negotiation. • DH group 2: 1024-bit Diffie-Hellman group is used during IKE negotiation. • DH group 5: 1536-bit Diffie-Hellman group is used during IKE negotiation. • DH group 14: 2048-bit Diffie-Hellman group is used during IKE negotiation. • DH group 19: 256-bit ECP Diffie-Hellman group is used during IKE negotiation. • DH group 20: 384-bit ECP Diffie-Hellman group is used during IKE negotiation. • DH group 21: 521-bit ECP Diffie-Hellman group is used during IKE negotiation. To specify a PFS, run the **pfs** command.
Remote Name	Remote name used in IKE negotiation. To configure the remote name used in IKE negotiation, run the **remote-name** command. When the **local-id-type name** command is used, the local and remote names are used for IKE negotiation. If **ike local-name** is not configured on the remote end, the name specified by the **sysname** command is used for IKE negotiation.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
PKI Object	PKI domain bound to the Efficient VPN policy. To bind a PKI domain to an Efficient VPN policy, run the **12.6.124 pki realm** command.
Re-auth interval	IKEv2 re-authentication interval. To configure IKEv2 re-authentication interval, run the **12.6.133 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 **ipsec 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 **12.6.92 ipsec anti-replay enable** command.
Qos pre-classify	Whether pre-extraction of original IP packets is enabled: • 0: Pre-extraction of original IP packets is enabled. • 1: Pre-extraction of original IP packets is disabled. To enable pre-extraction of original IP packets, run the **qos pre-classify** command.
Qos group	QoS group to which IPSec packets belong. To configure the QoS group, run the **qos group** command. - indicates that no QoS group is specified for IPSec packets.
Service-scheme name	Name of the bound service scheme. To configure the name of the bound service scheme, run the **12.6.169 service-scheme (Efficient VPN policy view)** command.
DPD Msg Type	Sequence of the payload in DPD packets. • seq-notify-hash • seq-hash-notify To configure the sequence of the payload, run the **12.6.51 dpd msg** command.
Sim-based-username Type	Type of the SIM card user name. • IMEI: international mobile equipment identity. • IMSI: international mobile subscriber identity.
RSA signature-padding	Padding mode of an RSA signature. To specify the padding mode, run the **12.6.152 rsa signature-padding** command.

Copyright © Huawei Technologies Co., Ltd.

Item	Description
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.
Dns server IP	DNS server IP address. To configure a DNS server IP address, run the **dns** command.
Wins server IP	WINS server IP address. To configure a WINS server IP address, run the **wins** command.
Dns default domain name	DNS domain name. To configure a DNS domain name, run the **dns-name** command.
Auto-update url	URL of the file used to upgrade a remote device. To configure the URL of the file used to upgrade a remote device, run the **auto-update url** command.
Auto-update version	Version number of the version file. To configure the version number of the version file, run the **auto-update url** command.
IP pool	IP address obtained from the address pool.
Resource acl list	Delivered ACL list. The value is the number of configured ACL rules. This field is available only when ACL delivery is enabled using the **resource acl** command.
IP address/mask	Delivered IP address or mask. To specify an IP address or port number, run the **rule (advanced ACL view)** command.
Source port number	Delivered source port number. To specify a source port number, run the **rule (advanced ACL view)** command.
Destination port number	Delivered destination port number. To specify a destination port number, run the **rule (advanced ACL view)** command.
Protocol ID	Delivered protocol ID. To specify a protocol ID, run the **rule (advanced ACL view)** command.

Display the IPSec configuration supported by an Efficient VPN policy.

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

 IKEv1 Global Supported Algorithms
```

 Copyright © Huawei Technologies Co., Ltd.

```
-------------------------------------------------------------
  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 | RSA_SIG

  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 | NULL
  Supported Encryption Algorithms:
    DES | 3DES | AES128 | AES192 | AES256 | NULL
```

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 12-37 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. To configure a DH group on the server, run the **dh** command.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Supported Encryption Algorithms	Supported encryption algorithms when IKEv1 or IKEv2 is used. To configure an authentication algorithm on the server, run the **authentication-algorithm** command.
Supported Authentication Algorithms	Supported authentication algorithms when IKEv1 is used. To configure an authentication algorithm on the server, run the **authentication-algorithm** command.
Supported Authentication Methods	Supported authentication algorithms when IKEv1 is used: • Pre Shared Key: pre-shared key authentication • RSA_SIG: RSA signature authentication To configure an authentication mode on the server, run the **authentication-method** command.
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, run the **12.6.87 integrity-algorithm** command.
Supported PRF	Supported PRF algorithms when IKEv2 is used. To configure a PRF algorithm on the server, run the **prf** command.
IPSEC Global Supported Algorithms	Algorithms supported by the system.
Supported Security Protocols	Security protocol supported by IPSec: ESP. To configure a security protocol, run the **transform** command.
Supported Encapsulation Modes	Encapsulation mode supported by IPSec: tunnel mode. To configure an encapsulation mode, run the **encapsulation-mode** command.

Copyright © Huawei Technologies Co., Ltd.

Item	Description
Supported Authentication Algorithms	Authentication algorithm supported by IPSec. To configure an authentication algorithm on the server, run the **esp authentication-algorithm** command.
Supported Encryption Algorithms	Encryption algorithm supported by IPSec. To configure an encryption algorithm on the server, run the **esp encryption-algorithm** command.

Display running status of remote devices.

```
<Huawei> display ipsec efficient-vpn remote
 Total number of remote : 1

 Local interface         : GigabitEthernet0/0/2
 Client IP address       : 10.1.1.1:500
 Client system MAC       : 5489-98f4-78f4
 Client description      :
 Client alloc address    : 10.1.1.254
 Client version ID       : 2
 Client last upgrade info: Failed to get the upgrade information.
```

Table 12-38 Description of the **display ipsec efficient-vpn remote** command output

Item	Description
Total number of remote	Number of remote devices.
Local interface	Interface bound to an IPSec policy on the server. To bind an IPSec policy group to an interface, run the **12.6.104 ipsec policy (interface view)** command.
Client IP address	IP address of the remote device.
Client system MAC	MAC address of the remote device.
Client description	Device information and version information about the remote device.
Client alloc address	IP address delivered by the Efficient VPN server to the remote device.
Client version ID	Version number of the version file delivered from the server to the remote device.
Client last upgrade info	Information about the last automatic upgrade on the remote device.

Copyright © Huawei Technologies Co., Ltd.

Related Topics

12.6.98 ipsec efficient-vpn (system view)
12.6.97 ipsec efficient-vpn (interface view)

12.6.31 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:
==============================
Interface             : GigabitEthernet1/0/1
remote-address        : 2.1.1.1
remote-port           : 500
VPN-name              : 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
```

 Copyright © Huawei Technologies Co., Ltd.

```
last-offline-time      : 2017-07-17 20:25:31
offline-times-in-24Hour: 1
```

Table 12-39 Description of the **display ipsec history record** command output

Item	Description
IPSec history record	Display history information about IPSec tunnels.
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-name	Name of a VPN instance.
flow-source	Source address segment of data flows.
flow-destination	Destination address segment of data flows.

 Copyright © Huawei Technologies Co., Ltd.

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. • peer address switch: An SA is deleted due to change of the peer address. • hard expiry triggered by port mismatch: A hard timeout occurs due to mismatch NAT port number. • kick old sa with same flow: The old SA is deleted for the same incoming flow. • 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. • nhrp notify: NHRP notifies the device that the SA needs to be deleted. • disconnect track nqa/bfd/vrrp: The IPSec tunnel is torn down based on the NQA test instance, NQA group, VRRP, BFD session, or BFD group status. • 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.
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.

 Copyright © Huawei Technologies Co., Ltd.

12.6.32 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
  IPSec df-bit                                        : copy
  IPSec fragmentation                                 : disable
  IPSec nat-traversal source-port                     : 8000
  IPSec invalid-spi-recovery                          : disable
  IPSec netmask source                                : 24
  IPSec netmask destination                           : 24
------------------------------------------------------------------
```

Table 12-40 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.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
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 **12.6.92 ipsec anti-replay enable** command.
IPSec df-bit	IPSec tunnel don't fragment (DF) bit: • clear: The DF bit is set to 0, allowing packets to be fragmented. • set: The DF bit is set to 1, prohibiting packets from being fragmented. • copy: The DF bit is that of original packets. To set the DF bit, run the **12.6.96 ipsec df-bit** command.
IPSec fragmentation	IPSec tunnel packet fragmentation mode: • enable: Fragmentation before IPSec encryption. • disable: Fragmentation after IPSec encryption To set the fragmentation mode, run the **12.6.99 ipsec fragmentation before-encryption** command.
IPSec nat-traversal source-port	Port number used for IPSec NAT traversal. To configure the port number used for IPSec NAT traversal, run the **12.6.101 ipsec nat-traversal source-port** command.
IPSec invalid-spi-recovery	Whether the invalid SPI recovery function is enabled: • enable • disable To configure the invalid SPI recovery function, run the **12.6.100 ipsec invalid-spi-recovery enable** command.
IPSec netmask source	Source address mask of data flows. To configure the source address mask of data flows, run the **12.6.102 ipsec netmask** command. When the source address mask is not configured, the mask length is 0.
IPSec netmask destination	Destination address mask of data flows. To configure the destination address mask of data flows, run the **12.6.102 ipsec netmask** command. When the destination address mask is not configured, the mask length is 0.

Copyright © Huawei Technologies Co., Ltd.

12.6.33 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        : policy1
  Using interface     : GigabitEthernet1/0/0
  IPSec policy number : 10
  IPSec policy Type   : policy
-------------------------------------------------
```

Table 12-41 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 policy (interface view)**, **ipsec profile (interface view)**, or **ipsec efficient-vpn (interface view)** command.
Using interface	Interface to which an IPSec policy is applied.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
IPSec policy number	Sequence number of the IPSec policy bound to the interface. To configure an IPSec policy, run the **ipsec policy (system view)** or **ipsec profile (system view)** command.
IPSec policy Type	Type of the IPSec policy bound to an interface: • policy: IPSec policy in manual or IKE negotiation mode • profile: IPSec profile • template: IPSec policy template • efficient-vpn: Efficient VPN policy

12.6.34 display ipsec policy (all views)

Function

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

Format

display ipsec policy [**brief** | **name** *policy-name* [*seq-number*]]

Parameters

Parameter	Description	Value
brief	Displays brief information about all IPSec policies.	-
name *policy-name*	Displays detailed information about an IPSec policy with a specified name.	The value must be an existing IPSec policy name.
seq-number	Displays detailed information about an IPSec policy with a specified sequence number.	The value must be an existing IPSec policy sequence number.

Views

All views

Default Level

1: Monitoring level

Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

If no parameter is specified, this command displays detailed information about all IPSec policies.

You can use the **display ipsec policy brief** command to check brief information about all IPSec policies, including:

- Name and sequence number
- Negotiation mode
- ACL number
- IKE peer
- Local address
- Remote address

Using the **name** parameter, you can view details on the specified IPSec policy. In this case, the information is displayed in detailed format. If you specify **name** *policy-name* and do not specify *seq-number*, the command displays detailed information about an IPSec policy group.

Example

Display brief information about all the IPSec policies.

```
<Huawei> display ipsec policy brief
Number of policies group : 1
Number of policies       : 1

Policy name          Mode     ACL        Peer name   Local address    Remote address
------------------------------------------------------------------------------------------
policy1-100          isakmp   3002/IPv4  peer1
```

Table 12-42 Description of the **display ipsec policy brief** command output

Item	Description
Number of policies group	Number of IPSec policy groups. An IPSec policy is identified by its name and sequence number, and multiple IPSec policies with the same name constitute an IPSec policy group.
Number of policies	Number of IPSec policies.
Policy name	Name and sequence number of an IPSec policy. To configure an IPSec policy, run the **ipsec policy (system view)** command.

Copyright © Huawei Technologies Co., Ltd.

Item	Description
Mode	Mode in which an IPSec policy is created: • isakmp: The IPSec policy is created in IKE negotiation mode. • template: The IPSec policy is created using an IPSec policy template. • manual: The IPSec policy is created manually. To configure IPSec policy creation mode, run the **ipsec policy (system view)** command.
ACL	ACL referenced in the IPSec policy. To reference an ACL in an IPSec policy, run the **security acl** command.
Peer name	Name of the IKE peer referenced in the IPSec policy. To configure an IKE peer, run the **ike-peer** command.
Local address	Local IP address used in IPSec negotiation. To configure the local IP address used in IPSec negotiation, run the **12.6.174 tunnel local** command.
Remote address	Remote IP address used in IPSec negotiation. To configure the remote IP address used in IPSec negotiation, run the **12.6.175 tunnel remote** command.

Display information about all IPSec policies.

```
<Huawei> display ipsec policy
==========================================
IPSec policy group: "10"
Using interface: GigabitEthernet6/0/0
==========================================
    Sequence number: 10
    Policy Alias: map1-10
    Security data flow: 3000/IPv4
    Peer name    :  rut2
    Perfect forward secrecy: DH group 14
    Proposal name:  prop1
    IPSec SA local duration(time based): 3600 seconds
    IPSec SA local duration(traffic based): 1843200 kilobytes
    SA trigger mode: Traffic-based
    Route inject: None
    Route inject state: -
    Route inject nexthop: -
    Route inject preference: -
    Policy state: Enable
    Anti-replay window size: 1024
    Fragment before-encryption: Disable
```

 Copyright © Huawei Technologies Co., Ltd.

```
  Respond-only: Enable
  Policy status  : Inactive
  Qos pre-classify: Disable
  Qos group: -
  Sa keep-holding-to hard-duration : Disable
```

Table 12-43 Description of the **display ipsec policy** command output

Item	Description
IPSec policy group	Name of an IPSec policy group. To configure an IPSec policy group, run the **ipsec policy (system view)** command.
Using interface	Interface to which an IPSec policy group is applied.
Sequence number	Sequence number of an IPSec policy. To configure a sequence number, run the **ipsec policy (system view)** command.
Policy Alias	Alias of the IPSec policy. To configure an alias for an IPSec policy, run the **12.6.2 alias** command.
Security data flow	ACL referenced in the IPSec policy. To reference an ACL in an IPSec policy, run the **security acl** command.
Peer name	IKE peer referenced in the IPSec policy. To configure an IKE peer, run the **ike-peer** command.

Copyright © Huawei Technologies Co., Ltd.

Item	Description
Perfect forward secrecy	Perfect Forward Secrecy (PFS) used in IKE negotiation: • DH group 1: 768-bit Diffie-Hellman group is used during IKE negotiation. • DH group 2: 1024-bit Diffie-Hellman group is used during IKE negotiation. • DH group 5: 1536-bit Diffie-Hellman group is used during IKE negotiation. • DH group 14: 2048-bit Diffie-Hellman group is used during IKE negotiation. • DH group 19: 256-bit ECP Diffie-Hellman group is used during IKE negotiation. • DH group 20: 384-bit ECP Diffie-Hellman group is used during IKE negotiation. • DH group 21: 521-bit ECP Diffie-Hellman group is used during IKE negotiation. To configure the PFS used in IKE negotiation, run the **pfs** command.
Proposal name	IPSec proposal referenced in the IPSec policy. To reference an IPSec proposal, run the **proposal** command.
IPSec SA local duration(time based)	Time-based IPSec SA lifetime. To set the time-based lifetime of the local SA, run the **sa duration time-based** command in the IPSec policy view.
IPSec SA local duration(traffic based)	Traffic-based IPSec SA lifetime. To set the traffic-based lifetime of the local SA, run the **sa duration traffic-based** command in the IPSec policy view.
SA trigger mode	SA trigger mode: • Automatic • Traffic-based To configure an SA trigger mode, run the **sa trigger-mode** command.

Copyright © Huawei Technologies Co., Ltd.

Item	Description
Route inject state	Route injection status: • Dynamic, Preference: Dynamic route injection is enabled and a priority is configured for the static routes generated through route injection. • Static, Preference: Static route injection is enabled and a priority is configured for the static routes generated through route injection. • None: Route injection is disabled. • Dynamic: Dynamic route injection is enabled. • Static: Static route injection is enabled. To configure route injection, run the **route inject** command.
Route inject nexthop	Next hop of a generated route. To configure route injection, run the **route inject** command.
Route inject preference	Priority of a generated route. To configure route injection, run the **route inject** command.
Policy state	Policy status: • Enable • Disable
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 **12.6.5 anti-replay window** command.
Fragment before-encryption	IPSec fragmentation mode: • Enable: IPSec packets are fragmented before encryption. • Disable: IPSec packets are fragmented after encryption. To configure an IPSec fragmentation mode, run the **12.6.99 ipsec fragmentation before-encryption** command.

Copyright © Huawei Technologies Co., Ltd.

Item	Description
Respond-only	Whether the local end is enabled to initiate IPSec negotiation when an IPSec policy in ISAKMP mode is used to create an IPSec tunnel. • Enable: The local end functions as the IPSec responder and does not initiate IPSec negotiation. • Disable: The local end initiates IPSec negotiation.
Policy status	IPSec policy status: • Active • Inactive To set an IPSec policy to the active state, run the **12.6.125 policy enable** command.
Qos pre-classify	Pre-extraction of original IP packets. To configure pre-extraction of original IP packets, run the **12.6.132 qos pre-classify** command.
Qos group	QoS group to which the IPSec packets belong. To configure the QoS group, run the **12.6.131 qos group** command.
Sa keep-holding-to hard-duration	Whether the device deletes the original IPSec SA after the hard lifetime expires during IPSec SA re-negotiation. • Enable: The device will delete the original IPSec SA after the hard lifetime expires. • Disable: The device deletes the original IPSec SA immediately. To configure the device to delete the original IPSec SA after the hard lifetime expires, run the **12.6.161 sa keep-holding-to hard-duration** command.

12.6.35 display ipsec policy ctrl-plane

Function

Using the **display ipsec policy ctrl-plane** command, you can view information about the IPSec policy on control plane.

Copyright © Huawei Technologies Co., Ltd.

Format

display ipsec policy [**brief** | **name** *policy-name* [*seq-number*]] **ctrl-plane**

Parameters

Parameter	Description	Value
brief	Displays brief information about all the IPSec policies.	-
name *policy-name*	Specifies the name of an IPSec policy.	The value is an existing IPSec policy name.
seq-number	Specifies the sequence number of an IPSec policy	The value is an existing IPSec policy number.

Views

User view

Default Level

1: Monitoring level

Usage Guidelines

If the policy name or the sequence number is not specified, detailed information about all IPSec policies is displayed.

Using the **display ipsec policy brief ctrl-plane** command, you can view the following brief information about all IPSec policies. In this case, the information is displayed in brief format.

- Name and sequence number
- Negotiation mode
- ACL number
- IKE peer
- Local address
- Remote address

Using the **name** parameter, you can view details on the specified IPSec policy. In this case, the information is displayed in detailed format. If you specify **name** *policy-name* and do not specify *seq-number*, the command displays detailed information about an IPSec policy group.

Example

Display brief information about all the IPSec policies.

```
<Huawei> display ipsec policy brief ctrl-plane
Number of policies group : 1
```

 Copyright © Huawei Technologies Co., Ltd.

```
Number of policies      : 1

Policy name          Mode     ACL   Peer name   Local address    Remote address
------------------------------------------------------------------------------
policy1-100          isakmp   3002  peer1       60.1.1.1         60.1.1.2
```

Table 12-44 Description of the **display ipsec policy brief ctrl-plane** command output

Item	Description
Number of policies group	Number of IPSec policy groups. An IPSec policy is identified by its name and sequence number and multiple IPSec policies with the same IPSec policy name constitute an IPSec policy group.
Number of policies	Number of IPSec policies.
Policy name	Name and sequence number of an IPSec policy.
Mode	Mode in which an IPSec policy is created: • isakmp: An IPSec policy is created in IKE negotiation mode. • template: An IPSec policy is created using an IPSec policy template. • manual: An IPSec policy is created manually.
ACL	ACL referenced by the IPSec policy.
Peer name	Name of the IKE peer referenced by the IPSec policy.
Local address	Local IP address used in IKE negotiation (Only the manual mode IPSec policies display the local address).
Remote address	Remote IP address used in IKE negotiation (Only the manual mode IPSec policies display the remote address).

View the information about the security policy.

```
<Huawei> display ipsec policy ctrl-plane
==========================================
IPSec policy group: "10"
Using interface: {GigabitEthernet6/0/0}
==========================================
    Policy Alias: map1-10
    Security data flow: 3000
```

 Copyright © Huawei Technologies Co., Ltd.

```
Peer name    : rut2
Perfect forward secrecy: None
Proposal name:  prop1
IPSec SA local duration(time based): 3600 seconds
IPSec SA local duration(traffic based): 1843200 kilobytes
SA trigger mode: Traffic-based
Route inject: None
Policy state: Enable
Anti-replay: -
Anti-replay window size: 1024
Fragment before-encryption: Disable
Respond-only: Disable
Policy status  : Inactive
Qos pre-classify: Disable
Qos group: -
```

Table 12-45 Description of the **display ipsec policy ctrl-plane** command output

Item	Description
IPsec policy group	Name of an IPSec policy group.
Using interface	Interface to which the IPSec policy group is applied.
sequence number	sequence number of an IPSec policy.
Security data flow	ACL used by an IPSec policy.
Peer name	IKE peer end used in the IPSec policy.
Perfect forward secrecy	DH group used by the PFS function: • DH group 1: 768-bit Diffie-Hellman group is used during IKE negotiation. • DH group 2: 1024-bit Diffie-Hellman group is used during IKE negotiation. • DH group 5: 1536-bit Diffie-Hellman group is used during IKE negotiation. • DH group 14: 2014-bit Diffie-Hellman group is used during IKE negotiation. • None: PFS is not used during IKE negotiation.
Proposal name	IPSec proposal used by an IPSec policy.
IPSec SA local duration(time based)	Time-based IPSec SA duration.
IPSec SA local duration(traffic based)	traffic-based IPSec SA duration.
SA trigger mode	SA trigger mode: • Automatic. • Traffic-based.

Copyright © Huawei Technologies Co., Ltd.

Route inject	Route injection status: • Dynamic, Preference: Dynamic route injection is enabled and a priority is configured for the static route generated through route injection. • Static, Preference: Static route injection is enabled and a priority is configured for the static route generated through route injection. • None: Route injection is disabled.
Policy state	Policy status: • Enable. • Disable.

Anti-replay	Whether the Anti-replay function is enabled.
Anti-replay window size	IPSec anti-replay window size. This field is available only when the IPSec anti-replay function is enabled.
Fragment before-encryption	IPSec fragment mode: • Enable: fragment before encryption. • Disable: Fragment after encryption.
Respond-only	Whether the local end is enabled to initiate IPSec negotiation when an IPSec policy in ISAKMP mode is used to create an IPSec tunnel. • Enable: The local end functions as the IPSec responder and does not initiate IPSec negotiation. • Disable: The local end initiates IPSec negotiation.
Policy status	IPSec policy status: • Active. • Inactive.
Qos Pre-classify	Pre-extraction of original IP packets.
Qos group	QoS group to which the IPSec packets belong.

12.6.36 display ipsec policy-template (all views)

 Copyright © Huawei Technologies Co., Ltd.

Function

The **display ipsec policy-template** command displays IPSec policy template information.

Format

display ipsec policy-template [**brief** | **name** *policy-template-name* [*seq-number*]]

Parameters

Parameter	Description	Value
brief	Displays brief information about all IPSec policy templates.	-
name *policy-template-name*	Displays detailed information about the IPSec policy template with a specified name.	The value must be an existing IPSec policy template name.
seq-number	Displays detailed information about the IPSec policy template with a specified sequence number.	The value must be an existing IPSec policy template sequence number.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

If no parameter is specified, this command displays detailed information about all IPSec policy templates.

You can use the **display ipsec policy-template brief** command to check the following brief information about all IPSec policy templates, including:

- Template name and sequence number
- ACL number
- IKE Peer

If **name** is specified, the command displays detailed information about the IPSec policy template. If you specify **name** and do not specify *seq-number*, the command displays detailed information about an IPSec policy template group.

Example

Display brief information about all IPSec policy templates.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> display ipsec policy-template brief
Number of templates group : 1
Number of templates       : 1

Policy template name     ACL          Peer name
-------------------------------------------------------
temp1-10                 3001/IPv4    rut3
```

Table 12-46 Description of the **display ipsec policy-template brief** command output

Item	Description
Number of templates group	Number of IPSec policy template groups. An IPSec policy template is identified by its name and sequence number. Multiple IPSec policy templates with the same IPSec policy template name constitute an IPSec policy template group.
Number of templates	Number of IPSec policy templates.
Policy template name	Name and sequence number of an IPSec policy template. To configure an IPSec policy template, run the **ipsec policy-template** command.
ACL	ACL referenced in the IPSec policy template. To reference an ACL in an IPSec policy template, run the **security acl** command.
Peer name	Name of the IKE peer referenced in the IPSec policy template. To reference an IKE peer, run the **ike-peer** command.

Display information about a specified IPSec policy template group.

```
<Huawei> display ipsec policy-template name tem3

=============================================
IPSec policy template group: "tem3"
=============================================

  Sequence number: 1
  Policy Alias: tem3-1
  Security data flow: 3001/IPv4
  Peer name    :  zc3
  Perfect forward secrecy: DH group 14
  Proposal name:  3
  IPSec SA local duration(time based): 3600 seconds
  IPSec SA local duration(traffic based): 1843200 kilobytes
  Anti-replay window size: 1024
  Fragment before-encryption: Disable
  Route inject state: -
  Route inject nexthop: -
  Route inject preference: -
  Policy state: Enable
  Qos pre-classify: Enable
```

 Copyright © Huawei Technologies Co., Ltd.

```
Qos group: -
Sa keep-holding-to hard-duration : Disable
```

Table 12-47 Description of the **display ipsec policy-template name** command output

Item	Description
IPSec policy template group	Name of an IPSec policy template. To configure an IPSec policy template, run the **ipsec policy-template** command.
Sequence number	Sequence number of an IPSec policy template. To configure an IPSec policy template, run the **ipsec policy-template** command.
Policy Alias	Alias of an IPSec policy template. To configure an alias, run the **12.6.2 alias** command.
Security data flow	ACL referenced in the IPSec policy template. To reference an ACL referenced in an IPSec policy template, run the **security acl** command.
Peer name	Name of the IKE peer referenced in the IPSec policy template. To reference an IKE peer, run the **ike-peer** command.
Perfect forward secrecy	Perfect Forward Secrecy (PFS) used in IKE negotiation: • DH group 1: 768-bit Diffie-Hellman group is used during IKE negotiation. • DH group 2: 1024-bit Diffie-Hellman group is used during IKE negotiation. • DH group 5: 1536-bit Diffie-Hellman group is used during IKE negotiation. • DH group 14: 2048-bit Diffie-Hellman group is used during IKE negotiation. • DH group 19: 256-bit ECP Diffie-Hellman group is used during IKE negotiation. • DH group 20: 384-bit ECP Diffie-Hellman group is used during IKE negotiation. • DH group 21: 521-bit ECP Diffie-Hellman group is used during IKE negotiation. To specify an algorithm used to generate a pseudo random number, run the **pfs** command.
Proposal name	Name of an IPSec proposal referenced in the IPSec policy template. To reference an IPSec proposal, run the **proposal** command.
IPSec SA local duration(time based)	Time-based lifetime of the local SA. To set the time-based lifetime of the local SA, run the **sa duration time-based** command.

Copyright © Huawei Technologies Co., Ltd.

Item	Description
IPSec SA local duration(traffic based)	Traffic-based lifetime of the local SA. To set the traffic-based lifetime of the local SA, run the **sa duration traffic-based** 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 **ipsec anti-replay window** command.
Fragment before-encryption	Packet fragmentation mode for an IPSec tunnel: • Enable: IPSec packets are fragmented before encryption. • Disable: IPSec packets are fragmented after encryption. To configure a packet fragmentation mode for an IPSec tunnel, run the **12.6.99 ipsec fragmentation before-encryption** command.
Route inject state	Route injection status. Dynamic: Dynamic route injection is enabled To configure route injection, run the **route inject** command.
Route inject nexthop	Next hop of a generated route. To configure route injection, run the **route inject** command.
Route inject preference	Priority of a generated route. To configure route injection, run the **route inject** command.
Policy state	Status of the IPSec policy that references the IPSec policy template: • Enable: The IPSec policy is enabled. • Disable: The IPSec policy is disabled. To set an IPSec policy to the state, run the **12.6.125 policy enable** command.
Qos pre-classify	Pre-extraction of original IP packets. To configure pre-extraction of original IP packets, run the **12.6.132 qos pre-classify** command.
Qos group	QoS group to which the IPSec packets belong. To configure the QoS group, run the **12.6.131 qos group** command.

Copyright © Huawei Technologies Co., Ltd.

Item	Description
Sa keep-holding-to hard-duration	Whether the device deletes the original IPSec SA after the hard lifetime expires during IPSec SA re-negotiation. • Enable: The device will delete the original IPSec SA after the hard lifetime expires. • Disable: The device deletes the original IPSec SA immediately. To configure the device to delete the original IPSec SA after the hard lifetime expires, run the **12.6.161 sa keep-holding-to hard-duration** command.

12.6.37 display ipsec policy-template ctrl-plane

Function

The **display ipsec policy-template ctrl-plane** command displays information about the IPSec policy template on control plane.

Format

display ipsec policy-template [**brief** | **name** *policy-template-name* [*seq-number*]] **ctrl-plane**

Parameters

Parameter	Description	Value
brief	Displays brief information about all the IPSec policy templates.	-
name *policy-template-name*	Specifies the name of an IPSec policy template.	The value is an existing IPSec policy template name.
seq-number	Specifies the sequence number of an IPSec policy template.	The value is an existing IPSec policy template number.

Views

User view

Default Level

1: Monitoring level

Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

If the no parameter is not specified, detailed information about all IPSec policy templates is displayed.

If **brief** is specified, you can view the following brief information about the IPSec policy template. In this case, the information is displayed in brief format.

- Template name and sequence number
- ACL number
- IKE Peer

If **name** is specified, the command displays detailed information about the IPSec policy template.

Example

Display information about all the IPSec policy template.

```
<Huawei> display ipsec policy-template brief ctrl-plane
Number of templates group : 1
Number of templates       : 1

Policy template name     ACL          Peer name
-----------------------------------------------------------
temp1-10                              rut3
```

Table 12-48 Description of the **display ipsec policy-template brief ctrl-plane** command output

Item	Description
Number of templates group	Number of IPSec policy template groups. An IPSec policy template is identified by its name and sequence number and multiple IPSec policy templates with the same IPSec policy template name constitute an IPSec policy template group.
Number of templates	Number of IPSec policy templates.
Policy template name	Name and sequence number of an IPSec policy template.
ACL	ACL used by an IPSec policy template.
Peer name	IKE peer involved.

Display information about a specified IPSec policy template.

```
<Huawei> display ipsec policy-template name tem3 ctrl-plane

=============================================
IPSec policy template group: "tem3"
=============================================
```

 Copyright © Huawei Technologies Co., Ltd.

```
Sequence number: 1
Policy Alias: tem3-1
Security data flow: 0
Peer name    : zc3
Perfect forward secrecy: None
Proposal name:  3
IPSec SA local duration(time based): 3600 seconds
IPSec SA local duration(traffic based): 1843200 kilobytes
Anti-replay: -
Anti-replay window size: 1024
Fragment before-encryption: Disable
Route inject: None
Policy state: Enable
Qos pre-classify: Enable
Qos group: -
```

Table 12-49 Description of the **display ipsec policy-template name tem3 ctrl-plane** command output

Item	Description
IPSec policy template group	Name of an IPSec policy template.
Sequence number	Sequence number in the IPSec policy template.
Policy Alias	Alias of the IPSec policy template.
Security data flow	ACL referenced by the IPSec policy template.
Peer name	Name of the IKE peer referenced by the IPSec policy template.
Perfect forward secrecy	Perfect Forward Secrecy (PFS) used in IKE negotiation: • DH group 1: 768-bit Diffie-Hellman group is used during IKE negotiation. • DH group 2: 1024-bit Diffie-Hellman group is used during IKE negotiation. • DH group 5: 1536-bit Diffie-Hellman group is used during IKE negotiation. • DH group 14: 2014-bit Diffie-Hellman group is used during IKE negotiation. • DH group 19: 256-bit ECP Diffie-Hellman group is used during IKE negotiation. • DH group 20: 384-bit ECP Diffie-Hellman group is used during IKE negotiation. • DH group 21: 521-bit ECP Diffie-Hellman group is used during IKE negotiation. • None: PFS is not used during IKE negotiation.
Proposal name	Name of an IPSec proposal referenced by the IPSec policy template.
IPSec SA local duration(time based)	Time-based lifetime of the local SA.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
IPSec SA local duration(traffic based)	Traffic-based lifetime of the local SA.
Anti-replay	Whether IPSec anti-replay is enabled in an IPSec policy template: • Enable: IPSec anti-replay is enabled. • -: IPSec anti-replay is disabled for an IPSec tunnel. The global IPSec anti-replay function is used.
Anti-replay window size	IPSec anti-replay window size.
Fragment before-encryption	Packet fragmentation mode for an IPSec tunnel: • Enable: IPSec packets are fragmented before encryption. • Disable: IPSec packets are fragmented after encryption.
Route inject	Route injection status: • Dynamic , Preference: Dynamic route injection is enabled and a priority is configured for the route generated through route injection. • Static , Preference: Dynamic route injection is enabled and a priority is configured for the route generated through route injection. • None: Route injection is disabled.
Policy state	Status of the IPSec policy that references the IPSec policy template: • Enable: The IPSec policy is enabled. • Disable: The IPSec policy is disabled.
Qos Pre-classify	Pre-extraction of original IP packets.
Qos group	QoS group to which the IPSec packets belong.

12.6.38 display ipsec profile (all views)

Function

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

Format

display ipsec profile [**brief** | **name** *profile-name*]

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
brief	Displays brief information about all IPSec profiles.	-
name *profile-name*	Displays information about the specified IPSec profile.	The value must be an existing IPSec profile name.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

If no parameter is specified, you can view information about all IPSec profiles.

If the **brief** parameter is specified, you can view brief information about all IPSec policies.

If the **name** parameter is specified, you can view detailed information about the specified IPSec policy.

Example

Display brief information about all IPSec profiles.

```
<Huawei> display ipsec profile brief
 Total number of IPSec profile: 1
 Profile name      Peer name
 ---------------------------------
 a                 spub
```

Table 12-50 Description of the **display ipsec profile brief** command output

Item	Description
Total number of IPSec profile	Number of IPSec profiles on a device.
Profile name	Name of an IPSec profile. To configure an IPSec profile, run the **ipsec profile (system view)** command.
Peer name	Name of the IKE peer referenced by the IPSec profile. To reference an IKE peer, run the **ike-peer** command.

Display information about IPSec profile **a**.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> display ipsec profile name a
==========================================
IPSec profile  : a
Using interface: Tunnel0/0/1
==========================================
 IPSec Profile Name        : a
 Peer Name                 : -
 PFS   Group               : DH group 14
 SecondsFlag               : 0 (0:Global 1:Local)
 SA Life Time Seconds      : 3600
 KilobytesFlag             : 0 (0:Global 1:Local)
 SA Life Kilobytes         : 1843200
 Anti-replay Window Size   : 1024
 Fragment Before-encryption: Disable
 Number of IPSec Proposals : 0
 IPSec Proposals Name      : -
 IKE Identity Name         : identity1
 Qos Pre-classify          : 0 (0:Disable 1:Enable)
 Qos group                 : -
```

Table 12-51 Description of the **display ipsec profile name** command output

Item	Description
IPSec profile	Name of an IPSec profile. To configure an IPSec profile, run the **ipsec profile (system view)** command.
Using interface	Interface to which an IPSec profile is applied.
IPSec Profile Name	Name of an IPSec profile. To configure an IPSec profile, run the **ipsec profile (system view)** command.
Peer Name	Name of the IKE peer referenced by the IPSec profile. To reference an IKE peer, run the **ike-peer** command.

Copyright © Huawei Technologies Co., Ltd.

Item	Description
PFS Group	Perfect Forward Secrecy (PFS) used in IKE negotiation: • DH group 1: 768-bit Diffie-Hellman group is used during IKE negotiation. • DH group 2: 1024-bit Diffie-Hellman group is used during IKE negotiation. • DH group 5: 1536-bit Diffie-Hellman group is used during IKE negotiation. • DH group 14: 2048-bit Diffie-Hellman group is used during IKE negotiation. • DH group 19: 256-bit ECP Diffie-Hellman group is used during IKE negotiation. • DH group 20: 384-bit ECP Diffie-Hellman group is used during IKE negotiation. • DH group 21: 521-bit ECP Diffie-Hellman group is used during IKE negotiation. To specify the PFS, run the **pfs** command.
SecondsFlag	Flag bit indicating aging of the SA. • 0: The SA ages based on the time. The flag bit takes effect globally. To configure a global time-based SA lifetime, run the **ipsec sa global-duration time-based** command. • 1: The SA ages based on the time. The flag bit takes effect in specified views only.
SA Life Time Seconds	Time-based IPSec SA lifetime.
KilobytesFlag	Flag bit indicating aging of the SA. • 0: The SA ages based on the traffic. The flag bit takes effect globally. To configure a global traffic-based SA lifetime, run the **ipsec sa global-duration traffic-based** command. • 1: The SA ages based on the traffic.
SA Life Kilobytes	Traffic-based IPSec SA lifetime.
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 **12.6.5 anti-replay window** command.

Copyright © Huawei Technologies Co., Ltd.

Item	Description
Fragment Before-encryption	Packet fragmentation mode. • Enable: IPSec packets are fragmented before encryption. • Disable: IPSec packets are fragmented after encryption. To configure a packet fragmentation mode, run the **12.6.99 ipsec fragmentation before-encryption** command.
Number of IPSec Proposals	Number of IPSec proposals referenced by an IPSec profile.
IPSec Proposals Name	Name of the referenced IPSec proposal. To configure an IPSec proposal, run the **proposal** command.
IKE Identity Name	Name of the referenced IKE identity. To referenced an IKE identity, run the **match ike-identity** command.
Qos Pre-classify	Pre-extraction of original IP packets. To configure pre-extraction of original IP packets, run the **12.6.132 qos pre-classify** command.
Qos group	QoS group to which the IPSec packets belong. To configure the QoS group, run the **12.6.131 qos group** command.

12.6.39 display ipsec profile ctrl-plane

Function

The **display ipsec profile ctrl-plane** command displays information about an IPSec profile on the ctrl-plane.

Format

display ipsec profile [**brief** | **name** *profile-name*] **ctrl-plane**

Parameters

Parameter	Description	Value
brief	Displays brief information about all IPSec profiles.	-

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
name *profile-name*	Displays information about the specified IPSec profile.	The value is an existing IPSec profile name.

Views

User view

Default Level

1: Monitoring level

Usage Guidelines

If no parameter is specified, information about all IPSec profiles is displayed.

If the **brief** parameter is specified, you can view brief information about all IPSec policies.

If the **name** parameter is specified, you can view detailed information about the specified IPSec policy.

Example

View information about the **a** IPSec profile.

```
<Huawei> display ipsec profile name a ctrl-plane
=========================================
IPSec profile  : a
Using interface:
=========================================
 IPSec Profile Name        :a
 Peer Name                 :
 PFS   Group               :DH group 14
 SecondsFlag               :0 (0:Global 1:Local)
 SA Life Time Seconds      :3600
 KilobytesFlag             :0 (0:Global 1:Local)
 SA Life Kilobytes         :1843200
 Anti-replay               :-
 Anti-replay Window Size   :1024
 Fragment Before-encryption:Disable
 Number of IPSec Proposals :0
 IPSec Proposals Name      :
 IKE Identity Name         :identity1
 Qos Pre-classify          :0 (0:Disable 1:Enable)
 Qos group                 : -
```

Table 12-52 Description of the **display ipsec profile name a ctrl-plane** command output

Item	Description
IPSec profile	Name of an IPSec profile
Using interface	Interface to which an IPSec profile is applied

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
IPSec Profile Name	Name of an IPSec profile
Peer name	Name of the IKE peer referenced by the IPSec profile.
PFS Group	Perfect Forward Secrecy (PFS) used in IKE negotiation: ● DH group 1: Indicates the 768-bit Diffie-Hellman group during negotiation. ● DH group 2: Indicates the 1024-bit Diffie-Hellman group during negotiation. ● DH group 5: Indicates the 1536-bit Diffie-Hellman group during negotiation. ● DH group 14: Indicates the 2048-bit Diffie-Hellman group during negotiation.
SecondsFlag	Flag bits that the SA ages by time: ● 0: Global configurations aged by time ● 1: Local configurations aged by time
SA Life Time Seconds	Time-based IPSec SA duration.
KilobytesFlag	Flag bits that the SA ages by traffic: ● 0: Global configurations aged by traffic ● 1: Local configurations aged by traffic
SA Life Kilobytes	traffic-based IPSec SA duration.
Anti-replay	Whether the IPSec anti-replay function is enabled.
Anti-replay Window Size	IPSec anti-replay window size. This field is available only when the IPSec anti-replay function is enabled.
Fragment Before-encryption	IPSec fragment mode: ● Enable: fragment before encryption ● Disable: Fragment after encryption
Number of IPSec Proposals	Proposals referenced by the IPSec profile.
IPSec Proposals Name	Name of an IPSec proposal
IKE Identity Name	Name of the referenced IKE identity.
Qos Pre-classify	pre-extraction of original IP packets.
Qos group	QoS group to which the IPSec packets belong.

 Copyright © Huawei Technologies Co., Ltd.

View brief information about all IPSec profiles.

```
<Huawei> display ipsec profile brief ctrl-plane
 Total number of IPSec profile: 1
 Profile name      Peer name
 ---------------------------------
 a                 spub
```

Table 12-53 Description of the **display ipsec profile brief ctrl-plane** command output

Item	Description
Total number of IPSec profile	Number of IPSec profiles on a device
Profile name	Name of an IPSec profile
Peer name	Name of the IKE peer referenced by the IPSec profile.

12.6.40 display ipsec proposal (All views)

Function

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

Format

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

Parameters

Parameter	Description	Value
brief	Displays brief information about IPSec proposals.	-
name *proposal-name*	Displays detailed information about an IPSec proposal with a specified name.	The value must be an existing IPSec proposal name.

Views

All views

Default Level

1: Monitoring level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

You can run the **display ipsec proposal** command to view the following information:

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

If no parameter is specified, this command displays detailed information about all IPSec proposals.

Example

Display detailed information about all IPSec proposals.

```
<Huawei> display ipsec proposal

Number of proposals: 2

IPSec proposal name: 1
 Encapsulation mode: Tunnel
 Transform         : esp-new
 ESP protocol      : Authentication SHA2-HMAC-256
                   Encryption AES-256

IPSec proposal name: 2
 Encapsulation mode: Tunnel
 Transform         : ah-esp-new
 AH protocol       : Authentication SHA2-HMAC-256
 ESP protocol      : Authentication SHA2-HMAC-256
                   Encryption     AES-256
```

Display brief information about all IPSec proposals.

```
<Huawei> display ipsec proposal brief

Current ipsec proposal number: 5
 -------------------------------------------------------------
 Proposal Name     Encapsulation mode    Transform
 -------------------------------------------------------------
 1                 Tunnel                esp-new
 2                 Tunnel                ah-esp-new
 3                 Tunnel                ah-esp-new
 4                 Tunnel                esp-new
 prop1               Tunnel                  esp-new
```

Table 12-54 Description of the **display ipsec proposal** command output

Item	Description
Number of proposals/Current ipsec proposal number	Current total number of IPSec proposals.
IPSec proposal name/Proposal Name	Name of the IPSec proposal. To configure an IPSec proposal, run the **ipsec proposal** command.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Encapsulation mode	Encapsulation mode in the IPSec proposal, which can be transport or tunnel. To configure an encapsulation mode, run the **12.6.54 encapsulation-mode** command.
Transform	Security protocol in the IPSec proposal. The value can be: • ah-new • esp-new • ah-esp-new To configure a security protocol, run the **12.6.172 transform** command.
ESP protocol	Authentication and encryption algorithms used by ESP. To configure authentication and encryption algorithms, run the **12.6.57 esp authentication-algorithm** and **12.6.59 esp encryption-algorithm** commands.

12.6.41 display ipsec proposal ctrl-plane

Function

The **display ipsec proposal ctrl-plane** command displays information about the IPSec proposal on the ctrl-plane.

Format

display ipsec proposal [**brief** | **name** *proposal-name*] **ctrl-plane**

Parameters

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

Views

User view

Copyright © Huawei Technologies Co., Ltd.

Default Level

1: Monitoring level

Usage Guidelines

The output of the **display ipsec proposal ctrl-plane** command is as follows:

- Name of the IPSec proposal
- Adopted encapsulation mode
- Adopted security protocol
- Authentication and encryption algorithms defined in the security protocol

If the name of the IPSec proposal is not specified, all proposals are displayed.

Example

Display detailed information about all IPSec proposals.

```
<Huawei> display ipsec proposal ctrl-plane
Number of proposals: 3

IPSec proposal name: newprop1
 Encapsulation mode: Tunnel
 Transform         : esp-new
 ESP protocol      : Authentication SHA2-HMAC-256
                   Encryption AES-256

IPSec proposal name: prop1
 Encapsulation mode: Tunnel
 Transform         : ah-new
 AH protocol       : Authentication SHA2-HMAC-256

IPSec proposal name: prop
 Encapsulation mode: Tunnel
 Transform         : esp-new
 ESP protocol      : Authentication SHA2-HMAC-256
                   Encryption AES-256
```

Display brief information about all IPSec proposals.

```
<Huawei> display ipsec proposal brief ctrl-plane
Current ipsec proposal number: 1
-------------------------------------------------------
Proposal Name      Encapsulation mode      Transform
-------------------------------------------------------
prop1              Tunnel                  esp-new
```

Table 12-55 Description of the **display ipsec proposal ctrl-plane** command output

Item	Description
Number of proposals/Current ipsec proposal number	Total number of IPSec proposals in the current system.
IPsec proposal name/Proposal Name	Name of the proposal
Encapsulation mode	Modes used by the proposal, including transport mode and tunnel mode

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Transform	Security protocols used by the proposal, including AH and ESP
AH protocol	Authentication and encryption algorithms used by AH
ESP protocol	Authentication and encryption algorithms used by ESP

12.6.42 display ipsec proto-protect proposal

Function

The **display ipsec proto-protect proposal** command displays information about security proposals.

Format

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

Parameters

Parameter	Description	Value
name *proposal-name*	Specifies the name of a security proposal.	The value is a string of 1 to 15 case-insensitive characters.

Views

All views

Default Level

1: Monitoring Level

Usage Guidelines

Usage Scenario

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

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

- Name of the IPSec security proposal
- Encapsulation mode defined in the security proposal

 Copyright © Huawei Technologies Co., Ltd.

- Security protocol defined in the security proposal
- Authentication and encryption algorithms defined in the security proposal

Example

Display information about all security proposals.

```
<Huawei> display ipsec proto-protect proposal
 Total IP security proposal number: 2

 IP security proposal name: proposal1
   encapsulation mode: transport
   transform: esp-new
   ESP protocol: authentication SHA1-HMAC-96, encryption 256-aes

 IP security proposal name: proposal2
   encapsulation mode: transport
   transform: ah-new
   AH protocol: authentication SHA1-HMAC-96
```

Table 12-56 Description of the **display ipsec proto-protect proposal** command output

Item	Description
Total IP security proposal number	Number of security proposals created
IP security proposal name	Name of a security proposal
encapsulation mode	Encapsulation mode: • transport • tunnel **NOTE** Currently only **transport** mode is supported.
transform	Security protocol defined in the security proposal: • esp-new: specifies the Encapsulating Security Payload (ESP). • ah-new: specifies the Authentication Header (AH).
ESP protocol	ESP configuration.
AH protocol	AH configuration.

12.6.43 display ipsec proposal (User view)

Function

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

 Copyright © Huawei Technologies Co., Ltd.

Format

display ipsec proposal [**brief** | **name** *proposal-name*] **ctrl-plane**

Parameters

Parameter	Description	Value
brief	Displays brief information about the IPSec proposal.	-
name *proposal-name*	Specifies the name of the proposal.	The value is an existing IPSec proposal name.
ctrl-plane	Displays information about the IPSec profiles on the ctrl-plane.	-

Views

User view

Default Level

1: Monitoring level

Usage Guidelines

The output of the **display ipsec proposal** command is as follows:

- Name of the IPSec proposal
- Adopted encapsulation mode
- Adopted security protocol
- Authentication and encryption algorithms defined in the security protocol

If the name of the IPSec proposal is not specified, all proposals are displayed.

Example

Display detailed information about all IPSec proposals.

```
<Huawei> display ipsec proposal ctrl-plane

Number of proposals: 2

IPSec proposal name: 1
 Encapsulation mode: Tunnel
 Transform         : esp-new
 ESP protocol      : Authentication SHA2-HMAC-256
                   Encryption AES-256

IPSec proposal name: 2
 Encapsulation mode: Tunnel
 Transform         : ah-esp-new
 AH protocol       : Authentication SHA2-HMAC-256
 ESP protocol      : Authentication SHA2-HMAC-256
                   Encryption     AES-256
```

 Copyright © Huawei Technologies Co., Ltd.

Display brief information about all IPSec proposals.

```
<Huawei> display ipsec proposal brief ctrl-plane

Current ipsec proposal number: 5
 ------------------------------------------------------------
 Proposal Name     Encapsulation mode    Transform
 ------------------------------------------------------------
 1                 Tunnel                esp-new
 2                 Tunnel                ah-esp-new
 3                 Tunnel                ah-esp-new
 4                 Tunnel                esp-new
 prop1               Tunnel                esp-new
```

Table 12-57 Description of the **display ipsec proposal** command output

Item	Description
Number of proposals/Current ipsec proposal number	Current total number of IPSec proposals.
IPSec proposal name/Proposal Name	Name of the IPSec proposal. To configure an IPSec proposal, run the **ipsec proposal** command.
Encapsulation mode	Encapsulation mode in the IPSec proposal, which can be transport or tunnel. To configure an encapsulation mode, run the **12.6.54 encapsulation-mode** command.
Transform	Security protocol in the IPSec proposal. The value can be: • ah-new • esp-new • ah-esp-new To configure a security protocol, run the **12.6.172 transform** command.
ESP protocol	Authentication and encryption algorithms used by ESP. To configure authentication and encryption algorithms, run the **12.6.57 esp authentication-algorithm** and **12.6.59 esp encryption-algorithm** commands.

12.6.44 display ipsec sa

Function

The **display ipsec sa** command displays IPSec SA information.

Copyright © Huawei Technologies Co., Ltd.

Format

display ipsec sa [**brief** | **duration** | **efficient-vpn** *efficient-vpn-name* | **policy** *policy-name* [*seq-number*] | **profile** *profile-name* | **remote** *ipv4-address*]

Parameters

Parameter	Description	Value
brief	Displays brief information about all IPSec SAs.	-
duration	Displays detailed information about IPSec SAs with specified lifetime.	-
efficient-vpn *efficient-vpn-name*	Displays SA information of an Efficient VPN policy with a specified name.	The value is an existing Efficient VPN policy name.
policy *policy-name*	Displays detailed information about IPSec SAs established using an IPSec policy with a specified name.	The value must be an existing IPSec policy name.
seq-number	Displays detailed information about IPSec SAs established using an IPSec policy with a specified sequence number.	The value must be an existing IPSec policy sequence number.
profile *profile-name*	Displays detailed information about IPSec SAs established using a specified IPSec profile.	The value must be an existing IPSec profile name.
remote *ipv4-address*	Displays detailed information about IPSec SAs with the specified remote IPv4 address.	The value is in dotted decimal notation.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

If no parameter is specified, detailed information about all IPSec SAs is displayed.

If **duration** is specified, the command displays information about global IPSec SAs with specified time-based or traffic-based lifetime. For details, see the **12.6.158 sa duration (ISAKMP IPSec policy view, IPSec policy template view, IPSec profile view)** command.

Example

Display brief information about all IPSec SAs.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> display ipsec sa brief
IPSec SA information:

  Src address    Dst address   SPI     VPN   Protocol    Algorithm
-------------------------------------------------------------------------------
  10.3.1.1       10.3.1.10     123456  vrf1  AH          A:SHA2_256_128
  10.3.1.1       10.3.1.10     754321  vrf1  ESP         E:AES-256 A:SHA2_256_128
  10.3.1.10      10.3.1.1      123457  vrf1  ESP         E:AES-256 A:SHA2_256_128
  10.3.1.10      10.3.1.1      654321  vrf1  AH          A:SHA2_256_128

Number of IPSec SA: 4
-------------------------------------------------------------------------------
```

Display information about all IPSec SAs in the IPSec policy mode.

```
<Huawei> display ipsec sa
ipsec sa information:
===============================
Interface: GigabitEthernet2/0/10
===============================
 ----------------------------
  IPSec policy name: "pc2"
  Sequence number  : 1
  Acl group        : 3061
  Acl rule         : 5
  Mode             : Template
  ----------------------------
    Connection ID     : 67108879
    Encapsulation mode: Tunnel
    Holding time      : 0d 0h 4m 29s
    Tunnel local      : 10.0.0.1:500
    Tunnel remote     : 10.0.0.2:500
    Flow source       : 10.0.0.1/255.255.255.255 17/1701
    Flow destination  : 10.0.0.2/255.255.255.255 17/39725
    Flow dscp         : af11

    [Outbound ESP SAs]
      SPI: 4055669516 (0xf1bc9b0c)
      Proposal: ESP-ENCRYPT-3DES-192 SHA2-256-128
      SA remaining key duration (kilobytes/sec): 5242880/3355
      Outpacket count       : 0
      Outpacket encap count : 0
      Outpacket drop count  : 0
      Slice Failure: 0
      Max sent sequence-number: 2377
      UDP encapsulation used for NAT traversal: N

    [Inbound ESP SAs]
      SPI: 1050491168 (0x3e9d3920)
      Proposal: ESP-ENCRYPT-3DES-192 SHA2-256-128
      SA remaining key duration (kilobytes/sec): 5242880/3355
      Inpacket count        : 0
      Inpacket decap count  : 0
      Inpacket drop count   : 0
      Authentication Failure: 0
      Replay Failure: 0
      Decrypt Check Failure: 0
      Max received sequence-number: 0
      UDP encapsulation used for NAT traversal: N
      Anti-replay : Enable
      Anti-replay window size: 1024

================================
Interface: Tunnel0/0/2
================================

 ----------------------------
  IPSec profile name: "1"
  Mode             : PROF-ISAKMP
  ----------------------------
    Connection ID     : 232
```

 Copyright © Huawei Technologies Co., Ltd.

```
Encapsulation mode: Tunnel
Holding time      : 0d 0h 4m 29s
Tunnel local      : 3.1.1.1:500
Tunnel remote     : 2.1.1.1:500
Flow source       : 10.0.0.1/255.255.255.255 47/0-65535
Flow destination  : 10.0.0.2/255.255.255.255 47/0-65535

[Outbound AH SAs]
  SPI: 12306225 (0xbbc731)
  Proposal: AH-SHA2-256-128
  SA remaining key duration (kilobytes/sec): 5242880/3355
  Outpacket count       : 1
  Outpacket encap count : 1
  Outpacket drop count  : 0
  Slice Failure: 0
  Max sent sequence-number: 1
  UDP encapsulation used for NAT traversal: N

[Inbound AH SAs]
  SPI: 2513644 (0x265aec)
  Proposal: AH-SHA2-256-128
  SA remaining key duration (kilobytes/sec): 5242880/3355
  Inpacket count        : 0
  Inpacket decap count  : 0
  Inpacket drop count   : 0
  Authentication Failure: 0
  Replay Failure: 0
  Decrypt Check Failure: 0
  Max received sequence-number: 0
  UDP encapsulation used for NAT traversal: N
  Anti-replay : Enable
  Anti-replay window size: 1024
```

Table 12-58 Description of the **display ipsec sa** command output

Item	Description
ipsec sa information	Information about the IPSec SA.
Interface	Interface to which the IPSec policy is applied.
IPSec policy name	Name of the IPSec policy. To configure an IPSec policy, run the **ipsec policy (system view)** command.
IPSec profile name	Name of the IPSec profile. To configure an IPSec profile, run the **12.6.108 ipsec profile (system view)** command.
Sequence number	Sequence number of the IPSec policy. To configure an IPSec policy, run the **ipsec policy (system view)** command.
Acl group	ACL number used in the IPSec policy. To configure an ACL referenced by an IPSec policy, run the **security acl** command.
Acl rule	ID of the matched ACL rule. The ACL rule ID is not displayed if the IPSec tunnel is created manually.

Copyright © Huawei Technologies Co., Ltd.

Item	Description
Mode	Mode in which an IPSec policy is created: • template: An IPSec policy is created using an IPSec policy template. • isakmp: An IPSec policy is created in ISAKMP mode. • manual: An IPSec policy is created manually. To configure an IPSec policy, run the **ipsec policy (system view)** command.
Connection ID	ID of the IPSec SA connection.
Encapsulation mode	Encapsulation mode in an IPSec proposal. **tunnel** indicates that the encapsulation mode is tunnel mode, and **transport** indicates that the encapsulation mode is transport mode. To configure an encapsulation mode, run the **12.6.54 encapsulation-mode** command.
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 and NAT traversal port of the local interface, run the **12.6.174 tunnel local** and **12.6.101 ipsec nat-traversal source-port** command.
Tunnel remote	IP address and NAT traversal port of the remote interface. To configure the IP address and NAT traversal port of the remote interface, run the **12.6.175 tunnel remote**/ **12.6.134 remote-address (IKE peer view)** and **12.6.101 ipsec nat-traversal source-port** command.
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. To configure the SPI for the SA created using a manually configured IPSec policy, run the **sa spi** command. The SPI is automatically generated when an IPSec policy is created in IKE negotiation mode.
Proposal	Name of an IPSec proposal referenced by the IPSec policy. To reference an IPSec proposal, run the **proposal** command.

Copyright © Huawei Technologies Co., Ltd.

Item	Description
SA remaining key duration (kilobytes/sec)	Hard remaining lifetime of an SA, in kilobytes or seconds. To set the SA lifetime, run the **12.6.158 sa duration (ISAKMP IPSec policy view, IPSec policy template view, IPSec profile view)** command.
Outpacket count	Number of packets that can be encrypted with the IPSec SA.
Outpacket encap count	Number of sent packets that are successfully encrypted.
Outpacket drop count	Number of discarded packets during encryption.
Max sent sequence-number	Maximum sequence number of sent packets. The sequence number increases during communication and is used for anti-replay.
Slice Failure	Number of packets that fail to be fragmented.
UDP encapsulation used for NAT traversal	Whether NAT traversal is enabled: • Y • N To enable NAT traversal, run the **nat traversal** command.
Inbound ESP SAs	Inbound IPSec SA information using ESP.
Inpacket count	Number of packets that can be decrypted with the IPSec SA.
Inpacket decap count	Number of received packets that are successfully decrypted.
Inpacket drop count	Number of discarded packets during decryption.
Authentication Failure	Number of packets that fail to be authenticated.
Replay Failure	Number of packets discarded by the anti-replay function.
Decrypt Check Failure	Number of packets discarded because of a failure in IPSec check.
Max received sequence-number	Maximum sequence number of received packets.
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 **12.6.92 ipsec anti-replay enable** command.

Copyright © Huawei Technologies Co., Ltd.

Item	Description
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 **12.6.5 anti-replay window** or **12.6.93 ipsec anti-replay window** command.
Src address	IP address of the local interface. To configure the IP address of the local interface, run the **12.6.174 tunnel local** command.
Dst address	IP address of the remote interface. To configure the IP address of the remote interface, run the **12.6.175 tunnel remote** or **12.6.134 remote-address (IKE peer view)** command.
VPN	VPN instance that the IPSec tunnel belongs to. To configure a VPN instance that the IPSec tunnel belongs to, run the **12.6.155 sa binding vpn-instance** command.
Protocol	Security protocol used by the IPSec SA: • AH: AH is used. • AH-ESP: AH and ESP are used. • ESP: ESP is used. To configure a security protocol, run the **12.6.172 transform** command.
Algorithm	Authentication and encryption algorithms used by a security protocol. A indicates the authentication algorithm, and E indicates the encryption algorithm. To configure an authentication algorithm, run the **12.6.3 ah authentication-algorithm** or **12.6.57 esp authentication-algorithm** command. To configure an encryption algorithm, run the **12.6.59 esp encryption-algorithm** command.

12.6.45 display ipsec proto-protect sa

Function

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

Format

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

Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
name *sa-name*	Specifies the SA name.	The value is an existing IPSec Security Association 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 proto-protect 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 proto-protect 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 proto-protect sa
IP security association name: sa1
Number of references: 0
  proposal name: p1
  inbound AH setting:
    AH spi: 267 (0x10b)
    AH string-key:
    AH authentication hex key: %^%#'RCZaI8Z:_E!Q8T!3,AO_OKZ>\U!O]*>(U(9CS9!%^%#
  inbound ESP setting:
    ESP spi: 789 (0x315)
    ESP string-key: DN]I8$];]3+Q=^Q`MAF4<1!!
    ESP encryption hex key:
    ESP authentication hex key:
  outbound AH setting:
    AH spi: 267 (0x10b)
```

 Copyright © Huawei Technologies Co., Ltd.

```
  AH string-key:
  AH authentication hex key: %^%#'RCZaI8Z:_E!Q8T!3,AO_OKZ>\U!O]*>(U(9CS9!%^%#
outbound ESP setting:
  ESP spi: 789 (0x315)
  ESP string-key: DN]I8$];]3+Q=^Q`MAF4<1!!
  ESP encryption hex key:
  ESP authentication hex key:
```

Table 12-59 Description of the **display ipsec proto-protect 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
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

12.6.46 display ipsec statistics

 Copyright © Huawei Technologies Co., Ltd.

Function

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

Format

display ipsec statistics [**tunnel-number**]

Parameters

None.

Parameter	Description	Value
tunnel-number	Displays the number of IPSec tunnels.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

You can run the **display ipsec 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 statistics** command only displays the number of plaintext bytes.

Example

Display statistics about all IPSec packets.

```
<Huawei> display ipsec 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
```

 Copyright © Huawei Technologies Co., Ltd.

```
    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
```

Display the number of IPSec tunnels.

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

Table 12-60 Description of the **display ipsec 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.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
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.
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.

 Copyright © Huawei Technologies Co., Ltd.

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

Related Topics

12.6.144 reset ipsec statistics

 Copyright © Huawei Technologies Co., Ltd.

12.6.47 display ipsec statistics route

Function

The **display ipsec statistics route** command displays IPSec route injection statistics.

Format

display ipsec statistics route

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

In an IPSec route injection scenario, you can run the **display ipsec statistics route** command to view IPSec route injection statistics for fault location.

Example

Display IPSec route injection statistics.

```
<Huawei> display ipsec statistics route
IPSec route statistics information:

Route add                    send:1          receive:1
Route del                    send:0          receive:0
Route syn                    send:674        receive:674
Route syn  round             send:674        receive:674
Route syn                    add :0          del    :0
Route send to route module    add :2          del    :1
Route send to ipsec module    add :1          del    :0
Route msg ipc send error          :0
Route msg process error           :0
Route add:
  dest addr equal with peer addr          :0
  add no memery                           :0
  same route same slot                    :0
  same route diff slot or interface down  :1
  cpu not exist                           :0
  vrf invalid                             :0
Route del:
  route not exist                         :0
  not delete state                        :0
  same route send by other slot           :0

HA data
Route HA send num                         :675
```

 Copyright © Huawei Technologies Co., Ltd.

```
Route HA receive num                :0
Route HA send error num             :0
```

Table 12-61 Description of the **display ipsec statistics route** command output

Item	Description
IPSec route statistics information	IPSec route statistics.
Route add	Routes are added from the LPU to MPU: ● send: indicates the number of routes sent by the LPU. ● receive: indicates the number of routes received by the MPU.
Route del	Routes are deleted by the LPU from the MPU: ● send: indicates the number of routes sent by the LPU. ● receive: indicates the number of routes received by the MPU.
Route syn	Routes are synchronized by the LPU with the MPU: ● send: indicates the number of routes sent by the LPU. ● receive: indicates the number of routes received by the MPU. ● add: indicates the number of routes added by the MPU because routes do not exist. ● del: indicates the number of routes deleted by the MPU due to residual routing entries.
Route syn round	Number of times the LPU synchronizes routes with the MPU: ● send: indicates the number of times the LPU sends routes to the MPU. ● receive: indicates the number of times the MPU receives routes from the LPU.
Route send to route module	Routes are added to or deleted from the routing module: ● add: indicates the number of added routes. ● del: indicates the number of deleted routes.
Route send to ipsec module	Routes are added to or deleted from the IPSec module: ● add: indicates the number of added routes. ● del: indicates the number of deleted routes.
Route msg ipc send error	Number of times IPC fails to send routing information.
Route msg process error	Number of times the LPU fails to process routing information.
Route add	Added routes.

Copyright © Huawei Technologies Co., Ltd.

Item	Description
dest addr equal with peer addr	Number of times the route destination address is consistent with the peer address specified in intelligent path selection during route addition.
add no memery	Number of failures to apply for memory during route addition.
same route same slot	Number of times the same slot has the same routes during route addition.
same route diff slot or interface down	Number of times boards in different slots have the same routes or have interfaces in Down state during route addition.
cpu not exist	Number of times the CPU does not exist during route addition.
vrf invalid	Number of times the VPN instance becomes invalid during route addition.
Route del	Deleted routes.
route not exist	Number of routes that do not exist during route deletion.
not delete state	Number of routes that do not exist in the routing table during route deletion.
same route send by other slot	Number of the same routes that boards in other slots send to the MPU during route deletion.
HA data	Active/standby backup data.
Route HA send num	Number of routes sent by the active device during active/standby backup.
Route HA receive num	Number of routes received by the standby device during active/standby backup.
Route HA send error num	Number of routes that fail to be sent by the active device during active/standby backup.

12.6.48 display ipsec proto-protect statistics

Function

Using the **display ipsec proto-protect statistics** command, you can view the statistics about packets processed by IPSec.

Format

display ipsec proto-protect statistics [**sa-name** *sa-name*]

Parameters

Parameter	Description	Value
sa-name *sa-name*	Specifies the IPSec Security Association (SA) name.	The value is an existing IPSec Security Association name.

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 proto-protect 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 proto-protect 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
```

 Copyright © Huawei Technologies Co., Ltd.

```
    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 12-62 Description of the **display ipsec proto-protect statistics** command output

Item	Description
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
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

 Copyright © Huawei Technologies Co., Ltd.

12.6.49 dn

Function

The **dn** command specifies the distinguished name (DN) of an allowed peer for IKE negotiation.

The **undo dn** command deletes the DN of an allowed peer.

By default, no DN of allowed peer for IKE negotiation is configured.

Format

dn *name*

undo dn *name*

Parameters

Parameter	Description	Value
name	Specifies the DN of an allowed peer for IKE negotiation.	The value is a string of 1 to 255 case-sensitive characters without spaces.

Views

Identity filter set view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can run this command to specify an allowed peer based on the DN (PKI domain configuration referenced in the IKE peer configured on a remote device) in the identity filter set for IKE negotiation.

Precautions

An IPSec tunnel can be established only when the remote end matches one or more parameters in the identity filter set and the IPSec negotiation parameters at both ends are consistent.

If you run this command in the same view multiple times, the latest configuration does not override earlier ones.

Example

Set the name of the allowed peer for IKE negotiation to **huawei**.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> system-view
[Huawei] ike identity identity1
[Huawei-ike-identity-identity1] dn c=cn,st=jiangsu,l=nanjing,o=huawei,ou=vpn,cn=ipsec
```

Related Topics

12.6.70 ike identity

12.6.50 dpd

Function

The **dpd** command configures the dead peer detection (DPD) idle time, DPD packet retransmission interval, and maximum number of DPD packet retransmissions on the specified IKE peer.

The **undo dpd** command restores the default DPD idle time, DPD packet retransmission interval, and maximum number of DPD packet retransmissions on the specified IKE peer.

By default, the DPD idle time, DPD packet retransmission interval, and maximum number of DPD packet retransmissions on an IKE peer are 30s, 15s, and 3 respectively.

Format

dpd { **idle-time** *interval* | **retransmit-interval** *interval* | **retry-limit** *times* }

undo dpd { **idle-time** | **retransmit-interval** | **retry-limit** }

Parameters

Parameter	Description	Value
idle-time *interval*	Specifies the DPD idle time.	The value is an integer that ranges from 10 to 3600, in seconds.
retransmit-interval *interval*	Specifies the DPD packet retransmission interval.	The value is an integer that ranges from 2 to 60, in seconds.
retry-limit *times*	Specifies the maximum number of DPD packet retransmissions.	The value is an integer that ranges from 3 to 10.

Views

IKE peer view

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

Usage Scenario

When peers implement IPSec communication, the heartbeat mechanism can detect peer faults to avoid traffic loss. However, the periodic heartbeat message exchanges consume CPU resources on the two ends. The DPD mechanism enables a device to send DPD messages for peer detection only when the device does not receive IPSec packets from the peer within a period. This mechanism can detect peer faults and save CPU resources.

The device sets the DPD mode and enables the DPD function based on the **dpd type** command. Two DPD modes are available:

- On-demand DPD

  When the local end needs to send IPSec packets to the remote end, the local end sends a DPD request packet to the remote end for DPD detection.
- Periodic DPD

  If the local end does not receive IPSec packets or a DPD request packet from the remote end after the DPD idle time expires, it periodically sends a DPD request packet to the remote end.

The local end retransmits DPD request packets if it does not receive any DPD response packet from the remote end within the retransmission interval. If the local end still does not receive any DPD response packet within the retransmission interval after the maximum number of retransmissions is reached, the local end considers that the remote end is offline and deletes the involved IKE SA and IPSec SA.

Precautions

- The **dpd** command must be used with the **dpd type** and **dpd msg** commands.
- Parameters in the **dpd** command can be configured for each IKE peer separately and do not need to be the same as the parameters on the peer device.

Example

Set the DPD idle time, DPD packet retransmission interval, and maximum number of DPD packet retransmissions on the IKE peer **test** to 300s, 10s, and 4.

```
<Huawei> system-view
[Huawei] ike peer test
[Huawei-ike-peer-test] dpd idle-time 300
[Huawei-ike-peer-test] dpd retransmit-interval 10
[Huawei-ike-peer-test] dpd retry-limit 4
```

Related Topics

12.6.51 dpd msg

12.6.52 dpd type

12.6.75 ike peer

12.6.51 dpd msg

 Copyright © Huawei Technologies Co., Ltd.

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

IKE peer view, 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. You can use the **dpd msg** command to set the same payload sequence of DPD packets on the two ends.

Precautions

This command applies only when an IKE peer uses IKEv1.

 Copyright © Huawei Technologies Co., Ltd.

Example

Set the payload sequence of DPD packets to **hash-notify** on the IKE peer **huawei**.

```
<Huawei> system-view
[Huawei] ike peer huawei
[Huawei-ike-peer-huawei] dpd msg seq-hash-notify
```

Related Topics

12.6.52 dpd type
12.6.34 display ipsec policy (all views)
12.6.36 display ipsec policy-template (all views)
12.6.38 display ipsec profile (all views)
12.6.30 display ipsec efficient-vpn

12.6.52 dpd type

Function

The **dpd type** command configures the DPD mode on an IKE peer.

The **undo dpd type** command deletes the DPD mode on an IKE peer.

By default, the DPD mode is not configured on an IKE peer.

Format

dpd type { **on-demand** | **periodic** }

undo dpd type

Parameters

Parameter	Description	Value
on-demand	Configures on-demand DPD.	-
periodic	Configures periodic DPD.	-

Views

IKE peer view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

 Copyright © Huawei Technologies Co., Ltd.

When peers implement IPSec communication, the heartbeat mechanism can detect peer faults to avoid traffic loss. However, the periodic heartbeat message exchanges consume CPU resources on the two ends. The DPD mechanism enables a device to send DPD messages for peer detection only when the device does not receive IPSec packets from the peer within a period. This mechanism can detect peer faults and save CPU resources.

The device sets the DPD mode and enables the DPD function based on the **dpd type** command. Two DPD modes are available:

- On-demand DPD

  When the local end needs to send IPSec packets to the remote end, the local end sends a DPD request packet to the remote end for DPD detection.
- Periodic DPD

  If the local end does not receive IPSec packets or a DPD request packet from the remote end after the DPD idle time expires, it periodically sends a DPD request packet to the remote end.

The local end retransmits DPD request packets if it does not receive any DPD response packet from the remote end within the retransmission interval. If the local end still does not receive any DPD response packet within the retransmission interval after the maximum number of retransmissions is reached, the local end considers that the remote end is offline and deletes the involved IKE SA and IPSec SA.

Precautions

The sequence of the payload in DPD packets configured on IKE peers using the **dpd msg** command must be the same. Otherwise, DPD does not take effect.

When multiple branches are connected to the headquarters, you are advised not to set the DPD mode of the headquarters to periodic detection. This is because an IPSec tunnel will frequently flap, causing high CPU usage, if the network is unstable. You are advised to set the DPD mode of the headquarters to on-demand detection or not to configure the DPD mode.

Example

Configure on-demand DPD.

```
<Huawei> system-view
[Huawei] ike peer huawei
[Huawei-ike-peer-huawei] dpd type on-demand
```

Related Topics

12.6.50 dpd
12.6.51 dpd msg
12.6.75 ike peer

12.6.53 dscp

Function

The **dscp** command sets the DSCP priority of IKE packets on a specified IKE peer.

 Copyright © Huawei Technologies Co., Ltd.

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

By default, the DSCP priority of IKE packets on a specified IKE peer is 0.

Format

dscp *dscp-value*

undo dscp

Parameters

Parameter	Description	Value
dscp-value	Specifies the 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

IKE peer view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

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 an IKE peer, run this command.

Precautions

The DSCP priority of IKE packets can be configured in the IKE peer view or system view. The system preferentially uses the DSCP priority configured in the IKE peer view. If the DSCP priority is not configured in the IKE peer view, the system uses the global DSCP priority.

Example

Set the DSCP priority of IKE packets to CS2 for the IKE peer **ik1**.

```
<Huawei> system-view
[Huawei] ike peer ik1
[Huawei-ike-peer-ik1] dscp cs2
```

 Copyright © Huawei Technologies Co., Ltd.

12.6.54 encapsulation-mode

Function

The **encapsulation-mode** command sets the IPSec encapsulation mode.

The **undo encapsulation-mode** command restores the default IPSec encapsulation mode.

By default, the tunnel mode is used.

Format

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

undo encapsulation-mode

Parameters

Parameter	Description	Value
transport	Encapsulates IP packets in transport mode.	-
tunnel	Encapsulates IP packets in tunnel mode.	-

Views

IPSec proposal view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

IPSec encapsulates IP packets by adding an AH or ESP header and ESP tail to original IP packets for authentication and encryption. The following two IPSec encapsulation modes are available:

- Tunnel mode

  In tunnel mode, IPSec adds a new IP header to an IP packet. The source and destination addresses of the new IP header are the IP addresses of two ends of a tunnel. The tunnel mode is more secure than the transport mode. In terms of performance, the tunnel mode consumes more bandwidth than the transport mode.

  The tunnel mode is often used between two security gateways. The packets encrypted by one security gateway can only be decrypted by the other security gateway.
- Transport mode

  In transport mode, IPSec does not add a new header to an IP packet. The source and destination addresses of the original packet are the IP addresses of

 Copyright © Huawei Technologies Co., Ltd.

two ends of a tunnel. In transport mode, the two devices that encrypt and decrypt packets must be the original packet sender and final receiver respectively.

Since most data traffic between two security gateways is not communication traffic of the two gateways, the transport mode is not used between security gateways. The transport mode is suited for the communication between two hosts or between a host and a security gateway; however, the transport mode is not recommended because it provides low security.

Precautions

The two IPSec tunnel ends must use the same encapsulation mode.

When IKEv2 is used, the encapsulation mode in all the IPSec proposals configured on the IKE negotiation initiator must be the same; otherwise, IKE negotiation fails.

Example

Set the IPSec encapsulation mode to the transport mode.

```
<Huawei> system-view
[Huawei] ipsec proposal newprop1
[Huawei-ipsec-proposal-newprop1] encapsulation-mode transport
```

12.6.55 encapsulation-mode (ipsec-proto-protect-proposal view)

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 proto-protect proposal view

 Copyright © Huawei Technologies Co., Ltd.

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 (such as a gateway workstation and a router), 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 (routers) 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 proto-protect proposal prop2
[Huawei-ipsec-proto-protect-proposal-prop2] encapsulation-mode transport
```

12.6.56 encryption-algorithm

Function

The **encryption-algorithm** command configures an encryption algorithm for IKE negotiation.

The **undo encryption-algorithm** command restores the default configuration.

By default, the AES-256 encryption algorithm is used for IKE negotiation.

Format

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

undo encryption-algorithm

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
des	Configures the 56-bit Data Encryption Standard (DES) algorithm in Cipher Block Chaining (CBC) mode.	-
3des	Configures the 168-bit Triple Data Encryption Standard (3DES) algorithm in CBC mode.	-
aes-128	Configures the 128-bit AES algorithm in CBC mode.	-
aes-192	Configures the 192-bit AES algorithm in CBC mode.	-
aes-256	Configures the 256-bit AES algorithm in CBC mode.	-

Views

IKE proposal view

Default Level

2: Configuration level

Usage Guidelines

The following encryption algorithms used in IKE proposals are listed in descending order of security level: **aes-256** > **aes-192** > **aes-128** > **3des** > **des**.

NOTE

The **3des** and **des** algorithms provide low security and so are not recommended.

Example

Set the AES-192 algorithm for IKE proposal 10.

```
<Huawei> system-view
[Huawei] ike proposal 10
[Huawei-ike-proposal-10] encryption-algorithm aes-192
```

12.6.57 esp authentication-algorithm

Function

The **esp authentication-algorithm** command configures the Encapsulating Security Payload (ESP) authentication algorithm.

The **undo esp authentication-algorithm** command configures ESP not to authenticate packets.

By default, the ESP authentication algorithm is Secure Hash Algorithm SHA2-256.

Format

esp authentication-algorithm { **md5** | **sha1** | **sha2-256** | **sha2-384** | **sha2-512** }

 Copyright © Huawei Technologies Co., Ltd.

undo esp authentication-algorithm

Parameters

Parameter	Description	Value
md5	Specifies MD5 as the ESP authentication algorithm.	-
sha1	Specifies SHA1 as the ESP authentication algorithm.	-
sha2-256	Specifies SHA2-256 as the ESP authentication algorithm.	-
sha2-384	Specifies SHA2-384 as the ESP authentication algorithm.	-
sha2-512	Specifies SHA2-512 as the ESP authentication algorithm.	-

NOTE

AR100&AR120 series, AR161, AR161W, AR161EW, AR161EW-M1, AR161G-L, AR161G-Lc, AR161G-U, AR169, AR169G-L, AR169CVW, AR169CVW-4B4S, AR169W, AR169W-P-M9, AR169RW-P-M9, AR169EW, AR169EGW-L, AR1220C, AR1220-8GE, AR2204-27GE, AR2204E-D-27GE, AR2204-24GE, AR2204-27GE-P, AR2204-48GE-P, AR2204-51GE, AR2204-51GE-P, AR2204-51GE-R, AR2204E, AR2204E-D, AR2204XE, and AR2204XE-DC do not support SHA2-384 and SHA2-512 authentication algorithms.

Views

IPSec proposal view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

ESP supports the following encryption and authentication modes: both, encryption-only, authentication-only, and none. In the efficient VPN scenario, do not configure encryption or authentication algorithm for ESP when the remote device does not support IPSec encryption or authentication.

NOTE

When ESP is not used to encrypt or authenticate packets, the IKEV2 version of the IPSec tunnel cannot be established.

Prerequisites

esp or **ah-esp** has been specified in the **transform** command.

Precautions

ESP authentication algorithms in the IPSec proposals referenced in the IPSec policies configured at both ends of an IPSec tunnel must be the same.

 Copyright © Huawei Technologies Co., Ltd.

The **undo esp authentication-algorithm** command sets the ESP authentication algorithm to blank (non-authentication) and takes effect only when an ESP authentication algorithm has been specified.

The following algorithms are listed in descending order of security level: **sha2-512** > **sha2-384** > **sha2-256** > **sha1** > **md5**.

The **sha2-256**, **sha2-384**, and **sha2-512** algorithms are recommended for security purposes. The **md5** and **sha1** algorithms are not recommended.

Example

Set ESP and SHA2-256 in the IPSec proposal **newprop1**.

```
<Huawei> system-view
[Huawei] ipsec proposal newprop1
[Huawei-ipsec-proposal-newprop1] transform esp
[Huawei-ipsec-proposal-newprop1] esp authentication-algorithm sha2-256
```

Related Topics

12.6.40 display ipsec proposal (All views)

12.6.58 esp authentication-algorithm (ipsec-proto-protect-proposal view)

Function

The **esp authentication-algorithm** command configures the authentication algorithm for Encapsulating Security Payload (ESP).

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

By default, the authentication algorithm SHA2-256 is used for ESP.

Format

esp authentication-algorithm { **md5** | **sha1** | **sha2-256** }

undo esp authentication-algorithm

Parameters

Parameter	Description	Value
md5	Indicates that the authentication algorithm MD5 is used for ESP. **NOTE** To ensure high security, do not use the MD5 algorithm as the ESP authentication algorithm.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
sha1	Indicates that the authentication algorithm Secure Hash Algorithm-1 (SHA-1) is used for ESP. **NOTE** To ensure high security, do not use the SHA-1 algorithm as the ESP authentication algorithm.	-
sha2-256	Indicates the authentication algorithm SHA-2 256 is used for ESP.	-

Views

IPSec proto-protect proposal view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

IPSec can use Authentication Header (AH) or ESP to authenticate packets, preventing packets from being intercepted or modified. When ESP is used, the authentication and encryption algorithms must be configured. You can run the **transform** command to configure AH or ESP. When ESP is used, you can run the **esp authentication-algorithm** command to specify an authentication algorithm for ESP.

ESP currently supports MD5, SHA-1 and SHA2-256 authentication algorithms.

- MD5: generates a 128-bit message summary for an input message of any length.
- SHA-1: generates a 160-bit message summary for an input message of less than 2^{64} bits.
- SHA2-256: generates a 256-bit message summary for an input message of less than 2^{64} bits

MD5 is faster than SHA-1, but is less secure.

NOTE

The **undo esp authentication-algorithm** command functions differently from the **undo ah authentication-algorithm** command. The **undo esp authentication-algorithm** command configures ESP not to authenticate packets, whereas the **undo ah authentication-algorithm** command restores the default authentication algorithm for AH.

Prerequisite

IPSec ensures security using AH or ESP. An authentication algorithm can be configured only after AH or ESP is specified. Therefore, you can configure an ESP authentication algorithm only after running the **transform** command to specify ESP.

Copyright © Huawei Technologies Co., Ltd.

Precautions

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

The authentication algorithms on both IPSec peers must be identical.

Example

Set the authentication algorithm to SHA-1 for ESP.

```
<Huawei> system-view
[Huawei] ipsec proto-protect proposal prop1
[Huawei-ipsec-proto-protect-proposal-prop1] transform esp
[Huawei-ipsec-proto-protect-proposal-prop1] esp authentication-algorithm sha1
```

12.6.59 esp encryption-algorithm

Function

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

The **undo esp encryption-algorithm** command sets the ESP encryption algorithm to blank (non-encryption).

By default, the ESP encryption algorithm is Advanced Encryption Standard AES-256.

Format

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

undo esp encryption-algorithm

Parameters

Parameter	Description	Value
des	Configures the 56-bit Data Encryption Standard (DES) algorithm in Cipher Block Chaining (CBC) mode.	-
3des	Configures the 168-bit Triple Data Encryption Standard (3DES) algorithm in CBC mode.	-
aes-128	Configures the 128-bit AES algorithm in CBC mode.	-
aes-192	Configures the 192-bit AES algorithm in CBC mode.	-
aes-256	Configures the 256-bit AES algorithm in CBC mode.	-

Views

IPSec proposal view

 Copyright © Huawei Technologies Co., Ltd.

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

ESP supports the following encryption and authentication modes: both, encryption-only, authentication-only, and none. In the efficient VPN scenario, do not configure encryption or authentication algorithm for ESP when the remote device does not support IPSec encryption or authentication.

NOTE

When ESP is not used to encrypt or authenticate packets, the IKEV2 version of the IPSec tunnel cannot be established.

Prerequisites

esp or **ah-esp** has been specified in the **transform** command.

Precautions

ESP encryption algorithms in the IPSec proposals referenced in the IPSec policies configured at both ends of an IPSec tunnel must be the same.

The **undo esp encryption-algorithm** command sets the ESP encryption algorithm to blank (non-encryption) and takes effect only when an ESP encryption algorithm has been specified.

The following encryption algorithms are listed in descending order of security level: **aes-256** > **aes-192** > **aes-128** > **3des** > **des**.

The **aes-256**, **aes-192**, and **aes-128** algorithms are recommended for security purposes. The **3des** and **des** algorithms are not recommended.

Example

Set ESP and AES-128 in the IPSec proposal **newprop1**.

```
<Huawei> system-view
[Huawei] ipsec proposal newprop1
[Huawei-ipsec-proposal-newprop1] transform esp
[Huawei-ipsec-proposal-newprop1] esp encryption-algorithm aes-128
```

Related Topics

12.6.40 display ipsec proposal (All views)

12.6.60 esp encryption-algorithm (ipsec-proto-protect-proposal view)

Function

The **esp encryption-algorithm** command configures the encryption algorithm for Encapsulating Security Payload (ESP).

 Copyright © Huawei Technologies Co., Ltd.

The **undo esp encryption-algorithm** command configures ESP not to encrypt packets.

By default, the encryption algorithm AES 128 is used for ESP.

Format

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

undo esp encryption-algorithm

Parameters

Parameter	Description	Value
des	Indicates that ESP uses DES algorithm to encrypt packets. To ensure high security, do not use the DES algorithm as the ESP encryption algorithm.	-
3des	Indicates that ESP uses 3DES algorithm to encrypt packets.	-
aes	Indicates that ESP uses Advanced Encryption Standard (AES) algorithm 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 proto-protect proposal view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

IPSec uses authentication and encryption algorithms to protect IP packet transmission, preventing packets from being intercepted or modified. Therefore, specify an encryption algorithm before using ESP to ensure security.

 Copyright © Huawei Technologies Co., Ltd.

- DES: uses a 56-bit key to encrypt a 64-bit packet in plain text.
- 3DES: uses three 56-bit keys (in effect, a 168-bit key) to encrypt a packet in plain text.
- AES: uses 128, 192, 256-bit keys respectively to encrypt a packet in plain text.

3DES is CPU incentive and encrypts packets slowly, but provides a more secure service than DES. AES is more secure and performance is also better than 3DES.

Prerequisite

You can configure an encryption algorithm only after ESP is used.

Precautions

The **undo esp encryption-algorithm** command does not restore the default encryption algorithm but configures ESP not to encrypt packets.

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

The encryption algorithms on both IPSec peers must be identical.

NOTE

You cannot setup a peer with ESP encryption algorithm configuration.

Example

Set the encryption algorithm to 3DES for ESP.

```
<Huawei> system-view
[Huawei] ipsec proto-protect proposal prop1
[Huawei-ipsec-proto-protect-proposal-prop1] transform esp
[Huawei-ipsec-proto-protect-proposal-prop1] esp encryption-algorithm 3des
```

Set the encryption algorithm to AES 128 bits for ESP.

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

12.6.61 exchange-mode

Function

The **exchange-mode** command configures the IKEv1 phase 1 negotiation mode.

The **undo exchange-mode** command restores the default IKEv1 phase 1 negotiation mode.

By default, the main mode is used.

Format

exchange-mode { **aggressive** | **main** }

undo exchange-mode

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
aggressive	Configures the aggressive mode.	-
main	Configures the main mode.	-

Views

IKE peer view

Default Level

2: Configuration level

Usage Guidelines

Two key exchange and negotiation modes are defined in IKEv1 phase 1:

- In main mode, key exchange information is separated from identity and authentication information to protect identity information.
- In aggressive mode, only three messages are exchanged. Therefore, IKE SAs can be set up more quickly in aggressive mode. However, the first two messages exchanged in aggressive mode are not encrypted, and identity authentication is transmitted in plain text. This brings security risks.

When selecting a negotiation mode, you can determine the main or aggressive mode based on network requirements:

- In the scenario where multiple pre-shared keys are configured in the IKE user table, if the IP address of the negotiation initiator is unknown or unstable and the two ends expect to set up SAs using the pre-shared key, only the aggressive mode can be used.
- If the initiator knows the policy of the responder, IKE SAs can be set up more quickly in aggressive mode.

Example

Configure the aggressive IKE negotiation mode for the IKE peer **peer1**.

```
<Huawei> system-view
[Huawei] ike peer peer1
[Huawei-ike-peer-peer1] exchange-mode aggressive
```

Related Topics

12.6.20 display ike peer (all views)

12.6.62 fqdn

Function

The **fqdn** command specifies the name of an allowed peer for IKE negotiation.

The **undo fqdn** command deletes the name of an allowed peer.

 Copyright © Huawei Technologies Co., Ltd.

By default, no name of allowed peer for IKE negotiation is configured.

Format

fqdn *fqdn-name*

undo fqdn *fqdn-name*

Parameters

Parameter	Description	Value
fqdn-name	Specifies the name of an allowed peer.	The value is a string of 1 to 255 case-sensitive characters without spaces.

Views

Identity filter set view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can run this command to specify an allowed peer based on the name (configured on a remote device using the **ike local-name** command) in the identity filter set for IKE negotiation.

Precautions

An IPSec tunnel can be established only when the remote end matches one or more parameters in the identity filter set and the IPSec negotiation parameters at both ends are consistent.

If you run this command in the same view multiple times, the latest configuration does not override earlier ones.

Example

Set the name of the allowed peer for IKE negotiation to **huawei**.

```
<Huawei> system-view
[Huawei] ike identity identity1
[Huawei-ike-identity-identity1] fqdn huawei
```

Related Topics

12.6.70 ike identity

12.6.71 ike local-name

 Copyright © Huawei Technologies Co., Ltd.

12.6.63 id-type

Function

The **id-type** command configures the IKE user ID type and ID.

The **undo id-type** command deletes the IKE user ID type and ID.

By default, the IKE user ID type and ID are not configured.

Format

id-type { **any** *any-id* | **fqdn** *remote-fqdn* | **ip** *ipv4-address* | **user-fqdn** *remote-user-fqdn* }

undo id-type

Parameters

Parameter	Description	Value
any *any-id*	Indicates that the remote ID type of an IKE peer can be any type and configures the remote ID.	The value is a string of 1 to 255 case-sensitive characters without question marks (?).
fqdn *remote-fqdn*	Uses the name as the remote ID of an IKE peer and configures the remote ID.	The value is a string of 1 to 255 case-sensitive characters without question marks (?).
ip *ipv4-address*	Uses the IPv4 address as the remote ID of an IKE peer and configures the remote ID.	The value is in dotted decimal notation.
user-fqdn *remote-user-fqdn*	Uses the domain name as the remote ID of an IKE peer and configures the remote ID.	The value is a string of 1 to 255 case-sensitive characters without question marks (?).

Views

IKE user view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

 Copyright © Huawei Technologies Co., Ltd.

In a point-to-multipoint scenario, the device functions as the VPN gateway of the headquarters, an IPSec policy is created using an IPSec policy template, and the VPN gateway receives IPSec connection setup requests of different branches. When the pre-shared key is used for identity authentication and all branches use the same ID and pre-shared key, there are security risks. That is, if the ID and pre-shared key of one branch leak, the ID and pre-shared key of all branches leak. To prevent this problem, you are advised to run the **id-type** and **pre-shared-key** commands in the view of the IKE user in the IKE user table.

An IKE user table records the mapping between remote IDs of IKE peers and pre-shared keys. After an IKE peer references an IKE user table, the device searches for the pre-shared key matching the remote ID of the IKE peer in the IKE user table to complete identity authentication during IKE negotiation. In this manner, branches use different IDs and pre-shared keys.

Precautions

- After an IKE peer references an IKE user table, the ID configured using this command can be used to find required resources, for example, the pre-shared key can be found based on the configured ID.
- When IKEv1 in main mode and pre-shared key authentication is used, the value of **id-type** must be set to **ip**. In NAT traversal scenarios, *ipv4-address* should be set to the IP address that is translated using NAT.

Example

Configure the IKE user ID type and ID.

```
<Huawei> system-view
[Huawei] ike user-table 10
[Huawei-ike-user-table-10] user user1
[Huawei-ike-user-table-10-user1] id-type ip 1.1.1.1
```

Related Topics

12.6.127 pre-shared-key (IKE user view)
12.6.137 remote-id-type
12.6.136 remote-id
12.6.27 display ike user-table (all views)

12.6.64 ike call admission limit in-negotiation-sa

Function

The **ike call admission limit in-negotiation-sa** command specifies the maximum number of IKE SAs waiting in a queue.

The **undo ike call admission limit in-negotiation-sa** command restores the default maximum number of IKE SAs waiting in a queue.

By default, the maximum number of IKE SAs waiting in a queue is 800 on a CPU.

Format

ike call admission limit in-negotiation-sa *limit-value*

 Copyright © Huawei Technologies Co., Ltd.

undo ike call admission limit in-negotiation-sa

Parameters

Parameter	Description	Value
limit-value	Specifies the maximum number of IKE SAs waiting in a queue.	The value is an integer that ranges from 1 to 800.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

You can run this command to set the maximum number of IKE SAs waiting in a queue to defend against DOS attacks.

Example

Set the maximum number of IKE SAs waiting in a queue to 100.

```
<Huawei> system-view
[Huawei] ike call admission limit in-negotiation-sa 100
```

12.6.65 ike certificate-check disable

Function

The **ike certificate-check disable** command disables validity verification on certificates of all IKE peers.

The **undo ike certificate-check disable** command restores the default configuration.

By default, the device verifies certificates of all IKE peers.

Format

ike certificate-check disable

undo ike certificate-check disable

Parameters

None

Views

IKE peer view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When IPSec uses certificate authentication, users cannot update certificates after they become invalid, leading to unavailable certificates and IPSec authentication failure. If users still want to use these invalid certificates, run the **ike certificate-check disable** command to disable validity verification on certificates of all IKE peers. If users only want to disable validity verification on certificates of a specified IKE peer, run the **12.6.9 certificate-check disable** command.

Precautions

Disabling validity verification on certificates will lead to security risks.

Example

Configure the device not to verify certificates of all IKE peers.

```
<Huawei> system-view
[Huawei] ike certificate-check disable
```

Related Topics

12.6.17 display ike global config

12.6.66 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.

 Copyright © Huawei Technologies Co., Ltd.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

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.

Precautions

The DSCP priority of IKE packets can be configured in the IKE peer view or system view. The system preferentially uses the DSCP priority configured in the IKE peer view. If the DSCP priority is not configured in the IKE peer view, the system uses the global DSCP priority.

Example

Set a global DSCP priority of IKE packets to CS2.

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

12.6.67 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** }

 Copyright © Huawei Technologies Co., Ltd.

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.

 Copyright © Huawei Technologies Co., Ltd.

Example

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

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

12.6.68 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

 Copyright © Huawei Technologies Co., Ltd.

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
```

12.6.69 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

 Copyright © Huawei Technologies Co., Ltd.

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
```

12.6.70 ike identity

Function

The **ike identity** command creates an identity filter set and enter the identity filter set view.

The **undo ike identity** command deletes an identity filter set.

By default, no identity filter set is configured.

Format

ike identity *identity-name*

undo ike identity *identity-name*

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
identity-name	Specifies the name of the identity filter set.	The value is a string of 1 to 31 case-sensitive characters without spaces.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can run this command to control user access. The remote peer parameters defined in an identity filter set include the name, DN, IP address of the peer. Only initiators that match the identity filter set can establish an IPSec tunnel with the device, improving access security.

Follow-up Procedure

Configure an allowed peer in the identity filter set view and reference this identity filter set with **match ike-identity** command in the policy template view or IPSec profile view.

Precautions

An IPSec tunnel can be established only when the remote end matches one or more parameters in the identity filter set and the IPSec negotiation parameters at both ends are consistent.

Example

Configure an identity filter set named **identity1**.

```
<Huawei> system-view
[Huawei] ike identity identity1
[Huawei-ike-identity-identity1]
```

Related Topics

12.6.121 match ike-identity

12.6.71 ike local-name

Copyright © Huawei Technologies Co., Ltd.

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 domain name, fully qualified domain name (FQDN), or USER-FQDN, the IKE peer uses the name for identity authentication. You can use the following methods to configure the local name:

- Run the **local-id** command in the IKE peer view. After this command is used, only the IKE peer uses the configured name for identity authentication.
- Run the **local-id** command in the system view. After this command is used, all IKE peers use the configured name for identity authentication.

The local name configured using the **local-id** command has a higher priority than that configured using the **ike local-name** command.

Example

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

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

12.6.72 ike nat-keepalive-timer interval

 Copyright © Huawei Technologies Co., Ltd.

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

Usage Scenario

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.

Prerequisites

NAT traversal has been enabled using the **nat traversal** command.

Example

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

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

12.6.73 ike sm-encryption-key-length enable

 Copyright © Huawei Technologies Co., Ltd.

Function

The **ike sm-encryption-key-length enable** command enables IKE negotiation packets to carry the SM encryption key length.

The **undo ike sm-encryption-key-length enable** command disables IKE negotiation packets from carrying the SM encryption key length.

By default, IKE negotiation packets do not carry the SM encryption key length.

Format

ike sm-encryption-key-length enable

undo ike sm-encryption-key-length enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

When a digital envelop is used for IKE negotiation, the negotiation fails if packets sent by the initiator carry the SM encryption key length but the responder cannot process the SM encryption key length. To solve this problem, run the **undo ike sm-encryption-key-length enable** command on the IKE initiator to disable IKE negotiation packets from carrying the SM encryption key length.

Example

Enable IKE negotiation packets to carry the SM encryption key length.

```
<Huawei> system-view
[Huawei] ike sm-encryption-key-length enable
```

Related Topics

12.6.17 display ike global config

12.6.74 ike user-table

Function

The **ike user-table** command creates an IKE user table and displays the IKE user table view, or directly displays the view of an existing IKE user table.

The **undo ike user-table** command deletes an IKE user table.

 Copyright © Huawei Technologies Co., Ltd.

By default, no IKE user table is configured.

Format

ike user-table *user-table-id*

undo ike user-table *user-table-id*

Parameters

Parameter	Description	Value
user-table-id	Specifies the ID of an IKE user table.	The value is an integer and the value range depends on device types. • AR120&150&160&200 series: 1 to 7. • AR1200 series, AR2201-48FE, AR2202-48FE, AR2204, AR2204E: 1 to 200. • AR2220, AR2240 (using SRU40 or SRU60), AR2240C, AR3200 (using SRU40 or SRU60) series: 1 to 400. • AR2204XE, AR2204XE-DC, AR2240 (using SRU80, SRU100, SRU200, SRU200E or SRU400), AR3200 (using SRU80, SRU100, SRU200, SRU200E or SRU400), AR3600 (using SRUX5) series: 1 to 600.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

 Copyright © Huawei Technologies Co., Ltd.

In a point-to-multipoint scenario, the device functions as the VPN gateway of the headquarters, an IPSec policy is created using an IPSec policy template, and the VPN gateway receives IPSec connection setup requests of different branches. Some parameters (for example, pre-shared key and VPN instance) of IKE peers are configured on the headquarters gateway that connect to branch gateways, and the parameters are used by all branches. In this case, services of branches cannot be distinguished, and there are even security risks. When the pre-shared key is used for identity authentication and all branches use the same ID and pre-shared key, there are security risks. That is, if the ID and pre-shared key of one branch leak, the ID and pre-shared key of all branches leak.

You are advised to configure an IKE user table to prevent this problem. The IKE user table records the mapping between remote IDs of IKE peers and other parameters. After an IKE peer references the IKE user table, the device searches for the parameters matching the remote ID of the IKE peer in the IKE user table during IKE negotiation. By doing this, branches use different services.

Follow-up Procedure

Run the **12.6.179 user-table** command in the IKE peer view to reference the IKE user table.

Precautions

The IKE user table that has been referenced by an IKE peer cannot be deleted.

Example

Create an IKE user table **10** and enter its view.

```
<Huawei> system-view
[Huawei] ike user-table 10
[Huawei-ike-user-table-10]
```

Related Topics

12.6.179 user-table

12.6.27 display ike user-table (all views)

12.6.75 ike peer

Function

The **ike peer** command creates an IKE peer and displays the IKE peer view.

The **undo ike peer** command deletes the specified IKE peer.

By default, no IKE peer is configured.

Format

ike peer *peer-name*

undo ike peer *peer-name*

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
peer-name	Specifies the name of an IKE peer.	The value is a string of 1 to 15 case-sensitive characters without question marks (?) and spaces.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can run the **ike peer** command to enter the IKE peer view and then define all parameters for the IKE peer, including:

- Negotiation mode
- ID type
- NAT traversal
- Pre-shared key
- Remote address
- Peer name

Follow-up Procedure

Run the **ike-peer** command to reference the IKE peer.

Example

Create an IKE peer named **peer1** and enter the IKE peer view.

```
<Huawei> system-view
[Huawei] ike peer peer1
[Huawei-ike-peer-peer1]
```

12.6.76 ike proposal

Function

The **ike proposal** command creates an IKE proposal and displays the IKE proposal view.

The **undo ike proposal** command deletes the IKE proposal.

By default, an IKE proposal **Default** with the lowest priority is available.

Table 12-63 describes the default configuration of an IKE proposal.

 Copyright © Huawei Technologies Co., Ltd.

Table 12-63 Default configurations of an IKE proposal

Parameter	Default Configuration
Authentication method	Pre-shared key authentication
Encryption algorithm	AES-256
Diffie-Hellman (DH) group parameter	DH14
IKE SA lifetime	86400 seconds
IKEv1 authentication algorithm	SHA2-256
IKEv2 pseudo-random function algorithm	SHA2-256
IKEv2 integrity function algorithm	SHA2-256

Format

ike proposal *proposal-number*

ike proposal default

undo ike proposal *proposal-number*

Parameters

Parameter	Description	Value
proposal-number	Specifies the number of an IKE proposal. A smaller value indicates a higher priority.	The value is an integer that ranges from 1 to 99.
default	Specifies the default IKE proposal.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

An IKE proposal is a component of an IKE peer and defines IKE negotiation parameters, including the encryption algorithm, authentication method, authentication algorithm, DH group, and SA lifetime.

A smaller IKE proposal number indicates a higher priority. You can create multiple IKE proposals with different priorities. The negotiation succeeds if any IKE proposal is matched.

 Copyright © Huawei Technologies Co., Ltd.

You can configure multiple IKE proposals for each IKE peer. The proposals will be tried in descending order of security level until a matching proposal is found. During an IKE negotiation, the initiator sends its IKE proposal to the remote end, and the remote end uses its IKE proposals starting from the highest priority to match the received proposal before a match is found. The matched IKE proposal will be used to create an IKE IPSec tunnel.

The negotiation mode of an IKE proposal varies depending on the IKE negotiation mode:

- Main mode

  In main mode, if an IKE proposal is specified in the IKE peer that initiates IKE negotiation, only the specified IKE proposal is sent during IKE negotiation. The responder searches for only the IKE proposal matching with that specified by the initiator. If such IKE proposal cannot be found, the negotiation fails.

  If no IKE proposal is specified in the IKE peer that initiates IKE negotiation, all IKE proposals are sent during IKE negotiation. The responder searches for the IKE proposals matching with these proposals sent by the initiator one by one.
- Aggressive mode

  In aggressive mode, if an IKE proposal is specified in the IKE peer that initiates IKE negotiation, the case is the same as that in main mode.

  If no IKE proposal is specified in the IKE peer that initiates IKE negotiation, only the default IKE proposal is sent during IKE negotiation. The responder also matches this IKE proposal with the default IKE proposal.

Follow-up Procedure

Run the **ike-proposal** command in the IKE peer view to reference the IKE proposal.

Example

Configure IKE proposal 10 and enter the IKE proposal view.

```
<Huawei> system-view
[Huawei] ike proposal 10
[Huawei-ike-proposal-10]
```

12.6.77 ike-peer

Function

The **ike-peer** command references an IKE peer in an IPSec policy.

The **undo ike-peer** command cancels the configuration.

By default, no IKE peer is referenced.

Format

ike-peer *peer-name*

undo ike-peer

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
peer-name	Specifies the name of the referenced IKE peer.	The value is an existing IKE peer name.

Views

ISAKMP IPSec policy view, IPSec policy template view, IPSec profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When you configure IKE negotiation, you need to reference an IKE peer in the specified view.

The remote IP address of the IKE peer referenced in an IPSec policy must be unique. You are recommended to configure the remote address range of the IKE peer in an IPSec policy template.

Prerequisites

An IKE peer has been created using the **ike peer** command.

Follow-up Procedure

Run the **12.6.78 ike-proposal** command to reference a configured IKE proposal and run the **12.6.134 remote-address (IKE peer view)** command to configure the remote address or domain name.

Example

Reference the IKE peer **peer1** in the IPSec policy **policy1**.

```
<Huawei> system-view
[Huawei] ipsec policy policy1 1 isakmp
[Huawei-ipsec-policy-isakmp-policy1-1] ike-peer peer1
```

Reference the IKE peer **peer1** in the IPSec profile **profile1**.

```
<Huawei> system-view
[Huawei] ipsec profile profile1
[Huawei-ipsec-profile-profile1] ike-peer peer1
```

12.6.78 ike-proposal

Function

The **ike-proposal** command configures an IKE proposal for an IKE peer.

 Copyright © Huawei Technologies Co., Ltd.

The **undo ike-proposal** command cancels the configuration.

By default, an IKE peer does not reference an IKE proposal.

Format

ike-proposal *proposal-number*

undo ike-proposal

Parameters

Parameter	Description	Value
proposal-number	Specifies the number of the IKE proposal to be used. A smaller value indicates a higher priority.	The value is an integer that ranges from 1 to 99.

Views

IKE peer view

Default Level

2: Configuration level

Usage Guidelines

Configure an IKE proposal using the **ike proposal** command before using this command.

IKE proposal negotiation complies with the following principles:

- If a configured IKE proposal is referenced in the IKE peer view, only the referenced proposal is sent during IKE negotiation, and the responder searches its IKE proposals for a match. If no match is found, the negotiation fails.
- If no IKE proposal is referenced in the IKE peer view (for example, pre-shared and certificate authentication modes are both supported), within the device specifications, a maximum 255 IKE proposals can be carried for IKE negotiation. The responder searches its IKE proposals for a match.

Example

Configure IKE peer **peer1** to reference an IKE proposal **10**.

```
[Huawei] ike peer peer1
[Huawei-ike-peer-peer1] ike-proposal 10
```

12.6.79 ikev1 phase1-phase2 sa dependent

 Copyright © Huawei Technologies Co., Ltd.

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.

Example

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

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

12.6.80 ikev2 authentication sign-hash

Function

The **ikev2 authentication sign-hash** command configures the certificate signature algorithm used by IKEv2.

The **undo ikev2 authentication sign-hash** command restores the default configuration.

 Copyright © Huawei Technologies Co., Ltd.

By default, the certificate signature algorithm used by IKEv2 is SHA2-256.

NOTE

Only V200R010C10 and later version support this command.

Format

ikev2 authentication sign-hash { **md5** | **sha1** | **sha2-256** | **sha2-384** | **sha2-512** }

undo ikev2 authentication sign-hash

Parameters

Parameter	Description	Value
md5	Specifies the certificate signature algorithm as MD5.	-
sha1	Specifies the certificate signature algorithm as SHA1.	-
sha2-256	Specifies the certificate signature algorithm as SHA2-256.	-
sha2-384	Specifies the certificate signature algorithm as SHA2-384.	-
sha2-512	Specifies the certificate signature algorithm as SHA2-512.	-

Views

IKE peer view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In an IKEv2 certificate authentication scenario, if the device functions as the sender, it uses the configured algorithm to sign the certificate. If the decryption algorithm used by the receiver is different from that used by the sender, the signature verification of the receiver fails. As a result, IKEv2 negotiation between the two ends fails. If the device functions as the receiver, it searches for a matching algorithm to verify the signature of packets. The device searches for the matching algorithm in the following sequence: **sha2-256** algorithm, configured algorithm, and then other algorithms. If no matching algorithm is found, the signature verification fails, and IKEv2 negotiation between the two ends fails. To prevent this problem, ensure that the certificate signature algorithms used on the two ends are the same.

Precautions

The following certificate signature algorithms are listed in descending order of security level: **sha2-512**, **sha2-384**, **sha2-256**, **sha1**, and **md5**.

 Copyright © Huawei Technologies Co., Ltd.

Example

Set the certificate signature algorithm used by IKEv2 as SHA2-256.

```
<Huawei> system-view
[Huawei] ike peer peer1
[Huawei-ike-peer-peer1] ikev2 authentication sign-hash sha2-256
```

12.6.81 ikev2 cookie-challenge

Function

The **ikev2 cookie-challenge** command sets the maximum number of half-open connections allowed by IKEv2.

The **undo ikev2 cookie-challenge** command restores the default setting.

By default, the maximum number of half-open connections allowed by IKEv2 is 25000.

Format

ikev2 cookie-challenge *number*

undo ikev2 cookie-challenge

Parameters

Parameter	Description	Value
number	Specifies the maximum number of half-open connections allowed by IKEv2.	The value is an integer that ranges from 1 to 1000.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

IKEv2 initial exchange messages are transmitted in plaintext. If an attack forges massive IKE_INIT_SA requests, the resources of the responder will be exhausted, causing DoS attacks.

Cookie exchange is defined in IKEv2. After receiving the first message from the sender, the responder replies an unprotected notify payload. In follow-up communications, the responder accepts only the IKE negotiation initiated by the sender of cookie-carrying notify payloads.

You can run this command for the device to determine whether and when to enable attack defense.

 Copyright © Huawei Technologies Co., Ltd.

Example

Enable the device to start attack defense when the number of half-open connections allowed by IKEv2 exceeds 200.

```
<Huawei> system-view
[Huawei] ikev2 cookie-challenge 200
```

12.6.82 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.

 Copyright © Huawei Technologies Co., Ltd.

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
```

12.6.83 ikev2 id-match-certificate enable

Function

The **ikev2 id-match-certificate enable** command enables the device to check certificate identity information of the remote device during IKEv2 certificate negotiation.

The **undo ikev2 id-match-certificate enable** command disables the device from checking certificate identity information of the remote device during IKEv2 certificate negotiation.

By default, the device does not check certificate identity information of the remote device during IKEv2 certificate negotiation.

Format

ikev2 id-match-certificate enable

undo ikev2 id-match-certificate enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

By default, the device does not check certificate identity information of the remote device, such as the IP address, fully qualified domain name (FQDN), and email during IKEv2 certificate negotiation. If the certificate of a branch gateway is used by another device, it can establish an IPSec tunnel with the headquarters, causing security risks.

To prevent security risks, you can run the **ikev2 id-match-certificate enable** command to enable the local device to check certificate identity information of the remote device. If the information differs from the ID (IP address, FQDN, or User-FQDN) of the remote device, IKEv2 negotiation fails.

 Copyright © Huawei Technologies Co., Ltd.

Precautions

You can run the **19.17.28 display pki certificate** command to view certificate identity information. The Subject field in the certificate corresponds to the DN, and the email corresponds to the User-FQDN.

Example

Enable the device to check certificate identity information of the remote device during IKEv2 certificate negotiation.

```
<Huawei> system-view
[Huawei] ikev2 id-match-certificate enable
```

12.6.84 ikev2 prf aes-xcbc-128 compatible

Function

The **ikev2 prf aes-xcbc-128 compatible** command configures the IKEv2 PRF AES-XCBC-128 algorithm as a non-standard RFC algorithm.

The **undo ikev2 prf aes-xcbc-128 compatible** command restores the default configuration.

By default, the IKEv2 PRF AES-XCBC-128 algorithm is a standard RFC algorithm.

NOTE

This command is supported in V200R010C10 and later versions.

Format

ikev2 prf aes-xcbc-128 compatible

undo ikev2 prf aes-xcbc-128 compatible

Parameters

None.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

When the device is connected to a device running V200R007 or an earlier version, if both ends use the IKEv2 PRF AES-XCBC-128 algorithm, run the **ikev2 prf aes-xcbc-128 compatible** command on the local device to configure the IKEv2 PRF AES-XCBC-128 algorithm as a non-standard RFC algorithm. Otherwise, the two ends cannot establish an IPSec tunnel.

 Copyright © Huawei Technologies Co., Ltd.

Example

Configure the IKEv2 PRF AES-XCBC-128 algorithm as a non-standard RFC algorithm.

```
<Huawei> system-view
[Huawei] ikev2 prf aes-xcbc-128 compatible
```

12.6.85 inband crl

Function

The **inband crl** command configures the device to validate the remote certificate based on the CRL sent from the remote device when IKEv2 uses RSA signature authentication.

The **undo inband crl** command restores the default configuration.

By default, the device does not validate the remote certificate based on the CRL sent from the remote device when IKEv2 uses RSA signature authentication.

Format

inband crl

undo inband crl

Parameters

None

Views

IKE peer view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When IKEv2 uses RSA signature authentication and the CRL is used for certificate validation, if the CA server is located in the private network of the headquarters, the branch cannot directly communicate with the CA server to obtain the CRL. As a result, the branch cannot use the latest CRL to validate the certificate in the headquarters. To enable the branch to obtain the CRL of the headquarters through IKEv2, run the **inband crl** command on the branch. After receiving the CRL sent from the headquarters through IKEv2, the branch uses this CRL to validate the certificate in the headquarters. If the certificate is not in the CRL, the certificate is considered valid and identity authentication succeeds. The branch can negotiate with the headquarters to establish an IPSec tunnel.

Precautions

 Copyright © Huawei Technologies Co., Ltd.

When you run both the **inband crl** and **12.6.86 inband ocsp** commands, the certificate is considered valid only when it passes the validity check in both OCSP and CRL modes.

The IKEv2 protocol defines the payload length as 2 bytes (that is, the maximum length is 65535). Therefore, when the CRL length exceeds 65535, IKEv2 cannot construct the CRL payload. As a result, the certificate validity check fails.

Example

Configure the device to validate the remote certificate based on the CRL sent from the remote device when IKEv2 uses RSA signature authentication.

```
<Huawei> system-view
[Huawei] ike peer mypeer
[Huawei-ike-peer-mypeer] version 2
[Huawei-ike-peer-mypeer] inband crl
```

12.6.86 inband ocsp

Function

The **inband ocsp** command configures the device to validate the remote certificate based on the OCSP validation result sent from the remote device when IKEv2 uses RSA signature authentication.

The **undo inband ocsp** command restores the default configuration.

By default, the device does not validate the remote certificate based on the OCSP validation result sent from the remote device when IKEv2 uses RSA signature authentication.

Format

inband ocsp

undo inband ocsp

Parameters

None

Views

IKE peer view

Default Level

2: Configuration level

Usage Guidelines

When IKEv2 uses RSA signature authentication and OCSP is used for certificate validation, if the OCSP server is located in the private network of the headquarters, the branch cannot directly communicate with the OCSP server to

 Copyright © Huawei Technologies Co., Ltd.

validate the certificate in the headquarters. To enable the branch to obtain the OCSP validation result of the headquarters through IKEv2, run the **inband ocsp** command on the branch. After receiving the OCSP validation result sent from the headquarters through IKEv2, the branch uses the OCSP validation result to validate the certificate in the headquarters. If the OCSP validation result is valid, the certificate is considered valid and identity authentication succeeds. The branch can negotiate with the headquarters to establish an IPSec tunnel.

When you run both the **inband ocsp** and **12.6.85 inband crl** commands, the certificate is considered valid only when it passes the validity check in both OCSP and CRL modes.

Example

Configure the device to validate the remote certificate based on the OCSP validation result sent from the remote device when IKEv2 uses RSA signature authentication.

```
<Huawei> system-view
[Huawei] ike peer mypeer
[Huawei-ike-peer-mypeer] version 2
[Huawei-ike-peer-mypeer] inband ocsp
```

12.6.87 integrity-algorithm

Function

The **integrity-algorithm** command configures an integrity algorithm for IKEv2 negotiation.

The **undo integrity-algorithm** command restores the default configuration.

By default, the HMAC-SHA2-256 integrity algorithm is used for IKEv2 negotiation.

Format

integrity-algorithm { **aes-xcbc-96** | **hmac-md5-96** | **hmac-sha1-96** | **hmac-sha2-256** | **hmac-sha2-384** | **hmac-sha2-512** }

undo integrity-algorithm

Parameters

Parameter	Description	Value
aes-xcbc-96	Indicates that the integrity algorithm is AES-XCBC-96.	-
hmac-md5-96	Indicates that the integrity algorithm is HMAC-MD5-96.	-
hmac-sha1-96	Indicates that the integrity algorithm is HMAC-SHA1-96.	-
hmac-sha2-256	Indicates that the integrity algorithm is HMAC-SHA2-256.	-
hmac-sha2-384	Indicates that the integrity algorithm is HMAC-SHA2-384.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
hmac-sha2-512	Indicates that the integrity algorithm is HMAC-SHA2-512.	-

Views

IKE proposal view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The integrity algorithms are listed as follows from the highest security level to the lowest security level: **hmac-sha2-512** > **hmac-sha2-384** > **hmac-sha2-256** > **aes-xcbc-96** > **hmac-sha1-96** > **hmac-md5-96**.

Precautions

On the device running a version earlier than V200R008, the **authentication-algorithm** command serves the same function as the **integrity-algorithm** command.

Example

Set the integrity algorithm to be used in IKEv2 proposal **10** to HMAC-SHA2-384.

```
<Huawei> system-view
[Huawei] ike proposal 10
[Huawei-ike-proposal-10] integrity-algorithm hmac-sha2-384
```

12.6.88 interface-assign

Function

The **interface-assign** command assigns an interface associated with an IKE user.

The **undo interface-assign** command deletes an interface associated with an IKE user.

By default, no interface on the device is associated with the IKE user.

Format

interface-assign *interface-type interface-number*

undo interface-assign

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
interface-type interface-number	Specifies the type and number of an interface. Currently, the interface can only be a tunnel interface.	-

Views

IKE user view

Default Level

2: Configuration level

Usage Guidelines

In a point-to-multipoint scenario, the device functions as the VPN gateway of the headquarters. The IKE user table in the headquarters contains multiple IKE users for managing parameters for interconnection between the headquarters and branches, such as the pre-shared key. If one IPSec profile in the headquarters is applied to multiple tunnel interfaces, IPSec negotiation may fail because the IKE peer in the headquarters fails to match the tunnel interface of each branch. In this case, you can run the **interface-assign** command to assign a tunnel interface associated with an IKE user, so that IKE users can successfully match tunnel interfaces of branches.

Example

Assign an interface associated with the IKE user.

```
<Huawei> system-view
[Huawei] interface tunnel 0/0/1
[Huawei] quit
[Huawei] ike user-table 10
[Huawei-ike-user-table-10] user user1
[Huawei-ike-user-table-10-user1] interface-assign tunnel 0/0/1
```

Related Topics

12.6.27 display ike user-table (all views)

12.6.89 interface tunnel-template

Function

The **interface tunnel-template** command creates a tunnel template interface and enters the tunnel template interface view.

The **undo interface tunnel-template** command deletes the tunnel template interface.

 Copyright © Huawei Technologies Co., Ltd.

By default, no tunnel template interface exists.

Format

interface tunnel-template *interface-number*

undo interface tunnel-template *interface-number*

Parameters

Parameter	Description	Value
interface-number	Specifies the number of the tunnel template interface.	The value range depends on the device.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A virtual tunnel template interface is similar to a virtual tunnel interface. You can create a tunnel template interface on the headquarters gateway and then apply an IPSec profile to the tunnel template interface and the tunnel interface of the branch gateway respectively to enable the gateways to send or accept subnet route information.

Follow-up Procedure

After creating a tunnel template interface, run the **tunnel-protocol ipsec** command to set the encapsulation mode of the tunnel template interface to IPSec.

Example

Create a tunnel template interface.

```
<Huawei> system-view
[Huawei] interface tunnel-template 1
[Huawei-Tunnel-Template1]
```

Related Topics

12.6.29 display interface tunnel-template

 Copyright © Huawei Technologies Co., Ltd.

12.6.90 ip address

Function

The **ip address** command specifies the IP address of an allowed peer for IKE negotiation.

The **undo ip address** command deletes the IP address of an allowed peer.

By default, no IP address of allowed peer for IKE negotiation is configured.

Format

ip address *ip-address* { *mask* | *mask-length* }

undo ip address *ip-address* { *mask* | *mask-length* }

Parameters

Parameter	Description	Value
ip-address { *mask* | *mask-length* }	Specifies the IP address of an allowed peer. • *ip-address* specifies the IP address. • *mask* specifies the mask of the IP address. • *mask-length* specifies the mask length of IP address.	• The value of *ip-address* is in dotted decimal notation. • The value of *mask* is in dotted decimal notation. • The value of *mask-length* is an integer that ranges from 0 to 32.

Views

Identity filter set view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can run this command to specify an allowed peer based on the IP address (configured on a remote device for establishing an IPSec tunnel) in the identity filter set for IKE negotiation.

Precautions

 Copyright © Huawei Technologies Co., Ltd.

An IPSec tunnel can be established only when the remote end matches one or more parameters in the identity filter set and the IPSec negotiation parameters at both ends are consistent.

If you run this command in the same view multiple times, the latest configuration does not override earlier ones.

Example

Configure the IP address **10.1.1.1** of an allowed peer for IKE negotiation.

```
<Huawei> system-view
[Huawei] ike identity identity1
[Huawei-ike-identity-identity1] ip address 10.1.1.1 24
```

Related Topics

12.6.70 ike identity

12.6.117 local-id-type

12.6.91 ip address ike-negotiated

Function

The **ip address ike-negotiated** command configures an IKE peer to request an IP address for an IPSec tunnel interface through IKEv2 negotiation.

The **undo ip address ike-negotiated** command cancels the configuration.

By default, an IKE peer does not request an IP address for an IPSec tunnel interface through IKEv2 negotiation.

Format

ip address ike-negotiated

undo ip address ike-negotiated

Parameters

None

Views

Tunnel interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the **ip address ike-negotiated** command is used in scenarios where many branches connect to the headquarters, the headquarters pushes the IP address of

 Copyright © Huawei Technologies Co., Ltd.

the IPSec tunnel interface. This reduces the configuration and maintenance workload of branches.

Prerequisites

The tunneling protocol has been configured as IPSec on the IPSec tunnel interface using the **tunnel-protocol ipsec command.**

Precautions

If the **ip address** command has been used to configure an IP address for the IPSec tunnel interface, when you run the **ip address ike-negotiated** command, the system displays a message indicating a conflict. If the **ip address ike-negotiated** command has been configured on the IPSec tunnel interface, the **ip address** command executed later will take effect.

Example

Configure an IKE peer to request an IP address for Tunnel0/0/1 through IKEv2 negotiation.

```
<Huawei> system-view
[Huawei] interface tunnel 0/0/1
[Huawei-Tunnel0/0/1] tunnel-protocol ipsec
[Huawei-Tunnel0/0/1] ip address ike-negotiated
```

Related Topics

12.3.21 tunnel-protocol

12.6.92 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

 Copyright © Huawei Technologies Co., Ltd.

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

Only SAs established in IKE negotiation mode support the anti-replay function. Manually configured SAs do not support the anti-replay function.

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
```

Related Topics

12.6.93 ipsec anti-replay window

12.6.93 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.

 Copyright © Huawei Technologies Co., Ltd.

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
```

Related Topics

12.6.92 ipsec anti-replay enable

 Copyright © Huawei Technologies Co., Ltd.

12.6.94 ipsec authentication sha2 compatible enable

Function

The **ipsec authentication sha2 compatible enable** command enables SHA-2 to be compatible with RFC standard algorithm versions.

The **undo ipsec authentication sha2 compatible enable** command disables SHA-2 from being compatible with RFC standard algorithm versions.

By default, the SHA-2 algorithm is not compatible with RFC standard algorithm versions.

Format

ipsec authentication sha2 compatible enable

undo ipsec authentication sha2 compatible enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When IPSec uses the SHA-2 algorithm, if the devices on two ends of an IPSec tunnel are from different vendors or run different software versions, they may use different encryption and decryption methods. In this situation, traffic between devices is interrupted.

To solve this problem, run the **ipsec authentication sha2 compatible enable** command to enable SHA-2 to be compatible with RFC standard algorithm versions.

Precautions

When AR routers are interconnected, ensure that the configuration are the same; otherwise, IPSec traffic fails to be transmitted.

This function takes effect only after you run the **reset ike sa** command.

Example

Enable the SHA-2 algorithm to be compatible with RFC standard algorithm versions.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> system-view
[Huawei] ipsec authentication sha2 compatible enable
```

12.6.95 ipsec decrypt check

Function

The **ipsec decrypt check** command enables a device to check decrypted IPSec packets.

The **undo ipsec decrypt check** command disables a device from checking decrypted IPSec packets.

By default, the device does not check decrypted IPSec packets.

Format

ipsec decrypt check

undo ipsec decrypt check

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

In tunnel mode, the IP header in the decrypted IPSec packet of the inbound SA may be not defined in an ACL, for example, the IP header of attack packets may be out of the range defined in the ACL. Therefore, the device checks whether the IP header of the decrypted IPSec packet is in the range defined by the ACL. If the decrypted IPSec packet matches the permit clause, the device continues to process the IPSec packet. If the decrypted IPSec packet does not match the permit clause, the device discards the IPSec packet. The device discards the IPSec packets failing the ACL check to improve network security.

When establishing an IPSec tunnel using a tunnel interface, if the **ipsec decrypt check** command is executed in the system view, packets decrypted by IPSec are check based on the ACL rule. Note the following points:

- When the encapsulation mode is set to IPSec, the source and destination addresses in the ACL are both any, indicating that all data flows destined for the IPSec tunnel interface are protected.
- When the encapsulation mode is set to GRE, the source and destination addresses in the ACL are the source and destination addresses of the IPSec tunnel interface respectively.

 Copyright © Huawei Technologies Co., Ltd.

Example

Disable the device from checking decrypted IPSec packets.

```
<Huawei> system-view
[Huawei] undo ipsec decrypt check
```

12.6.96 ipsec df-bit

Function

The **ipsec df-bit** command sets the don't fragment (DF) flag bit in an IPSec or a A2A VPN packet.

By default, the DF flag bit in an IPSec or a A2A VPN packet is the flag bit of original packets.

Format

ipsec df-bit { **clear** | **set** | **copy** }

Parameters

Parameter	Description	Value
clear	Sets the DF flag bit to 0, indicating that IP packets can be fragmented.	-
set	Sets the DF flag bit to 1, indicating that IP packets cannot be fragmented.	-
copy	Uses the flag bit of original packets.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After an original packet is encapsulated, the packet length may exceed the MTU of the device outbound interface. To prevent packet loss, fragment the packets.

Precautions

 Copyright © Huawei Technologies Co., Ltd.

If you run the **ipsec df-bit** command multiple times, only the latest configuration takes effect.

Example

Set the DF flag bit to 0 in an IPSec or a A2A VPN packet.

```
<Huawei> system-view
[Huawei] ipsec df-bit clear
```

Related Topics

12.6.99 ipsec fragmentation before-encryption

12.6.97 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

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

 Copyright © Huawei Technologies Co., Ltd.

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 **Ethernet 1/0/2**.

```
<Huawei> system-view
[Huawei] interface ethernet 1/0/2
[Huawei-Ethernet1/0/2] ipsec efficient-vpn evpn
```

Related Topics

12.6.30 display ipsec efficient-vpn

12.6.98 ipsec efficient-vpn (system view)

12.6.98 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-auto-cfg** | **network-plus** }]

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

 Copyright © Huawei Technologies Co., Ltd.

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-auto-cfg	Indicates the network-auto-cfg mode. The Network-auto-cfg mode is supported in IKEv1 only.	-
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

 Copyright © Huawei Technologies Co., Ltd.

remote device automatically enables NAT to translate its original IP address into the obtained IP address, and then uses this IP address to establish an IPSec tunnel with the headquarters.

The client mode applies to scenarios where traveling staff or 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. Therefore, NAT is not automatically enabled in network mode.

  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. NAT is not automatically enabled on the remote device.

- Network-auto-cfg mode

  Compared with the network-plus mode, the remote device applies to the Efficient VPN server for an IP address pool in network-auto-cfg mode. The IP address pool is used for allocating addresses to users.

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]
```

Related Topics

12.6.30 display ipsec efficient-vpn

12.6.97 ipsec efficient-vpn (interface view)

12.6.99 ipsec fragmentation before-encryption

 Copyright © Huawei Technologies Co., Ltd.

Function

The **ipsec fragmentation before-encryption** command sets the fragmentation mode of packets to fragmentation before encryption for all IPSec tunnels or a A2A VPN.

The **undo ipsec fragmentation before-encryption** command restores the default packet fragmentation mode.

By default, the packet fragmentation mode for all IPSec tunnels or a A2A VPN is fragmentation after encryption.

Format

ipsec fragmentation before-encryption

undo ipsec fragmentation before-encryption

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After an original packet is encapsulated, the packet length may exceed the MTU of the device outbound interface. To prevent packet loss, the device fragments the packets. Two fragmentation modes are available:

- Fragmentation before encryption: Before encapsulation, the encryption device calculates the predicted encapsulated packet length. If the packet length is larger than the MTU of the outbound interface, the encryption device fragments packets, and then encrypts the packets. In this situation, the decryption device requests the terminal to reassemble the packets, reducing the CPU usage on the decryption device.
- Fragmentation after encryption: If the size of the encapsulated VPN packets exceeds the MTU of the outbound interface, the encryption device fragments the packets based on the MTU of the outbound interface. In this case, the peer decryption device assembles and decrypts VPN fragments and then sends decrypted packets to the terminal host.

Precautions

Before IPSec packets can be fragmented, the **ipsec df-bit** command must be configured to permit IPSec packet fragmentation.

This command just specifies how the IPSec tunnels process packets. However, whether a packet is fragmented depends on:

 Copyright © Huawei Technologies Co., Ltd.

- The DF bit in IP header of the original packet if the fragmentation before encryption mode is selected
- The DF bit in IPSec header if the fragmentation after encryption mode is selected

For the established IPSec tunnels, you need to restart them after running this command. Otherwise, the command function does not take effect.

Example

Set the fragmentation mode of IPSec or a A2A VPN packets to fragmentation before encryption.

```
<Huawei> system-view
[Huawei] ipsec fragmentation before-encryption
```

12.6.100 ipsec invalid-spi-recovery enable

Function

The **ipsec invalid-spi-recovery enable** command enables the invalid SPI recovery function.

The **undo ipsec invalid-spi-recovery enable** command disables the invalid SPI recovery function.

By default, the invalid SPI recovery function is disabled.

Format

ipsec invalid-spi-recovery enable

undo ipsec invalid-spi-recovery enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the IPSec SA is lost on Gateway_1 at one end of an IPSec tunnel, the corresponding IKE SA still exists on Gateway_1. However, Gateway_2 at the other end of the IPSec tunnel still maintains the IPSec SA. If Gateway_1 receives IPSec packets encapsulated by Gateway_2 using the IPSec SA, Gateway_1 discards the

 Copyright © Huawei Technologies Co., Ltd.

packets because it cannot find the corresponding IPSec SA. At the same time, Gateway_1 sends a DELETE SA INFORMATIONAL message to Gateway_2 by default. After receiving the message, Gateway_2 immediately deletes the IPSec SA matching the invalid SPI. When Gateway_2 continues sending IPSec packets to Gateway_1, the two ends re-negotiate an IPSec SA to restore the IPSec service.

However, when neither IKE SA nor IPSec SA exists on Gateway_1, Gateway_1 does not send a DELETE SA INFORMATIONAL message to Gateway_2 until dead peer detection (DPD) shows that the IPSec SA is invalid or the SA lifetime has expired. This causes lengthy IPSec service interruption. In this case, you can enable the invalid SPI recovery function to solve the problem. When Gateway_1 sends IPSec packets to Gateway_2, the two ends re-negotiate an IPSec SA to restore the IPSec service.

Precautions

The invalid SPI recovery function may lead to denial of service (DoS) attacks.

When the device uses an IPSec policy configured using an IPSec policy template or has the **12.6.147 respond-only enable** command configured, the **ipsec invalid-spi-recovery enable** command does not take effect.

Example

Enable the invalid SPI recovery function.

```
<Huawei> system-view
[Huawei] ipsec invalid-spi-recovery enable
```

Related Topics

12.6.32 display ipsec global config

12.6.25 display ike statistics

12.6.101 ipsec nat-traversal source-port

Function

The **ipsec nat-traversal source-port** command configures a UDP port number for IPSec NAT traversal.

The **undo ipsec nat-traversal source-port** command restores the default UDP port number for IPSec NAT traversal.

By default, the UDP port number for IPSec NAT traversal is 4500.

Format

ipsec nat-traversal source-port *port-number*

undo ipsec nat-traversal source-port

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
port-number	Specifies the UDP port number for IPSec NAT traversal.	The value is an integer that ranges from 4501 to 49151.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

By default, IPSec NAT traversal uses UDP port 4500. If you want to use another UDP port for IPSec NAT traversal, run the **ipsec nat-traversal source-port** command.

Example

Set a UDP port number for IPSec NAT traversal.

```
<Huawei> system-view
[Huawei] ipsec nat-traversal source-port 4510
```

Related Topics

12.6.32 display ipsec global config

12.6.102 ipsec netmask

Function

The **ipsec netmask** command configures the IPSec mask filtering function.

The **undo ipsec netmask** command deletes the IPSec mask filtering function.

By default, IPSec mask filtering is not configured in the system.

Format

ipsec netmask { **source** *source-mask* | [**source** *source-mask*] **destination** *destination-mask* }

undo ipsec netmask [**source** | **destination**]

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
source *source-mask*	Specifies the source IPv4 address mask of data flows.	The value is an integer in the range from 1 to 32.
destination *destination-mask*	Specifies the destination IPv4 address mask of data flows.	The value is an integer in the range from 1 to 32.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In scenarios where branches connect to the headquarters, if a branch has a too large protection data flow range configured, traffic of other branches may be incorrectly diverted to the branch. In this case, you can run the **ipsec netmask** command to check and restrict the access of flow information negotiated by the IPSec tunnel. After this function is configured, the device checks the source and destination IP address masks of the peer device. If the mask values are greater than or equal to the configured values, subsequent negotiation continues. Otherwise, the IPSec SA negotiation fails.

Precautions

The device checks and restricts the access of flow information only when it adopts the IPSec policy template.

Example

Configure the IPSec mask filtering function.

```
<Huawei> system-view
[Huawei] ipsec netmask source 24 destination 24
```

Related Topics

12.6.32 display ipsec global config

 Copyright © Huawei Technologies Co., Ltd.

12.6.103 ipsec policy shared

Function

The **ipsec policy shared** command configures a security policy as a multi-link shared security policy.

The **undo ipsec policy shared** command cancels configuring a security policy as a multi-link shared security policy.

By default, no security policy is configured as a multi-link shared security policy.

Format

ipsec policy *policy-name* **shared local-interface loopback** *interface-number*

undo ipsec policy *policy-name* **shared**

Parameters

Parameter	Description	Value
policy-name	Specifies the name of a security policy. The security policy must have been configured in the system view.	The value is a string of 1 to 15 case-sensitive characters without question marks (?) or spaces.
local-interface loopback *interface-number*	Specifies the loopback interface number. The loopback interface must have been created.	The value is an integer that ranges from 0 to 1023.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To improve network reliability, the enterprise gateway often connects to the Internet Service Provider (ISP) through two egress links, which work in backup or load balancing mode. When two outbound interfaces are configured with IPSec policies with the same parameter settings, services need to be smoothly switched between the two links corresponding to the two outbound interfaces. The two outbound interfaces negotiate with their peers to establish IPSec SAs respectively. When one interface alternates between Up and Down states and an active/standby switchover occurs, the two peers need to perform IKE negotiate again to

 Copyright © Huawei Technologies Co., Ltd.

generate IPSec SAs. The IKE re-negotiation causes IPSec service interruption in a short time.

You can configure a multi-link shared security policy and use a loopback interface on the local device to establish an IPSec tunnel with the remote device. When an active/standby switchover occurs, IPSec services are not interrupted. The two IPSec-enabled physical interfaces share the same IPSec SA. When services are switched between links corresponding to the physical interfaces, the IPSec SA is not deleted as long as the loopback interface status remains unchanged. In addition, IKE re-negotiation is not required because the same IPSec SA is used to protect IPSec services.

In an A2A VPN scenario, a GDOI policy can also be configured as a multi-link shared security policy. GMs then register with the KS using loopback interfaces and negotiate to generate one KEK SA. In this manner, multiple interfaces to which the GDOI policy is applied share the same KEK SA.

Precautions

One loopback interface maps to only one multi-link shared security policy.

Example

Configure an IPSec policy as a multi-link shared security policy.

```
<Huawei> system-view
[Huawei] interface loopback 0
[Huawei-LoopBack0] quit
[Huawei] ipsec policy policy1 11 isakmp
[Huawei-ipsec-policy-isakmp-policy1-11] quit
[Huawei] ipsec policy policy1 shared local-interface loopback 0
```

Configure a GDOI policy as a multi-link shared security policy.

```
<Huawei> system-view
[Huawei] interface loopback 1
[Huawei-LoopBack1] quit
[Huawei] ipsec policy policy2 12 gdoi
[Huawei-ipsec-policy-gdoi-policy2-12] quit
[Huawei] ipsec policy policy2 shared local-interface loopback 1
```

12.6.104 ipsec policy (interface view)

Function

The **ipsec policy** command binds an IPSec policy group to an interface.

The **undo ipsec policy** command unbinds an IPSec policy group from an interface.

By default, no IPSec policy group is bound to an interface.

Format

ipsec policy *policy-name*

undo ipsec policy

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
policy-name	Specifies the name of an IPSec policy group bound to an interface.	The value must be the name of an existing IPSec policy group on the device.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can bind an IPSec policy group to a physical or logical interface to protect data flows. In addition to physical interfaces such as serial interfaces and Ethernet interfaces, you can bind an IPSec policy group to virtual interfaces such as Tunnel interfaces. IPSec policy groups can be used according to actual networking requirements. If an IPSec policy group is unbound from an interface, the interface cannot provide IPSec functions.

After an IPSec policy group is bound to an interface, all IPSec policies in the group are bound to the interface to protect different data flows.

When sending a packet, an interface matches the packet with IPSec policies in an IPSec policy group in ascending order of sequence number. If the packet matches the ACL referenced by an IPSec policy, the packet is processed based on the IPSec policy. If the packet does not match an IPSec policy, it searches for the next policy. If no matching ACL is found after all IPSec policies are checked, the interface sends the packet directly without IPSec protection.

Precautions

IPSec policy group can not be bound to VLANIF interface and loopback interface.

Only one IPSec policy group can be bound to an interface, and an IPSec policy group can be bound to only one interface. To bind a new IPSec policy group to an interface, remove the previous one first.

When an IPSec policy group contains both an IPSec policy configured using an IPSec policy template and an IPSec policy in ISAKMP mode, to match the IPSec policy in ISAKMP mode, ensure that the sequence number of the IPSec policy in ISAKMP mode is smaller than that of the IPSec policy configured using an IPSec policy template.

In an IPSec policy group, if multiple policies are bound to different IKE peers, the remote addresses specified in the IKE peers cannot be the same. Otherwise, IKE negotiation of some IPSec policies fails.

 Copyright © Huawei Technologies Co., Ltd.

If multiple IPSec policies are bound to the same IKE peer in an IPSec policy group, the same tunnel local address must be configured for these IPSec policies. Otherwise, IKE negotiation of some IPSec policies fails.

When the number of IPSec tunnels is larger than 50% of the maximum limit, high CPU usage alarms may be generated in a short period of time after the **undo ipsec policy** command is run. After all the SAs are cleared, the CPU usage restores to the normal range.

In the PPPoE scenario, the application of IPSec policies on the VT interface of the PPPoE server is not supported.

A tunnel interface and the source interface that is referenced by the tunnel interface cannot be both bound to IPSec policies.

Example

Apply the IPSec policy group **policy1** to Eth1/0/2.

```
<Huawei> system-view
[Huawei] ipsec policy policy1 1 isakmp
[Huawei-ipsec-policy-isakmp-policy1-1] quit
[Huawei] interface ethernet 1/0/2
[Huawei-Ethernet1/0/2
] ipsec policy policy1
```

Related Topics

12.6.105 ipsec policy (system view)

12.6.105 ipsec policy (system view)

Function

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

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

By default, no IPSec policy is configured.

Format

ipsec policy *policy-name seq-number* [**manual** | **isakmp** [**template** *template-name*]]

undo ipsec policy *policy-name* [*seq-number*]

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
policy-name	Specifies the name of an IPSec policy.	The value is a string of 1 to 15 case-sensitive characters without question marks (?) and spaces.
seq-number	Specifies the sequence number of an IPSec policy.	The value is an integer that ranges from 1 to 10000. A smaller value indicates a higher IPSec policy priority.
manual	Indicates that an IPSec SA is created manually.	-
isakmp	Indicates that an IPSec policy is established in IKE negotiation mode.	-
template *template-name*	Indicates that an IPSec policy is established by referencing an IPSec policy template.	The value must be an existing IPSec policy template name.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

An IPSec policy is uniquely defined by its name and sequence number. IPSec policies with the same name belong to one IPSec policy group.

- Manual mode

  IPSec parameters including the authentication/encryption key and SPI on IPSec peers must mirror each other. That is, IPSec parameters of the inbound SA at the local end must be the same as those of the outbound SA at the remote end, and IPSec parameters of the outbound SA at the local end must be the same as those of the inbound SA at the remote end.

- IKE negotiation mode

  IPSec parameters are automatically negotiated through IKE. This mode is classified into ISAKMP and IPSec policy template:

 Copyright © Huawei Technologies Co., Ltd.

- ISAKMP

  Negotiated IPSec parameters are defined in the IPSec policy view, and the initiator and responder must use the same IPSec parameters.

  Devices use the ISAKMP policy can be an initiator or a responder.

- IPSec policy template

  An IPSec policy template defines negotiated parameters. The initiator determines optional parameters, and the responder accepts the parameters delivered by the initiator.

  An IPSec policy template can reduce the workload of establishing multiple IPSec tunnels. The IPSec policy template is applicable to specific scenarios, for example, scenario where the remote IP address is variable or unknown (for example, the remote end obtains an IP address using PPPoE) and the remote device is allowed to initiate negotiation to the local end.

  ACLs in this mode are optional. If no ACL is configured, the responder uses the ACL configured on the initiator to protect data flows.

Follow-up Procedure

Define negotiated IPSec parameters in the IPSec policy view and run the **ipsec policy (interface view)** command to bind the IPSec policy to an interface.

Precautions

- The end where an IPSec policy template is configured can only function as the responder to receive negotiation requests.
- One IPSec policy group can have only one IPSec policy template.
- When creating an IPSec policy, you must specify the SA creation mode. If you have entered the IPSec policy view, you do not need to enter the SA creation mode.
- Before modifying the negotiation mode of a created IPSec policy, delete the IPSec policy and create an IPSec policy again.

Example

Set an IPSec policy using the ISAKMP negotiation mode. The IPSec policy name is **policy1** and the sequence number is **1**.

```
<Huawei> system-view
[Huawei] ipsec policy policy1 1 isakmp
[Huawei-ipsec-policy-isakmp-policy1-1]
```

Set an IPSec policy using the manual negotiation mode. The IPSec policy name is **policy2** and the sequence number is **1**.

```
<Huawei> system-view
[Huawei] ipsec policy policy2 1 manual
[Huawei-ipsec-policy-manual-policy2-1]
```

Related Topics

12.6.104 ipsec policy (interface view)
12.6.34 display ipsec policy (all views)

 Copyright © Huawei Technologies Co., Ltd.

12.6.106 ipsec policy-template

Function

The **ipsec policy-template** command creates an IPSec policy template and displays the IPSec policy template view.

The **undo ipsec policy-template** command deletes an IPSec policy template group or an IPSec policy template from the group.

By default, no IPSec policy template is created.

Format

ipsec policy-template *template-name seq-number*

undo ipsec policy-template *template-name* [*seq-number*]

Parameters

Parameter	Description	Value
template-name	Specifies the name of the policy template.	It is a string of 1 to 15 case sensitive characters and cannot contain the hyphen (-).
seq-number	Specifies the sequence number of the IPSec policy.	It is an integer that ranges from 1 to 10000. The smaller the value is, the higher the priority is.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Negotiated IPSec parameters are defined in the IPSec policy template view. The initiator determines optional parameters, and the responder accepts the parameters delivered by the initiator. If an IPSec policy template is configured at the local end, the local end can only function as the responder to receive negotiation requests.

An IPSec policy template can be used to configure multiple IPSec policies, reducing the workload of establishing multiple IPSec tunnels. An IPSec policy template is applicable to specific scenarios, for example, scenario where the remote IP address is variable or unknown and the remote peers are allowed to initiate negotiation to the local end.

 Copyright © Huawei Technologies Co., Ltd.

ACLs in this mode are optional. If no ACL is configured, the responder uses the ACL configured on the initiator to protect data flows.

Follow-up Procedure

Run the **ipsec policy** *policy-name seq-number* **isakmp template** *template-name* command to reference the created template.

Precautions

The IPSec policy template name must be different from the IPSec policy name.

Example

Create an IPSec policy template with the name **policy1** and the sequence number **1**.

```
<Huawei> system-view
[Huawei] ipsec policy-template policy1 1
[Huawei-ipsec-policy-templet-policy1-1]
```

Related Topics

12.6.36 display ipsec policy-template (all views)

12.6.105 ipsec policy (system view)

12.6.107 ipsec profile (interface view)

Function

The **ipsec profile** command applies an IPSec profile to a tunnel interface.

The **undo ipsec profile** command unbinds the IPSec profile from a tunnel interface.

By default, no IPSec profile is applied to a tunnel interface.

Format

ipsec profile *profile-name*

undo ipsec profile

NOTE

V200R010 does not support the shared parameter. That is, the same physical outbound interface cannot be specified for multiple tunnel interfaces.

Parameters

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

 Copyright © Huawei Technologies Co., Ltd.

Views

Tunnel interface view, Tunnel-Template interface view

Default Level

2: Configuration level

Usage Guidelines

Prerequisites

An IPSec profile has been created using the **ipsec profile (system view)** command.

A tunnel interface has been created using the **12.3.10 interface tunnel** command, and the encapsulation mode of the tunnel interface has been set to GRE or IPSec using the **12.3.21 tunnel-protocol** command.

Precautions

- A tunnel interface can be bound to only one IPSec profile. An IPSec profile can be applied to only one tunnel interface.
- A tunnel template interface can be bound to only one IPSec profile. An IPSec profile can be applied to only one tunnel template interface.
- When the number of IPSec tunnels is larger than 50% of the maximum limit, high CPU usage alarms may be generated in a short period of time after the **undo ipsec profile** command is run. After all the SAs are cleared, the CPU usage restores to the normal range.
- A tunnel interface and the source interface that is referenced by the tunnel interface cannot be both bound to IPSec profiles.

Example

Bind the IPSec profile **profile1** to tunnel interface **tunnel 0/0/1**.

```
<Huawei> system-view
[Huawei] interface tunnel 0/0/1
[Huawei-Tunnel0/0/1] tunnel-protocol ipsec
[Huawei-Tunnel0/0/1] source 10.1.1.1
[Huawei-Tunnel0/0/1] ipsec profile profile1
```

Related Topics

12.3.10 interface tunnel

12.3.21 tunnel-protocol

12.6.108 ipsec profile (system view)

12.6.38 display ipsec profile (all views)

12.6.108 ipsec profile (system view)

Function

The **ipsec profile** command creates an IPSec profile and enters the IPSec profile view.

 Copyright © Huawei Technologies Co., Ltd.

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

By default, no IPSec profile is configured.

Format

ipsec profile *profile-name*

undo ipsec profile *profile-name*

Parameters

Parameter	Description	Value
profile-name	Specifies the name of an IPSec profile.	The value is a string of 1 to 32 case-sensitive characters without question marks (?) and spaces.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

An IPSec profile is similar to an IPSec policy. However, different from an IPSec policy, an IPSec profile is identified by its name, and can only be configured in IKE negotiation mode. The IPSec profile does not support ACL configuration. The IPSec profile can be applied to only an IPSec tunnel interface. An IPSec profile defines IPSec proposals used to protect data flows, IKE negotiation parameters for SA setup, SA lifetime, and PFS status. After an IPSec profile is applied to an IPSec tunnel interface, only one IPSec tunnel is created. The IPSec tunnel protects all the data flows routed to the IPSec tunnel interface, simplifying IPSec policy management.

Follow-up Procedure

Define negotiated IPSec parameters in the IPSec profile view and run the **12.6.107 ipsec profile (interface view)** command to apply the IPSec profile to an interface.

Precautions

You do not need to specify the local and remote addresses for the IKE peer that is referenced by an IKE profile. Even if the local and remote addresses are specified for the IKE peer that is referenced by an IKE profile, the local and remote addresses are invalid. This is because the source and destination addresses of the IPSec tunnel interfaces are used as local and remote addresses when the IPSec profile performs IKE negotiation.

 Copyright © Huawei Technologies Co., Ltd.

Example

Create an IPSec profile named **profile1**.

```
<Huawei> system-view
[Huawei] ipsec profile profile1
[Huawei-ipsec-profile-profile1]
```

Related Topics

12.6.38 display ipsec profile (all views)
12.6.107 ipsec profile (interface view)

12.6.109 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-sensitive characters without question marks (?) and spaces.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

An IPSec proposal is a part of an IPSec policy or an IPSec profile. It defines IPSec protection methods and security parameters for IPSec SA negotiation. The parameters include the security protocol, encryption and authentication algorithms, and encapsulation mode.

 Copyright © Huawei Technologies Co., Ltd.

Follow-up Procedure

1. Configure security parameters including the security protocol, encryption and authentication algorithms, and encapsulation mode.
2. Run the **proposal** command to reference the IPSec proposal in an IPSec policy.

Precautions

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

Example

Create an IPSec proposal named **newprop1**.

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

Related Topics

12.6.172 transform
12.6.3 ah authentication-algorithm
12.6.57 esp authentication-algorithm
12.6.59 esp encryption-algorithm
12.6.54 encapsulation-mode
12.6.40 display ipsec proposal (All views)
12.6.129 proposal

12.6.110 ipsec proto-protect proposal

Function

The **ipsec proto-protect proposal** command creates a security proposal and displays the security proposal view.

The **undo ipsec proto-protect proposal** command deletes a security proposal.

By default, no security proposal is created.

Format

ipsec proto-protect proposal *proposal-name*

undo ipsec proto-protect proposal *proposal-name*

Parameters

Parameter	Description	Value
proposal-name	Specifies the name of a security proposal.	The value is a string of 1 to 15 case-insensitive characters.

 Copyright © Huawei Technologies Co., Ltd.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A security proposal defines the security protocol and authentication or encryption algorithm. Therefore, run the **ipsec proto-protect proposal** command to create a security proposal before configuring IPSec.

Follow-up Procedure

Configure the security protocol, authentication or encryption algorithm, and encapsulation mode.

Precautions

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

Configure a security proposal named **newprop1**.

```
<Huawei> system-view
[Huawei] ipsec proto-protect proposal newprop1
```

12.6.111 ipsec remote traffic-identical accept

Function

The **ipsec remote traffic-identical accept** command allows branch or other users to quickly access the headquarters network.

The **undo ipsec remote traffic-identical accept** command disables quick access to the headquarters network.

By default, the device allows branch or other users to quickly access the headquarters network after their IP addresses are changed.

Format

ipsec remote traffic-identical accept

undo ipsec remote traffic-identical accept

 Copyright © Huawei Technologies Co., Ltd.

Parameters

None.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After a branch and headquarters of a company establish an IPSec tunnel, the IP address of the branch gateway interface to which an IPSec policy group is applied changes due to the link status change or other reasons. For example, the branch gateway connects to the Internet through dialup and establishes an IPSec tunnel with the headquarters. As a result, the established IPSec tunnel between the headquarters and branch becomes unavailable. However, this IPSec tunnel still exists before timeout.

If quick access to the headquarters network is disabled, when a branch gateway initiates IPSec negotiation again, the headquarters retains the original IPSec tunnel before the tunnel expires. As a result, the data flows transmitted over the new negotiated IPSec tunnel are the same as those on the original IPSec tunnel, causing a conflict. In this case, the branch and headquarters cannot establish a new IPSec tunnel in a short period of time.

If quick access to the headquarters network is enabled, when a branch gateway initiates IPSec negotiation again, the headquarters deletes the original IPSec tunnel immediately so that the branch and headquarters can establish a new IPSec tunnel quickly.

Prerequisites

- The headquarters gateway functions as the responder and uses an IPSec policy template to establish an IPSec tunnel with the branch gateway.
- The ACL referenced by the IPSec policy does not change before and after the IPSec tunnel becomes unavailable.
- The interface that the branch uses to connect to the headquarters gateway does not change before and after the IPSec tunnel becomes unavailable.

Example

Allow the branch or other users to quickly access the headquarters network.

```
<Huawei> system-view
[Huawei] ipsec remote traffic-identical accept
```

 Copyright © Huawei Technologies Co., Ltd.

12.6.112 ipsec sa

Function

The **ipsec sa** command creates a Security Association (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.	It is a string of 1 to 15 case-insensitive characters, spaces not supported. The characters can be letters or numbers. 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**, **sa authentication-hex** or **sa encryption-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.

 Copyright © Huawei Technologies Co., Ltd.

Example

Create an SA.

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

12.6.113 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.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
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. During IPSec negotiation between a Huawei device and a Cisco device using IKEv1: • If the Huawei device functions as the initiator and the traffic hard lifetime is set to 0, the traffic hard lifetime value pushed by the Cisco device takes effect on the local end. • If the Huawei device functions as the responder and the traffic hard lifetime is set to 0, the value 0 takes effect on the local end.

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:

 Copyright © Huawei Technologies Co., Ltd.

- 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 12-64 lists the default soft lifetime values.

  Table 12-64 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

You only need to specify the SA lifetime for the SA setup through the IKE negotiation. That is, it is invalid to the SA manually set up. The manually set up SA is effective permanently.

The SA lifetime can be configured globally or based on an IPSec policy or profile. If no SA lifetime is configured for the IPSec policy or profile, the global lifetime is used. If both the global SA lifetime and lifetime based on the IPSec policy or profile are configured, the latter one takes effect.

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.

 Copyright © Huawei Technologies Co., Ltd.

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
```

Related Topics

12.6.158 sa duration (ISAKMP IPSec policy view, IPSec policy template view, IPSec profile view)

12.6.114 ipsec sm4 version

Function

The **ipsec sm4 version** command sets an SM4 algorithm version for IKE negotiation.

The **undo ipsec sm4 version** command restores the default SM4 algorithm version for IKE negotiation.

By default, the SM4 algorithm version **draft-standard** is used.

Format

ipsec sm4 version { **draft-standard** | **standard** }

undo ipsec sm4 version

Parameters

Parameter	Description	Value
draft-standard	Sets the SM4 algorithm version to that released in 2013. The attribute value of the SM4 algorithm is 127.	-
standard	Sets the SM4 algorithm version to that released in 2014. The attribute value of the SM4 algorithm is 129.	-

Views

IKE peer view

Default Level

2: Configuration level

Usage Guidelines

For IKE negotiation during interconnection with non-Huawei devices, if the SM4 algorithm versions used by devices of different vendors differ from each other, the

 Copyright © Huawei Technologies Co., Ltd.

IKE negotiation fails. In this case, run the **ipsec sm4 version** command to set the SM4 algorithm version consistent with that on non-Huawei devices.

Example

Set the SM4 algorithm version used for IKE negotiation to **standard**.

```
<Huawei> system-view
[Huawei] ike peer p1
[Huawei-ike-peer-p1] ipsec sm4 version standard
```

Related Topics

12.6.20 display ike peer (all views)

12.6.115 lifetime-notification-message enable

Function

The **lifetime-notification-message enable** command enables a device to send IKE SA lifetime notification messages.

The **undo lifetime-notification-message enable** command disables a device from sending IKE SA lifetime notification messages.

By default, the device does not send IKE SA lifetime notification messages.

Format

lifetime-notification-message enable

undo lifetime-notification-message enable

Parameters

None

Views

IKE peer view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can run the **12.6.157 sa duration (IKE proposal view)** command to configure an IKE SA lifetime in an IKE proposal. If the IKE SA lifetimes of two ends are different, the two ends use the smaller IKE SA lifetime for IKE negotiation.

- When a Huawei device (responder) wants to set up an IPSec tunnel with a Cisco systems VPN client (initiator) and the IKE SA lifetimes configured at two

 Copyright © Huawei Technologies Co., Ltd.

ends are different, you can run this command to enable the Huawei device to send IKE SA lifetime notification messages to the Cisco device to ensure successful IKE negotiation between them. If the Huawei device is disabled from sending IKE SA lifetime notification messages to the peer, the IKE negotiation fails.

- You can also run this command when two Huawei devices need to set up an IPSec tunnel. However, the configuration takes effect on the responder only. If you cannot determine which end is the initiator, you are advised to configure this command on devices at both ends.

Precautions

This command is supported by IKEv1 only.

Example

Enable the IKE peer named **peer1** to send IKE SA lifetime notification messages.

```
<Huawei> system-view
[Huawei] ike peer peer1
[Huawei-ike-peer-peer1] undo version 2
[Huawei-ike-peer-peer1] lifetime-notification-message enable
```

Related Topics

12.6.75 ike peer

12.6.157 sa duration (IKE proposal view)

12.6.116 local-address

Function

The **local-address** command assigns an IP address to the local end of IKE negotiation.

The **undo local-address** command cancels the configuration.

By default, the system selects an outbound interface according to a route and uses the IP address of the outbound interface as the local IP address.

Format

local-address *ip-address*

undo local-address

Parameters

Parameter	Description	Value
ip-address	Specifies the IP address of the local end of IKE negotiation.	The value is in dotted decimal notation.

 Copyright © Huawei Technologies Co., Ltd.

Views

IKE peer view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **local-address** command assigns an IP address to the local end of IKE negotiation.

When the local end and remote end establish an IPSec tunnel, the local IP address does not need to be configured during IKE negotiation. By default, the system selects an outbound interface according to a route and uses the IP address of the outbound interface as the local IP address.

- If the IP address of an interface bound to an IPSec policy is variable or unknown, run the **local-address** command to specify the IP address of another interface such as a loopback interface as the local IP address.
- If an interface bound to an IPSec policy is configured with one primary IP address and multiple secondary IP addresses, run the **local-address** command to specify one IP address as the local IP address.
- If the local and remote ends have equal-cost routes, run the **local-address** command to specify the local IP address so that IPSec packets can be sent out from the specified interface.

Precautions

The **local-address** at the local end must be the same as the **remote-address** at the remote end.

You do not need to specify **local-address** for an IKE peer referenced by an IPSec profile. During IKE negotiation, the IPSec profile uses the source addresses of the IPSec tunnel interface.

In a multi-link shared IPSec policy group scenario, the IP address of the local end cannot be the secondary IP address of a loopback interface. Otherwise, an IPSec tunnel cannot be established.

Example

Configure an IP address for the local end of IKE negotiation in the IKE peer view.

```
<Huawei> system-view
[Huawei] ike peer huawei
[Huawei-ike-peer-huawei] local-address 10.10.10.1
```

Related Topics

12.6.75 ike peer

12.6.20 display ike peer (all views)

 Copyright © Huawei Technologies Co., Ltd.

12.6.117 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 { **dn** | **fqdn** | **ip** [**ip-configurable**] | **key-id** | **user-fqdn** }

undo local-id-type

Parameters

Parameter	Description	Value
dn	Specifies the Distinguished Name (DN) as the local ID.	-
fqdn	Specifies the name as the local ID.	-
ip	Specifies the IP address as the local ID.	-
ip-configurable	Indicates that the IP address used as the local ID is configurable. This IP address can be configured using the **local-id** command. The IP address is the local IP address used for IKE negotiation by default. This parameter takes effect only in the IKE peer view.	-
key-id	Specifies the key-id as the local ID. This parameter takes effect only in the Efficient VPN policy view.	-
user-fqdn	Specifies the USER-FQDN as the local ID.	-

Views

IKE peer view, 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

 Copyright © Huawei Technologies Co., Ltd.

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.
- If IKEv1 is used, pre-shared key authentication requires the local ID on the local end to be the same as the remote ID on the remote end. If IKEv2 is used, pre-shared key authentication requires the local ID type or local ID on the local end to be the same as the remote ID type or remote ID on the remote end.
- For RSA signature authentication, the remote ID type or remote ID on the local end must be consistent with corresponding fields in the local certificate on the remote end.

Different authentication methods support different ID types, as shown in **Table 12-65**.

 Copyright © Huawei Technologies Co., Ltd.

Table 12-65 Relationship between local IKE ID types, local ID, and authentication methods

Authentication Method	IP	DN	FQDN	USER-FQDN	key-id
pre-share	Supported The ID is the local IP address used for IKE negotiation by default. Set an ID using the **local-id** command, indicating that the IKE peer uses this ID for identity authentication.	Not supported	Supported Set an ID using the **local-id** command, indicating that the IKE peer uses this ID for identity authentication. The ID specified by the **ike local-name** command, indicating that all peers on the device use this ID for identity authentication. The ID specified by the **local-id** command has a higher priority than the one specified by the **ike local-name** command.	Supported Set an ID using the **local-id** command, indicating that the IKE peer uses this ID for identity authentication. Set an ID using the **ike local-name** command, indicating that all peers on the device use this ID for identity authentication. The ID specified by the **local-id** command has a higher priority than the one specified by the **ike local-name** command.	Supported This parameter is often used when the device using the Efficient VPN policy functions as a remote end to communicate with Cisco devices.

Copyright © Huawei Technologies Co., Ltd.

Authentication Method	IP	DN	FQDN	USER-FQDN	key-id
rsa-signature	Supported The ID is the local IP address used for IKE negotiation by default. Set an ID using the **local-id** command, indicating that the IKE peer uses this ID for identity authentication.	Supported Use the default ID in the certificate. No configuration is required.	Supported Use the default ID in the certificate. No configuration is required.	Supported Use the default ID in the certificate. No configuration is required.	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 IKE peer **peer1** to FQDN.

```
<Huawei> system-view
[Huawei] ike peer peer1
[Huawei-ike-peer-peer1] local-id-type fqdn
```

Related Topics

12.6.20 display ike peer (all views)

12.6.30 display ipsec efficient-vpn

12.6.118 local-id

Function

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

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

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

Format

local-id *id*

undo local-id

Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
id	Specifies the local ID used in IKE negotiation	The value is a string of 1 to 255 case-sensitive characters.

Views

IKE peer view

Default Level

2: Configuration level

Usage Guidelines

If the ID type of the IKE peer is **IP**, **FQDN**, or **USER-FQDN**, you can configure the local end identity in the system view or IKE peer view.

The **local-id** command sets an ID, indicating that the IKE peer uses this ID for authentication. If the ID type is FQDN or User-FQDN, the **12.6.71 ike local-name** command sets an ID, indicating that all peers on the device use this ID for authentication. The ID specified by the **local-id** command has a higher priority than the one specified by the **12.6.71 ike local-name** command.

Example

Set the local ID to be **huawei** in IKE negotiation.

```
<Huawei> system-view
[Huawei] ike peer peer1
[Huawei-ike-peer-peer1] local-id huawei
```

Related Topics

12.6.117 local-id-type

12.6.71 ike local-name

12.6.119 local-id-preference certificate enable

Function

The **local-id-preference certificate enable** command enables the device to preferentially obtain the local ID from a field in a certificate when IKE uses certificate negotiation.

The **undo local-id-preference certificate enable** command disables the device from preferentially obtaining the local ID from a field in a certificate when IKE uses certificate negotiation.

By default, the device does not preferentially obtain the local ID from a field in a certificate when IKE uses certificate negotiation.

 Copyright © Huawei Technologies Co., Ltd.

Format

local-id-preference certificate enable

undo local-id-preference certificate enable

Parameters

None

Views

IKE peer view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When IKE uses certificate negotiation, the device can obtain its local ID from a field (IP address, FQDN, or email address) in the certificate, removing the need to configure the local ID.

After the **local-id-preference certificate enable** command is configured, the device preferentially obtains its local ID from a field in the certificate. If this method fails, it obtains its local ID based on the local configuration. If this method also fails, IKE negotiation fails.

Precautions

Before V500R005C00, the **local-id-preference certificate enable** command is supported only after a required patch is installed. By default, this command is disabled. In V500R005C00, this command is supported by default but is not displayed in the IKE peer view. In versions earlier than V5R5C20SPC500, this command is supported and displayed by default.

This command is not supported when the certificate negotiation mode is set to digital envelope authentication using the **authentication-method** command.

In IKEv2 negotiation scenarios, when both the **local-id-preference certificate enable** and **12.6.120 local-id-reflect enable** commands are configured, the **12.6.120 local-id-reflect enable** command takes effect.

You can run the **19.17.28 display pki certificate** command to view certificate identity information. The email address in the certificate corresponds to User-FQDN.

Example

Enable the device to preferentially obtain the local ID from a field in a certificate when IKE uses certificate negotiation.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei&gt; system-view
[Huawei] ike peer peer1
[Huawei-ike-peer-peer1] local-id-preference certificate enable
```

Related Topics

12.6.20 display ike peer (all views)

12.6.118 local-id

12.6.120 local-id-reflect enable

Function

The **local-id-reflect enable** command enables the function of using the local ID of the responder as the remote ID carried in the IKE packets sent by the initiator during IKEv2 negotiation.

The **undo local-id-reflect enable** command disables the function of using the local ID of the responder as the remote ID carried in the IKE packets sent by the initiator during IKEv2 negotiation.

By default, during IKEv2 negotiation, the local ID of the responder is not used as the remote ID carried in the IKE packets sent by the initiator.

Format

local-id-reflect enable

undo local-id-reflect enable

Parameters

None

Views

IKE peer view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

During IKEv2 negotiation, if the user does not know the remote ID configured for the initiator, run the **local-id-reflect enable** command on the responder. When the responder receives an IKE packet from the initiator, the responder uses the IDr payload (remote ID) in the received packet as its local ID. If the responder does not obtain the IDr payload, it obtains its local ID based on the local configuration.

Precautions

This command is not supported when IKEv2 uses a digital envelope for authentication during certificate negotiation.

 Copyright © Huawei Technologies Co., Ltd.

When both the **local-id-reflect enable** and **12.6.119 local-id-preference certificate enable** commands are configured, the **local-id-reflect enable** command takes effect.

Currently, the ID type can only be IP address, FQDN, or User-FQDN.

Example

Enable the function of using the local ID of the responder as the remote ID carried in the IKE packets sent by the initiator during IKEv2 negotiation.

```
<Huawei> system-view
[Huawei] ike peer peer1
[Huawei-ike-peer-peer1] local-id-reflect enable
```

Related Topics

12.6.20 display ike peer (all views)

12.6.118 local-id

12.6.136 remote-id

12.6.121 match ike-identity

Function

The **match ike-identity** command references an identity filter set.

The **undo match ike-identity** command removes the referenced identity filter set.

By default, no identity filter set is referenced.

Format

match ike-identity *identity-name*

undo match ike-identity

Parameters

Parameter	Description	Value
identity-name	Specifies the name of the identity filter set.	The value is an existing identity filter name.

Views

IPSec policy template view, IPSec profile view

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

Usage Scenario

1. During IKE negotiation, a device specifies the peer based on the identity filter set referenced in the policy template or IPSec profile.

   When the device functions as a responder, it can specify the peer allowed to connect to it to improve security.

2. In an IPSec over DSVPN application, multiple mGRE tunnel interfaces are configured on the hub which provides only one IP address for spoke access. The mGRE tunnel interfaces use the same source address or source interface; therefore, the hub cannot identify IKE packets from different mGRE tunnel interfaces. To solve this problem, set parameters in the identity filter set to specify the mGRE tunnel interface of each IKE packet.

   For details about DSVPN, see DSVPN Configuration.

Prerequisites

An identity filter set with a specific *identity-name* has been created using the **12.6.70 ike identity** command.

Precautions

- If you configure multiple IPSec policy templates and apply them to multiple interfaces on the same device, the parameters in the identity filter set referenced in different policy templates cannot be the same.
- If you configure multiple IPSec profiles and apply them to multiple tunnel interfaces on the same device, the parameters in the identity filter set referenced in different IPSec profiles cannot be the same.

If a remote device matches one parameter or more parameters in different identity filter sets in the local device, the access request of the remote device will be denied.

Example

Reference an identity filter set in the IPSec profile view.

```
<Huawei> system-view
[Huawei] ike identity identity1
[Huawei-ike-identity-identity1] fqdn peer1
[Huawei-ike-identity-identity1] quit
[Huawei] ipsec profile profile1
[Huawei-ipsec-profile-profile1] match ike-identity identity1
```

Related Topics

12.6.70 ike identity

12.6.106 ipsec policy-template

12.6.108 ipsec profile (system view)

12.6.122 nat traversal

 Copyright © Huawei Technologies Co., Ltd.

Function

The **nat traversal** command enables NAT traversal.

The **undo nat traversal** command disables NAT traversal.

By default, the NAT traversal is enabled.

Format

nat traversal

undo nat traversal

Parameters

None

Views

IKE peer view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In practice, if the initiator is located on a private network and the responder is located on the public network side. To ensure that an IPSec tunnel can be set up when the NAT device exists, NAT traversal needs to be configured.

NAT traversal allows ESP packets to pass through the NAT gateway during IKE negotiation.

Precautions

If NAT traversal is enabled, the IPSec proposal (**ipsec proposal**) supports only ESP.

Example

Enable NAT traversal in IKE peer named **peer1**.

```
<Huawei> system-view
[Huawei] ike peer peer1
[Huawei-ike-peer-peer1] nat traversal
```

Related Topics

12.6.75 ike peer

12.6.20 display ike peer (all views)

12.6.123 pfs

 Copyright © Huawei Technologies Co., Ltd.

Function

The **pfs** command enables Perfect Forward Secrecy (PFS) when the local end initiates negotiation.

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

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

Format

pfs { **dh-group1** | **dh-group2** | **dh-group5** | **dh-group14** | **dh-group19** | **dh-group20** | **dh-group21** }

undo pfs

Parameters

Parameter	Description	Value
dh-group1	Uses the 768-bit DH group.	-
dh-group2	Uses the 1024-bit DH group.	-
dh-group5	Uses the 1536-bit DH group.	-
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

ISAKMP IPSec policy view, IPSec policy template view, IPSec profile view, 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 **dh-group1**, **dh-group2**, and **dh-group5** have potential security risks. The other DH groups are recommended.

Table 12-66 describes the requirement for consistency of the PFS DH groups configured on the local and remote ends when the PFS function is enabled.

 Copyright © Huawei Technologies Co., Ltd.

Table 12-66 Description of PFS DH groups

Security Policy Mode on the Local and Remote Ends	Description
IPSec policy in ISAKMP mode on both ends	The DH groups specified on the two ends must be the same; otherwise, the IPSec SA negotiation fails.
IPSec policy in ISAKMP mode on one end and IPSec policy configured using an IPSec policy template on the other end	• If PFS is enabled in the IPSec policy template: The DH groups specified on the two ends must be the same; otherwise, the IPSec SA negotiation fails. • If PFS is disabled in the IPSec policy template: The IPSec SA negotiation may succeed when the DH groups specified on the two ends are different. The responder uses the DH group on the initiator.
IPSec profile on both ends	The DH groups specified on the two ends must be the same; otherwise, the IPSec SA negotiation fails.

Example

Use PFS when the IPSec policy named **policy1** is used in negotiation.

```
<Huawei> system-view
[Huawei] ipsec policy policy1 1 isakmp
[Huawei-ipsec-policy-isakmp-policy1-1] pfs dh-group14
```

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
```

Related Topics

12.6.105 ipsec policy (system view)

12.6.98 ipsec efficient-vpn (system view)

12.6.30 display ipsec efficient-vpn

12.6.34 display ipsec policy (all views)

12.6.124 pki realm

Function

The **pki realm** command binds a public key infrastructure (PKI) realm to an IKE peer or an Efficient VPN policy.

 Copyright © Huawei Technologies Co., Ltd.

The **undo pki realm** command unbinds a PKI realm from an IKE peer or an Efficient VPN policy.

By default, no PKI realm is bound to an IKE peer or an Efficient VPN policy.

Format

pki realm *realm-name*

undo pki realm

Parameters

Parameter	Description	Value
realm-name	Specifies the name of a PKI realm.	The PKI realm must already exist.

Views

IKE peer view, Efficient VPN policy view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A PKI realm is a set of identity information required when a PKI entity enrolls a certificate.

After a PKI realm is bound to an IKE peer or an Efficient VPN policy, the IKE peer can obtain the CA certificate and local certificate based on the PKI realm configuration.

Prerequisites

A PKI realm has been created using the **pki realm** command in the system view. And the CA certificate and local certificate have been imported in the PKI realm.

Example

Bind the PKI realm **test** to the IKE peer.

```
<Huawei> system-view
[Huawei] pki realm test
[Huawei-pki-realm-test] quit
[Huawei] ike peer huawei
[Huawei-ike-peer-huawei] pki realm test
```

Bind the PKI realm **test1** to the Efficient VPN policy.

```
<Huawei> system-view
[Huawei] pki realm test1
[Huawei-pki-realm-test1] quit
```

 Copyright © Huawei Technologies Co., Ltd.

```
[Huawei] ipsec efficient-vpn evpn mode client
[Huawei-ipsec-efficient-vpn-evpn] pki realm test1
```

Related Topics

12.6.75 ike peer

12.6.98 ipsec efficient-vpn (system view)

12.6.125 policy enable

Function

The **policy enable** command enables a policy in an IPSec policy group.

The **undo policy enable** command disables a policy in an IPSec policy group.

By default, all the policies in an IPSec policy group are enabled.

Format

policy enable

undo policy enable

Parameters

None

Views

ISAKMP IPSec policy view, IPSec policy template view

Default Level

2: Configuration level

Usage Guidelines

After you disable a policy, the policy is not used for tunnel establishment.

Example

Disable policy 1 in the IPSec policy group.

```
<Huawei> system-view
[Huawei] ipsec policy map1 1 isakmp
[Huawei-ipsec-policy-isakmp-map1-1] undo policy enable
```

Related Topics

12.6.105 ipsec policy (system view)

12.6.126 pre-shared-key (IKE peer view, Efficient VPN policy view)

 Copyright © Huawei Technologies Co., Ltd.

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 { **simple** | **cipher** } *key*

undo pre-shared-key

Parameters

Parameter	Description	Value
simple	Indicates the pre-shared key in plain text. The pre-shared key is displayed in plain text in the configuration file. **NOTICE** If **simple** is selected, the password is saved in the configuration file in plain text. This brings security risks. It is recommended that you select **cipher** to save the password in cipher text.	-
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.	-

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
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 contains at least 3 types of lowercase letters, uppercase letters, digits, and special characters, and contains at least 6 characters.

Views

IKE peer view, 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.

Prerequisites

Pre-shared key authentication has been specified in an IKE proposal or in an Efficient VPN policy.

Precautions

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

 Copyright © Huawei Technologies Co., Ltd.

Example

Configure the pre-shared key used by IKE peers to perform pre-shared key authentication as **Test!123**.

```
<Huawei> system-view
[Huawei] ike peer peer1
[Huawei-ike-peer-peer1] pre-shared-key cipher Test!123
```

Configure pre-shared key authentication in the Efficient VPN policy **evpn** and set the pre-shared key to **huawei@123** in cipher text.

```
<Huawei> system-view
[Huawei] ipsec efficient-vpn evpn mode client
[Huawei-ipsec-efficient-vpn-evpn] authentication-method pre-share
[Huawei-ipsec-efficient-vpn-evpn] pre-shared-key cipher huawei@123
```

Related Topics

12.6.75 ike peer

12.6.98 ipsec efficient-vpn (system view)

12.6.20 display ike peer (all views)

12.6.30 display ipsec efficient-vpn

12.6.127 pre-shared-key (IKE user view)

Function

The **pre-shared-key** command configures the pre-shared key used by IKE users when IKE peers use pre-shared key authentication during IKE negotiation.

The **undo pre-shared-key** command cancels the configuration.

By default, the pre-shared key used by IKE peers is not configured when IKE peers use pre-shared key authentication during IKE negotiation.

Format

pre-shared-key *key*

undo pre-shared-key

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
key	Specifies the pre-shared key used by IKE users when IKE peers use pre-shared key authentication during IKE negotiation.	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 quoted by double quotation marks (" "), the character string can contain spaces. **NOTE** For security purposes, it is recommended that the pre-shared key contains at least 3 types of lowercase letters, uppercase letters, digits, and special characters, and contains at least 6 characters.

Views

IKE user view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In a point-to-multipoint scenario, the device functions as the VPN gateway of the headquarters, an IPSec policy is created using an IPSec policy template, and the VPN gateway receives IPSec connection setup requests of different branches. When the pre-shared key is used for identity authentication and all branches use the same ID and pre-shared key, there are security risks. That is, if the ID and pre-shared key of one branch leak, the ID and pre-shared key of all branches leak. To prevent this problem, you are advised to run the **id-type** and **pre-shared-key** commands in the view of the IKE user in the IKE user table.

An IKE user table records the mapping between remote IDs of IKE peers and pre-shared keys. After an IKE peer references an IKE user table, the device searches for the pre-shared key matching the remote ID of the IKE peer in the IKE user table to complete identity authentication during IKE negotiation. In this manner, branches use different IDs and pre-shared keys.

Precautions

 Copyright © Huawei Technologies Co., Ltd.

- After an IKE peer references an IKE user table, the pre-shared key configured by this command takes precedence over the pre-shared key configured by the **12.6.126 pre-shared-key (IKE peer view, Efficient VPN policy view)** command.
- Pre-shared key authentication has been specified in an IKE proposal when IKE peers are configured.
- Both ends of IKE negotiation must use the same pre-shared key.

Example

Configure the pre-shared key as **Test!123** for IKE users.

```
<Huawei> system-view
[Huawei] ike user-table 10
[Huawei-ike-user-table-10] user user1
[Huawei-ike-user-table-10-user1] pre-shared-key Test!123
```

Related Topics

12.6.126 pre-shared-key (IKE peer view, Efficient VPN policy view)

12.6.63 id-type

12.6.27 display ike user-table (all views)

12.6.128 prf

Function

The **prf** command configures the pseudo-random function (PRF) algorithm used in IKEv2 negotiation.

The **undo prf** command restores the default configuration.

By default, the HMAC-SHA2-256 PRF algorithm is used in IKEv2 negotiation.

Format

prf { **aes-xcbc-128** | **hmac-md5** | **hmac-sha1** | **hmac-sha2-256** | **hmac-sha2-384** | **hmac-sha2-512** }

undo prf

Parameters

Parameter	Description	Value
aes-xcbc-128	Indicates that the PRF algorithm is AES-XCBC-128. This algorithm applies only to IKEv2 negotiation.	-
hmac-md5	Indicates that the PRF algorithm is HMAC-MD5.	-
hmac-sha1	Indicates that the PRF algorithm is HMAC-SHA1.	-
hmac-sha2-256	Indicates that the PRF algorithm is HMAC-SHA2-256.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
hmac-sha2-384	Indicates that the PRF algorithm is HMAC-SHA2-384.	-
hmac-sha2-512	Indicates that the PRF algorithm is HMAC-SHA2-512.	-

Views

IKE proposal view

Default Level

2: Configuration level

Usage Guidelines

The PRF algorithm is required in IKEv2 negotiation. The PRFs are listed as follows from the highest security level to the lowest security level: **hmac-sha2-512** > **hmac-sha2-384** > **hmac-sha2-256** > **aes-xcbc-128** > **hmac-sha1** > **hmac-md5**.

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

NOTE

hmac-md5 and **hmac-sha1** are not recommended due to their low security.

Example

Set hmac-sha2-256 as the PRF algorithm for IKEv2 proposal 10.

```
<Huawei> system-view
[Huawei] ike proposal 10
[Huawei-ike-proposal-10] prf hmac-sha2-256
```

Related Topics

12.6.76 ike proposal

12.6.129 proposal

Function

The **proposal** command references an IPSec proposal.

The **undo proposal** command deletes the referenced IPSec proposal.

By default, no IPSec proposal is referenced.

Format

Manual IPSec policy view:

proposal *proposal-name*

undo proposal

 Copyright © Huawei Technologies Co., Ltd.

ISAKMP IPSec policy view, IPSec policy template view, and IPSec profile view:

proposal *proposal-name*

undo proposal [*proposal-name*]

Parameters

Parameter	Description	Value
proposal-name	Specifies the name of the proposals.	It is a string of 1 to 15 case-insensitive characters.

Views

Manual IPSec policy view, ISAKMP IPSec policy view, IPSec policy template view, IPSec profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

An IPSec proposal defines IPSec protection methods and takes effect only after an IPSec policy or profile references the IPSec proposal.

Prerequisites

An IPSec proposal has been created using the **ipsec proposal** command.

Precautions

A manual IPSec policy can only reference one IPSec proposal.

An ISAKMP IPSec policy, an IPSec policy template, or IPSec profile can reference a maximum of 12 IPSec proposals. When devices at both ends of an IPSec tunnel perform IKE negotiation, they search for IPSec proposals in sequence where IPSec proposals were configured until a matching IPSec proposal is found. If no matching IPSec proposal is found, an SA cannot be set up and packets to be protected are discarded.

Example

Set a proposal named **prop1**, and apply this proposal to the IPSec policy in manual mode named **policy1**.

```
<Huawei> system-view
[Huawei] ipsec proposal prop1
[Huawei-ipsec-proposal-prop1] quit
[Huawei] ipsec policy policy1 1 manual
[Huawei-ipsec-policy-manual-policy1-1] proposal prop1
```

Related Topics

12.6.109 ipsec proposal

 Copyright © Huawei Technologies Co., Ltd.

12.6.105 ipsec policy (system view)
12.6.106 ipsec policy-template
12.6.108 ipsec profile (system view)

12.6.130 proposal (SA view)

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 a security proposal.	The value is a string of 1 to 15 case-insensitive characters.

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 proto-protect proposal** *proposal-name* 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.

Configuration Impact

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

 Copyright © Huawei Technologies Co., Ltd.

Example

Apply the security proposal named **prop1** to the SA named **sa1**.

```
<Huawei> system-view
[Huawei] ipsec proto-protect proposal prop1
[Huawei-ipsec-proto-protect-proposal-prop1] transform ah
[Huawei-ipsec-proto-protect-proposal-prop1] quit
[Huawei] ipsec sa sa1
[Huawei-ipsec-sa-sa1] proposal prop1
```

12.6.131 qos group

Function

The **qos group** command configures the QoS group to which the IPSec packets belong.

The **undo qos group** command deletes the QoS group to which the IPSec packets belong.

By default, no QoS group is configured.

Format

qos group *qos-group-value*

undo qos group

Parameters

Parameter	Description	Value
qos-group-value	Specifies the ID of the QoS group.	The value is an integer that ranges from 1 to 99.

Views

Manual IPSec policy view, IPSec policy view, IPSec policy template view, IPSec profile view, Efficient VPN policy view, GDOI policy view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When both an IPSec policy and a QoS policy are used on an interface, you can run this command to specify the QoS group to which the IPSec packets belong to facilitate QoS management.

Precautions

 Copyright © Huawei Technologies Co., Ltd.

This command takes effect in the packet encapsulation process but not the packet decapsulation process. That is, the command takes effect only for incoming packets.

Follow-up Procedure

After QoS for IPSec packets is enabled, run the **if-match qos-group** *qos-group-value* command in the traffic classifier view to configure a matching rule based on the QoS group.

Example

Configure the QoS group to which the IPSec packets belong in the IPSec policy view.

```
<Huawei> system-view
[Huawei] ipsec policy policy1 10 isakmp
[Huawei-ipsec-policy-isakmp-policy1-10] qos group 30
```

Related Topics

12.6.104 ipsec policy (interface view)
12.6.106 ipsec policy-template
12.6.107 ipsec profile (interface view)
12.6.98 ipsec efficient-vpn (system view)

12.6.132 qos pre-classify

Function

The **qos pre-classify** command enables pre-extraction of original IP packets.

The **undo qos pre-classify** command disables pre-extraction of original IP packets.

By default, pre-extraction of original IP packets is disabled.

Format

qos pre-classify

undo qos pre-classify

Parameters

None

Views

Tunnel interface view, Efficient VPN policy view, Manual IPSec policy view, IPSec policy view, IPSec policy template view, IPSec profile view, GDOI policy view, BD view, VBDIF interface view, VPN instance view, Virtual template interface view

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

Usage Scenario

In tunnel mode, QoS parameters such as the packet header and protocol type in original packets are hidden after IP packets are encapsulated through GRE, VXLAN, L2TP, and IPSec. Although GRE, VXLAN, L2TP, and IPSec uses the DSCP field in original packets as the DSCP field in the IP packet header, some QoS solutions require quintuple information. The encryption device can pre-extract quintuple information including the source address, destination address, protocol type, source port number, and destination port number to facilitate refined QoS management on GRE, VXLAN, L2TP, and IPSec packets.

In an A2A VPN solution, the device uses the IP header of original packets as the IP header for encapsulated A2A VPN packets. Therefore, you do not need to configure this command if the device classifies packets based on the source address, destination address, or protocol type only.

Follow-up Procedure

After pre-extraction of original IP packets is enabled, run the **if-match acl** { *acl-number* | *acl-name* } command in the traffic classifier view to configure a matching rule based on the ACL.

Example

Enable pre-extraction of original IP packets in the IPSec policy view.

```
<Huawei> system-view
[Huawei] ipsec policy policy1 10 isakmp
[Huawei-ipsec-policy-isakmp-policy1-10] qos pre-classify
```

Related Topics

12.6.104 ipsec policy (interface view)

12.6.106 ipsec policy-template

12.6.107 ipsec profile (interface view)

12.6.98 ipsec efficient-vpn (system view)

12.6.133 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

 Copyright © Huawei Technologies Co., Ltd.

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

IKE peer view, 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 of an IKE peer to 400 seconds.

```
<Huawei> system-view
[Huawei] ike peer peer1
[Huawei-ike-peer-peer1] re-authentication interval 400
```

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
```

12.6.134 remote-address (IKE peer 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 cancels the configuration.

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

 Copyright © Huawei Technologies Co., Ltd.

Format

remote-address { [**vpn-instance** *vpn-instance-name*] { *ipv4-address* | **host-name** *host-name* } [**track** { **nqa** *admin-name test-name* | **bfd-session** *session-name* } { **up** | **down** }] | **authentication-address** *start-ipv4-address* [*end-ipv4-address*] }

undo remote-address [*ipv4-address* | **host-name** *host-name* | **authentication-address**]

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Specifies the name of a VPN instance.	The value must be an existing VPN instance name. IPv4 multi-instance is supported.
ipv4-address	Specifies the IP address of the remote IKE peer.	The value is an IPv4 address 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.
track	Specifies association between IKE and NQA or BFD.	-
nqa *admin-name test-name*	Configures association between IKE negotiation and NQA so that the device can determine whether the remote address of the peer is valid according to the NQA test instance status. *admin-name* specifies the administrator name of an NQA test instance, and *test-name* specifies the name of an NQA test instance.	The administrator name or name of an NQA test instance must have been created.
bfd-session *session-name*	Specifies association between IKE and BFD so that the peer address depends on the BFD session status. *bfd-session-name* specifies the name of the BFD session.	The BFD session name must have been created.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
up	Indicates that the local address is used as the peer address for negotiation when the NQA test instance or BFD session status is Up.	-
down	Indicates that the local address is used as the peer address for negotiation when the NQA test instance or BFD session status is Down.	-
authentication-address *start-ipv4-address* [*end-ipv4-address*]	Specifies the IP address before NAT as the authentication address. • *start-ipv4-address*: Specifies the start IP address of the remote end. • *end-ipv4-address*: Specifies the end IP address of the remote end.	The value is an IPv4 address in dotted decimal notation.

Views

IKE peer view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The remote address negotiated by the IKE peers has two types: IP address and domain name.

When the configured remote address is an IP address and the remote gateway IP address is fixed, set **remote-address** to a fixed IP address. When an IPSec policy template is used and the remote gateway address is not fixed, set **remote-address** to an IP address segment.

When a domain name is configured as the remote address, the device obtains the remote address in either of the following modes:

 Copyright © Huawei Technologies Co., Ltd.

- Static mode: The device obtains the remote address based on the manually configured mapping between the domain name and IP address.
- Dynamic mode: The device obtains the remote address from the DNS server.

To improve network reliability, the headquarters provides four devices for branch gateways to access. In an IPSec policy, two remote IP addresses or domain names of the IKE peer can be configured on the branch gateway. The branch gateway attempts to use the first IP address or domain name to establish an IKE connection with the headquarters gateway. If the connection fails, the branch gateway uses the second IP address or domain name to establish an IKE connection, and so on.

If the IP address of the first IKE peer is unreachable in the scenario that two IP addresses are configured, the branch gateway uses the second IP address to establish an IKE connection only when establishing an IKE connection fails or the dead peer detection (DPD) fails. It takes a long time. To reduce the time required and determine validity of the IKE peer address in real time, configuring association between IKE negotiation and NQA or BFD to detect the link status and check validity of the IKE peer address based on the detection result.

In NAT traversal scenarios, when two ends use IKEv2, you can run the **remote-address authentication-address** *start-ipv4-address* [*end-ipv4-address*] command to specify the pre-NAT IP address or IP address segment as the authentication address if IP addresses need to be verified.

Prerequisites

- The VPN instance has been created using the **ip vpn-instance** command and the route distinguisher (RD) has been configured for the VPN instance using the **route-distinguisher** command if **vpn-instance** *vpn-instance-name* is specified.
- An NQA test instance has been created using the **nqa** command and the NQA test instance type has been set to ICMP using the **test-type** command if **nqa** *admin-name test-name* is specified.
- A BFD session has been created using the **bfd bind peer-ip** command and the BFD session has been set the local and remote discriminators using the **discriminator** command if **bfd-session** *bfd-session-name* is specified.

Precautions

- When an IPSec policy is used, if the local device functions as the initiator, run the **remote-address** command so that the initiator can use this address to search for the responder. Because both ends may be the initiator, run the **remote-address** command at both ends. The **remote-address** command is not required when the IKE peer functions as the responder and uses an IPSec policy template to establish an IPSec policy.
- You do not need to specify the **12.6.174 tunnel local** (local address) for the IKE peer referenced in an IPSec profile, because the local address is the source address of the GRE, mGRE or IPSec virtual tunnel interface. For the IKE peer referenced in an IPSec profile, **12.6.174 tunnel local** does not take effect.
- When applying an IPSec policy to a tunnel interface and running the **12.3.18 source** command to specify an IP address for the interface, you must run the **12.6.174 tunnel local** command to configure a tunnel local address. Otherwise, IKE negotiation will fail.

 Copyright © Huawei Technologies Co., Ltd.

- When an IPSec profile is used, the destination address of the IPSec tunnel interface configured using the **destination** command is preferentially used as the remote address for IKE negotiation. When the **remote-address** and **destination** commands are configured at the same time, ensure that the configured IP addresses are the same; otherwise, IKE negotiation will fail. To implement IKE peer redundancy, do not configure the **destination** command on the IPSec tunnel interface. Instead, configure the **remote-address** command on the IKE peer referenced by the IPSec profile.
- The remote IP address (**remote-address**) at the local end must be the same as the local IP address (**local-address**) at the remote end.
- The VPN instance specified by *vpn-instance-name* must be the same as the VPN instance that is configured by the **ip binding vpn-instance** command and bound to the physical interface negotiating IPSec tunnel setup.
- If more than one remote IP address or domain name is configured, the specified *vpn-instance-name* must be the same.
- If multiple remote IP addresses are configured, the device with redundant addresses must function as the IKE negotiation initiator.

Example

Set the remote IP address of IKE peer **peer1** to 10.1.1.1.

```
<Huawei> system-view
[Huawei] ike peer peer1
[Huawei-ike-peer-peer1] remote-address 10.1.1.1
```

Configure association between the IKE peer **huawei** with NQA and specify IP address 10.1.1.1 as the peer address for IKE negotiation when the NQA test instance (administrator name **admin** and instance name **test**) status is Up.

```
<Huawei> system-view
[Huawei] nqa test-instance admin test
[Huawei-nqa-admin-test] test-type icmp
[Huawei-nqa-admin-test] destination-address ipv4 10.1.1.1
[Huawei-nqa-admin-test] quit
[Huawei] ike peer huawei
[Huawei-ike-peer-huawei] remote-address 10.1.1.1 track nqa admin test up
```

Configure association between the IKE peer **huawei** and BFD and use the IP address 10.1.1.2 as the peer address for IKE negotiation when the status of the BFD session **test** is Up.

```
<Huawei> system-view
[Huawei] interface gigabitethernet 0/0/1
[Huawei-GigabitEthernet0/0/1] ip address 10.1.1.1 255.255.255.0
[Huawei-GigabitEthernet0/0/1] quit
[Huawei] bfd
[Huawei-bfd] quit
[Huawei] bfd test bind peer-ip 10.1.1.2 interface gigabitethernet 0/0/1
[Huawei-bfd-session-test] discriminator local 10
[Huawei-bfd-session-test] discriminator remote 20
[Huawei-bfd-session-test] commit
[Huawei-bfd-session-test] quit
[Huawei] ike peer huawei
[Huawei-ike-peer-huawei] remote-address 10.1.1.2 track bfd-session test up
```

Related Topics

12.6.75 ike peer
21.7.56 nqa

 Copyright © Huawei Technologies Co., Ltd.

21.7.95 test-type
18.5.3 bfd bind peer-ip
18.5.18 discriminator
12.6.171 switch-back enable

12.6.135 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*]

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

 Copyright © Huawei Technologies Co., Ltd.

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 v1
[Huawei-ipsec-efficient-vpn-evpn] remote-address 10.1.2.1 v1
```

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 v1
```

Related Topics

12.6.98 ipsec efficient-vpn (system view)

12.6.30 display ipsec efficient-vpn

12.6.136 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.

 Copyright © Huawei Technologies Co., Ltd.

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

IKE peer view, Efficient VPN policy view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If the remote ID type of the IKE peer is IP, 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-type** and **remote-id** commands to configure the remote ID type and 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 ID of the peer is the same as this remote ID.

Example

Set the remote ID of IKE peer **peer1** when pre-shared key authentication is used and the remote ID type is FQDN or USER-FQDN.

```
# Set the remote end of the tunnel.
<Huawei_A> system-view
[Huawei_A] ike local-name device_A
# Set the local end of the tunnel.
<Huawei_B> system-view
[Huawei_B] ike peer peer1
[Huawei_B-ike-peer-peer1] remote-id device_A
```

 Copyright © Huawei Technologies Co., Ltd.

Set the remote ID of IKE peer **peer1** when digital signature authentication is used.

- If the remote ID type is **DN**, set the remote ID as follows:

  ```
  <Huawei> system-view
  [Huawei] ike peer peer1
  [Huawei-ike-peer-peer1] remote-id /C=CN/ST=beijing
  ```

  If **remote-id** is set to the **subject** field in the certificate entity, the format is as follows: "/"+"subject". Note that spaces in the **subject** field are omitted and the comma is replaced by slash (/). For example, if the **subject** field is C=CN, ST=beijing, the command is **remote-id /C=CN/ST=beijing**.

- If the remote ID type is **FQDN**, set the remote ID as follows:

  ```
  <Huawei> system-view
  [Huawei] ike peer peer1
  [Huawei-ike-peer-peer1] remote-id www.hw.com
  ```

- If the remote ID type is **USER-FQDN**, set the remote ID as follows:

  ```
  <Huawei> system-view
  [Huawei] ike peer peer1
  [Huawei-ike-peer-peer1] remote-id user@hw.com
  ```

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
```

Related Topics

12.6.20 display ike peer (all views)

12.6.30 display ipsec efficient-vpn

12.6.137 remote-id-type

Function

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

The **undo remote-id-type** command cancels the remote ID type.

By default, no remote ID type is configured.

Format

remote-id-type { **any** | **dn** | **fqdn** | **ip** | **user-fqdn** | **none** }

undo remote-id-type

Parameters

Parameter	Description	Value
any	Specifies that the remote ID can be of any type.	-
dn	Specifies the distinguished name (DN) as the remote ID.	-
fqdn	Specifies the host name of the remote end as the remote ID.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
ip	Specifies the IP address of the remote end as the remote ID.	-
user-fqdn	Specifies the user domain name of the remote end as the remote ID.	-
none	Specifies the remote ID type of an IKE peer as none. After this parameter is specified, the remote ID type and remote ID are not checked during IKE negotiation.	-

Views

IKE peer view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Identity authentication is a protection mechanism for IKE negotiation. This mechanism ensures device security by confirming identities of communication parties. IKE peers can use different types of IDs. This command configures the remote ID type 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.
- If IKEv1 is used, pre-shared key authentication requires the local ID on the local end to be the same as the remote ID on the remote end. If IKEv2 is used, pre-shared key authentication requires the local ID type or local ID on the local end to be the same as the remote ID type or remote ID on the remote end.
- For RSA signature authentication, the remote ID type or remote ID on the local end must be consistent with corresponding fields in the local certificate on the remote end.

Support for remote ID types and their configuration methods differ depending on the authentication modes. **Table 12-67** describes the details.

Copyright © Huawei Technologies Co., Ltd.

Table 12-67 Relationships among the remote ID type, remote ID, and authentication mode

Authentication Mode	IP	DN	FQDN	USER-FQDN
Pre-shared key authentication (**pre-share**)	Supported To set a remote ID, run the **12.6.134 remote-address (IKE peer view)** command.	Not supported	Supported To set a remote ID, run the **remote-id** command. The remote IKE peer uses this ID for identity authentication.	Supported To set a remote ID, run the **remote-id** command. The remote IKE peer uses this ID for identity authentication.
RSA signature authentication (**rsa-signature**)	Supported To set a remote ID, run the **12.6.134 remote-address (IKE peer view)** command.	Supported To set a remote ID, run the **remote-id** command. The remote IKE peer uses the ID of the corresponding field in the certificate for identity authentication.	Supported To set a remote ID, run the **remote-id** command. The remote IKE peer uses the ID of the corresponding field in the certificate for identity authentication.	Supported To set a remote ID, run the **remote-id** command. The remote IKE peer uses the ID of the corresponding field in the certificate for identity authentication.

Example

Set the remote ID type of IKE peer **peer1** to **FQDN** for pre-shared key authentication.

```
<Huawei> system-view
[Huawei] ike peer peer1
[Huawei-ike-peer-peer1] remote-id-type fqdn
```

12.6.138 reset ike error-info

Function

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

Copyright © Huawei Technologies Co., Ltd.

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
```

12.6.139 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

 Copyright © Huawei Technologies Co., Ltd.

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
```

12.6.140 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

 Copyright © Huawei Technologies Co., Ltd.

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

When the number of IPSec tunnels is larger than 50% of the maximum limit, high CPU usage alarms may be generated in a short period of time after the command is run. After all the SAs are cleared, the CPU usage restores to the normal range.

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
```

Related Topics

12.6.24 display ike sa

12.6.141 reset ike statistics

Function

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

Format

reset ike statistics

 Copyright © Huawei Technologies Co., Ltd.

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
```

12.6.142 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

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

NOTICE

Statistics cannot be restored once being cleared.

You can run the **12.6.31 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
```

12.6.143 reset ipsec sa

Function

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

Format

reset ipsec sa [**remote** *ipv4-address* | **policy** *policy-name* [*seq-number*] | **parameters** *ipv4-address* { **ah** | **esp** } *spi* | **efficient-vpn** *efficient-vpn-name* | **profile** *profile-name*]

Parameters

Parameter	Description	Value
remote *ipv4-address*	Specifies the IPv4 address of the remote end.	The value is in dotted decimal notation.
policy *policy-name* [*seq-number*]	Specifies the name and sequence number of an IPSec policy. If *sequence-number* is not specified, all the IPSec policies in the IPSec policy group with the specified name are used.	The value must be an existing IPSec policy name or sequence number.
profile *profile-name*	Specifies the name of an IPSec profile. If **profile** is not specified, IPSec SAs established using all IPSec profiles are deleted.	The value must be an existing IPSec profile name.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
parameters *ipv4-address* { **ah** | **esp** } *spi*	Specifies the three elements that uniquely identify an IPSec SA. The three elements are *ipv4-address* (destination address), *protocol* (AH or ESP), and Security Parameter Index (SPI). To reset an SA, the three elements must be specified. If **parameters** is not specified, IPSec SAs established using any security protocol are deleted.	The three elements are described as follows: • *ipv4-address*: IPv4 address. • *protocol*: AH or 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:

- When the number of IPSec tunnels is larger than 50% of the maximum limit, high CPU usage alarms may be generated in a short period of time after the command is run. After all the SAs are cleared, the CPU usage restores to the normal range.
- If no parameter is specified, all IPSec SAs are deleted.
- If **parameters** is specified, the IPSec SAs in two directions are deleted simultaneously.
- If a manually created IPSec SA is deleted, the IKE peers automatically create a new IPSec SA based on the manually configured parameters.
- To delete IPSec SAs established through IKE negotiation, you must run the **reset ipsec sa** and **12.6.140 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.

Copyright © Huawei Technologies Co., Ltd.

Example

Delete all the IPSec SAs.
<Huawei> **reset ipsec sa**

Delete the IPSec SA with remote IP address 10.1.1.2.
<Huawei> **reset ipsec sa remote 10.1.1.2**

Delete all IPSec SAs created through IPSec policy group **policy1**.
<Huawei> **reset ipsec sa policy policy1**

Delete the IPSec SA with IPSec policy name **policy1** and sequence number 10.
<Huawei> **reset ipsec sa policy policy1 10**

Delete the IPSec SA whose remote IP address is 10.1.1.2, security protocol is AH, and SPI is 10000.
<Huawei> **reset ipsec sa parameters 10.1.1.2 ah 10000**

Delete the IPSec SA established through IPSec profile **profile1**.
<Huawei> **reset ipsec sa profile profile1**

Related Topics

12.6.44 display ipsec sa

12.6.144 reset ipsec statistics

Function

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

Format

reset ipsec 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.

 Copyright © Huawei Technologies Co., Ltd.

Example

Delete statistics about all IPSec packets.

```
<Huawei> reset ipsec statistics
```

Related Topics

12.6.46 display ipsec statistics

12.6.145 reset ipsec statistics route

Function

The **reset ipsec statistics route** command clears IPSec route injection statistics.

Format

reset ipsec statistics route

Parameters

None

Views

User view

Default Level

3: Management level

Usage Guidelines

NOTICE

Statistics cannot be restored once being cleared.

When locating IPSec route injection problems, you can collect the IPSec route injection statistics only within a specified period for fault location. Before collecting the statistics, run the **reset ipsec statistics route** command to clear the historical statistics and then run the **12.6.47 display ipsec statistics route** command to view IPSec route statistics.

Example

Clear IPSec route injection statistics.

```
<Huawei> reset ipsec statistics route
```

 Copyright © Huawei Technologies Co., Ltd.

12.6.146 reset ipsec proto-protect statistics

Function

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

Format

reset ipsec proto-protect statistics [**sa-name** *sa-name*]

Parameters

Parameter	Description	Value
sa-name *sa-name*	Specifies the IPSec Security Association (SA) name.	The value is an existing IPSec Security Association name.

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 proto-protect statistics** command to clear the original statistics.

Follow-up Procedure

Run the **display ipsec proto-protect 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 proto-protect statistics
```

12.6.147 respond-only enable

 Copyright © Huawei Technologies Co., Ltd.

Function

The **respond-only enable** command configures the local end as the IPSec responder that does not initiate IPSec negotiation.

The **undo respond-only enable** command cancels the configuration.

By default, if the local end establishes an IPSec tunnel using the ISAKMP IPSec policy, the local end initiates IPSec negotiation.

Format

respond-only enable

undo respond-only enable

Parameters

None

Views

ISAKMP IPSec policy view

Default Level

2: Configuration level

Usage Guidelines

If the IPSec peers establish IPSec tunnels using the ISAKMP IPSec policy, both ends initiate negotiation. You can configure one end as the responder that does not initiate negotiation, which can help you check the packet processing, and therefore diagnose and locate IPSec faults.

Example

Configure the peer in ISAKMP IPSec policy **policy1** with sequence number 100 as the responder for IPSec negotiation.

```
<Huawei> system-view
[Huawei] ipsec policy policy1 100 isakmp
[Huawei-ipsec-policy-isakmp-policy1-100] respond-only enable
```

12.6.148 resource acl

Function

The **resource acl** command defines subnet information of the headquarters on the Efficient VPN server.

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

By default, no subnet information of the headquarters is defined on the Efficient VPN server.

 Copyright © Huawei Technologies Co., Ltd.

Format

resource acl *acl-number*

undo resource acl

Parameters

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

Views

IKE peer view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The Efficient VPN server delivers headquarters network information defined in an ACL to the remote device. The ACL defines the headquarters subnets that branches can access. Traffic not destined for the subnets specified in the ACL is directly forwarded to the Internet. Such traffic does not pass through the IPSec tunnel.

When an Efficient VPN policy is configured, this command is used on the Efficient VPN server. You can reference the IKE peer on the Efficient VPN server to implement ACL delivery.

Prerequisites

An advanced ACL has been created.

Precautions

This command is only valid for IKEv1.

The sum of ACL rules pushed by the headquarters and ACL rules configured on the branch cannot exceed 512. Otherwise, the IPSec tunnels cannot be established.

Example

Configure ACL 3100 that defines headquarters subnet information on the IPSec Efficient VPN server.

```
<Huawei> system-view
[Huawei] acl 3100
[Huawei-acl-adv-3100] rule 5 permit ip source 10.1.1.0 0.0.0.255
[Huawei-acl-adv-3100] quit
```

 Copyright © Huawei Technologies Co., Ltd.

```
[Huawei] ike peer huawei
[Huawei-ike-peer-huawei] resource acl 3100
```

12.6.149 route accept

Function

The **route accept** command configures the device to generate routes based on the received subnet route information and define the priority and tag value for the routes.

The **undo route accept** command disables the function that generates routes based on the received subnet route information.

By default, the device does not generate routes based on the received subnet route information.

Format

route accept [**preference** *preference-number*] [**tag** *tag-value*]

undo route accept

Parameters

Parameter	Description	Value
preference *preference-number*	Specifies the priority for the route generated based on the received subnet route information.	The value is an integer that ranges from 1 to 255.
tag *tag-value*	Specifies the tag value for the route generated based on the received subnet route information.	The value is an integer that ranges from 1 to 4294967295.

Views

IKE peer view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When virtual tunnel interfaces are used for IPSec tunnel setup, you can run this command to allow the local device to accept subnet route information sent by the remote device.

 Copyright © Huawei Technologies Co., Ltd.

Precautions

The local device can accept subnet route information sent by the remote device only when both the **route accept** command and the **config-exchange set accept** command are configured.

NOTE

This command is supported by IKEv2 only.

Example

Configure the IKE peer named **peer1** to accept subnet route information sent by the remote device and set the priority and tag value of the generated route to 20 and 256 respectively.

```
<Huawei> system-view
[Huawei] ike peer peer1
[Huawei-ike-peer-peer1] route accept preference 20 tag 256
```

Related Topics

12.6.75 ike peer

12.6.11 config-exchange

12.6.150 route inject

Function

The **route inject** command configures route injection.

The **undo route inject** command cancels the configuration.

By default, route injection is not configured.

Format

route inject [**nexthop** *ipv4-address*] { **static** | **dynamic** } [**preference** *preference*]

undo route inject

Parameters

Parameter	Description	Value
nexthop *ipv4-address*	Specifies the next-hop IPv4 address to the remote end.	The value is in dotted decimal notation.
static	Enables static route injection. The parameter is only available in the ISAKMP IPSec policy view.	-
dynamic	Enables dynamic route injection.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
preference *preference*	Specifies the priority of a static route generated through route injection.	The value is an integer that ranges from 1 to 255. The default value is 60.

Views

ISAKMP IPSec policy view, IPSec policy template view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When an enterprise headquarters and its branch establish an IPSec tunnel, a static route to the branch subnet needs to be configured on the headquarters gateway. If there are many branch subnets, a large number of static routes need to be configured on the headquarters gateway. When branch subnets change, the static route configuration needs to be modified on the headquarters gateway, causing a difficulty in network maintenance. Route injection injects routes to branch subnets to the headquarters gateway based on IPSec tunnel information, which reduces manual configuration and improves configuration correctness. Route injection can also inject routes to headquarters subnets to the branch gateway based on IPSec tunnel information, implementing association between IPSec tunnel subnet information and routes.

Route injection works in two modes:

- Static mode: The generated static route is added to the local device immediately, and is independent of IPSec tunnel status change.
- Dynamic mode: If the IPSec tunnel is Up, the generated static route can be added to the local device. If the IPSec tunnel is Down, the generated static route can be deleted from the local device.

  Compared with static route injection, dynamic route injection is relevant to the IPSec tunnel status. Dynamic route injection prevents IPSec peers from sending IPSec packets over the IPSec tunnel in Down state, reducing packet loss.

You can configure a priority for the static route generated through route injection. For example, when there is another route to the same destination as the static route, specify the same priority for the routes so that traffic can be load balanced. If different priorities are specified for the routes, the routes can back up each other.

Precautions

Only IPSec SAs established in IKE negotiation mode support the route injection function. Manually configured IPSec SAs do not support the route injection function.

 Copyright © Huawei Technologies Co., Ltd.

The device does not support the route injection function when a Layer 2 interface is added to an IPSec policy group.

After the next hop is specified using the **route inject nexthop** command, the generated route is not used for IPSec packet forwarding if the IPSec tunnel remote address is not within the destination network segment of the injected route.

Example

Set the priority of a static route generated through route injection to 10.

```
<Huawei> system-view
[Huawei] ipsec policy policy1 10 isakmp
[Huawei-ipsec-policy-isakmp-policy1-10] route inject static preference 10
```

Related Topics

12.6.105 ipsec policy (system view)
12.6.106 ipsec policy-template

12.6.151 rsa encryption-padding

Function

The **rsa encryption-padding** command configures a padding mode for RSA encryption.

The **undo rsa encryption-padding** command restores the default padding mode for RSA encryption.

By default, the padding mode of RSA encryption is OAEP.

Format

rsa encryption-padding { **oaep** | **pkcs1** }

undo rsa encryption-padding

Parameters

Parameter	Description	Value
oaep	Set the padding mode of RSA encryption to Optimal Asymmetric Encryption Padding (OAEP).	-
pkcs1	Sets the padding mode of RSA encryption to Public-Key Cryptography Standards 1 (PKCS1).	-

Views

IKE peer view

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

On an IPSec-enabled network, identity authentication can be performed using an RSA digital envelope. When the padding mode of RSA encryption is set to PKCS1, there are security risks. To improve network security, run the **rsa encryption-padding** command to set the padding mode of RSA encryption to OAEP.

Example

Set the padding mode of RSA encryption to OAEP.

```
<Huawei> system-view
[Huawei] ike peer peer1
[Huawei-ike-peer-peer1] rsa encryption-padding oaep
```

Related Topics

12.6.20 display ike peer (all views)

12.6.152 rsa signature-padding

Function

The **rsa signature-padding** command configures a padding mode for the RSA signature.

The **undo rsa signature-padding** command restores the default padding mode for the RSA signature.

By default, the padding mode of the RSA signature is PSS.

Format

rsa signature-padding { **pkcs1** | **pss** }

undo rsa signature-padding

Parameters

Parameter	Description	Value
pkcs1	Sets the padding mode of the RSA signature to Public-Key Cryptography Standards 1 (PKCS1).	-
pss	Sets the padding mode of the RSA signature to Probabilistic Signature Scheme (PSS).	-

Views

IKE peer view, Efficient VPN policy view

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

On an IPSec-enabled network, identity authentication can be performed using an RSA signature or digital envelope. When the padding mode of the RSA signature in the certificate is set to PKCS1, there are security risks. To improve network security, run the **rsa signature-padding** command to set the padding mode of the RSA signature to PSS.

Example

Set the padding mode of the RSA signature to PSS.

```
<Huawei> system-view
[Huawei] ike peer peer1
[Huawei-ike-peer-peer1] rsa signature-padding pss
```

Related Topics

12.6.20 display ike peer (all views)

12.6.153 sa authentication-hex

Function

The **sa authentication-hex** command configures an authentication key for an IPSec SA in hexadecimal notation.

The **undo sa authentication-hex** command cancels the configuration.

By default, the authentication key is not configured for an IPSec SA.

Format

sa authentication-hex { **inbound** | **outbound** } { **ah** | **esp** } { **simple** | **cipher** } *hex-string*

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

Parameters

Parameter	Description	Value
inbound	Sets an authentication key for the inbound IPSec SA. IPSec uses the inbound IPSec SA to process incoming packets.	-
outbound	Sets an authentication key for the outbound IPSec SA. IPSec uses the outbound IPSec SA to process outgoing packets.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
ah	Sets an authentication key using the AH protocol. If the IPSec proposal referenced in an IPSec policy uses the AH protocol, the authentication key is set based on the *ah* keyword.	-
esp	Sets an authentication key using the ESP protocol. If the IPSec proposal referenced in an IPSec policy uses the ESP protocol, the authentication key is set based on the *esp* keyword.	-
simple	Indicates plain text authentication key. Type in an authentication key in plain text. The authentication key is displayed in plain text in the configuration file. **NOTICE** If **simple** is selected, the password is saved in the configuration file in plain text. This brings security risks. It is recommended that you select **cipher** to save the password in cipher text.	-
cipher	Indicates the cipher authentication key. You can enter an authentication key in plain text or cipher text. The authentication key is displayed in cipher text in the configuration file.	-
hex-string	Sets an authentication key for the IPSec SA.	The value is in the hexadecimal format. • If MD5 is used, the key length is 16 bytes. • If SHA1 is used, the key length is 20 bytes. • If SHA2-256 is used, the key length is 32 bytes. • If SHA2-384 is used, the key length is 48 bytes. • If SHA2-512 is used, the key length is 64 bytes.

Views

Manual IPSec policy view

Copyright © Huawei Technologies Co., Ltd.

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When manually configuring an IPSec policy, you must configure an authentication key for the inbound/outbound IPSec SA. The authentication key can be a hexadecimal number or a character string.

- The **sa authentication-hex** command sets an authentication key in hexadecimal notation.
- The **sa string-key** command sets a character string as the authentication key.

If two keys in different formats are configured, the key configured later takes effect.

Precautions

The inbound authentication key on the local end must be the same as the outbound authentication key on the remote end. The outbound authentication key on the local end must be the same as the inbound authentication key on the remote end.

The authentication key on both ends of an IPSec tunnel must use the same format. For example, an IPSec SA cannot be established if the authentication key on one end is a character string but that on the other end is a hexadecimal number.

Example

In IPSec policy **policy1** using AH and SHA2-256 on the local device, set the SPI and authentication key of the inbound IPSec SA to 10000 and 0x112233445566778899aabbccddeeff00aabbccddeeff001100aabbccddeeff00; set the SPI and authentication key of the outbound IPSec SA to 20000 and 0xaabbccddeeff001100aabbccddeeff00112233445566778899aabbccddeeff00.

```
<Huawei> system-view
[Huawei] ipsec proposal prop1
[Huawei-ipsec-proposal-prop1] transform ah
[Huawei-ipsec-proposal-prop1] ah authentication-algorithm sha2-256
[Huawei-ipsec-proposal-prop1] quit
[Huawei] ipsec policy policy1 1 manual
[Huawei-ipsec-policy-manual-policy1-1] sa spi inbound ah 10000
[Huawei-ipsec-policy-manual-policy1-1] sa authentication-hex inbound ah cipher
112233445566778899aabbccddeeff00aabbccddeeff001100aabbccddeeff00
[Huawei-ipsec-policy-manual-policy1-1] sa spi outbound ah 20000
[Huawei-ipsec-policy-manual-policy1-1] sa authentication-hex outbound ah cipher
aabbccddeeff001100aabbccddeeff00112233445566778899aabbccddeeff00
```

In IPSec policy **policy1** using AH and SHA2-256 on the remote device, set the SPI and authentication key of the inbound IPSec SA to 20000 and 0xaabbccddeeff001100aabbccddeeff00112233445566778899aabbccddeeff00; set the SPI and authentication key of the outbound IPSec SA to 10000 and 0x112233445566778899aabbccddeeff00aabbccddeeff001100aabbccddeeff00.

```
<Huawei> system-view
[Huawei] ipsec proposal prop1
```

 Copyright © Huawei Technologies Co., Ltd.

```
[Huawei-ipsec-proposal-prop1] transform ah
[Huawei-ipsec-proposal-prop1] ah authentication-algorithm sha2-256
[Huawei-ipsec-proposal-prop1] quit
[Huawei] ipsec policy policy1 1 manual
[Huawei-ipsec-policy-manual-policy1-1] sa spi inbound ah 20000
[Huawei-ipsec-policy-manual-policy1-1] sa authentication-hex inbound ah cipher
aabbccddeeff001100aabbccddeeff00112233445566778899aabbccddeeff00
[Huawei-ipsec-policy-manual-policy1-1] sa spi outbound ah 10000
[Huawei-ipsec-policy-manual-policy1-1] sa authentication-hex outbound ah cipher
11223344556778899aabbccddeeff00aabbccddeeff001100aabbccddeeff00
```

Related Topics

12.6.105 ipsec policy (system view)

12.6.164 sa string-key

12.6.154 sa authentication-hex (SA view)

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.	-

 Copyright © Huawei Technologies Co., Ltd.

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 authentication-hex** command.	-
cipher	Indicates the ciphertext 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.
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 is88. ● If authentication algorithm SHA2-256 is used, the length of the key is108.

Views

SA view

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

Usage Scenario

AH and ESP can use either MD5, SHA-1, or SHA-2 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.

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

Configure an authentication key in the hexadecimal format for the SA named **sa1**.

```
<Huawei> system-view
[Huawei] ipsec sa sa1
[Huawei-ipsec-sa-sa1] sa authentication-hex inbound ah abcdeF1234567891abcdeF1234567891
```

12.6.155 sa binding vpn-instance

Function

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

The **undo sa binding vpn-instance** command deletes 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

 Copyright © Huawei Technologies Co., Ltd.

Parameters

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

Views

IKE peer view, manual IPSec policy view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When multiple branches connected to the headquarters network across the Internet using IPSec, you can run the **sa binding vpn-instance** command to bind each VPN instance to an IPSec tunnel, thereby isolating traffic of different branches.

When configuring IPSec multi-instance, note the following points:

- If an IPSec policy is created using IKE and no VPN instance is specified, run the **sa binding vpn-instance** command in the IKE peer view to specify the VPN instance bound to the IPSec tunnel. The bound domain must be the same as the domain bound to the virtual interface that is generated during VPN instance creation.
- If an IPSec policy is created manually, run the **sa binding vpn-instance** command in the manual IPSec policy view to specify the VPN instance bound to the IPSec tunnel.
- In IPsec multi-instance, the security zone of decapsulated packets shall be identified with the decrypted packets inspection function. Therefore, the decrypted packets inspection function shall be enabled.

Prerequisites

The VPN instance has been created using the **ip vpn-instance** command and the route distinguisher (RD) has been configured for the VPN instance using the **route-distinguisher** command.

Precautions

The VPN instance specified by the **sa binding vpn-instance** command must be the same as the VPN instance bound to the ACL referenced by the IPSec tunnel.

Example

Configure the VPN instance **vpna** that IPSec tunnel traffic belongs to in the IPSec policy in manual mode.

 Copyright © Huawei Technologies Co., Ltd.

```
<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] quit
[Huawei-vpn-instance-vpna] quit
[Huawei] ipsec policy policy1 100 manual
[Huawei-ipsec-policy-manual-policy1-100] sa binding vpn-instance vpna
```

Related Topics

12.6.34 display ipsec policy (all views)
12.6.20 display ike peer (all views)

12.6.156 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 MPLS 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,

 Copyright © Huawei Technologies Co., Ltd.

these hosts can connect to the backbone network of the MPLS 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
```

Related Topics

12.6.98 ipsec efficient-vpn (system view)

12.6.30 display ipsec efficient-vpn

12.6.157 sa duration (IKE proposal view)

Function

The **sa duration** command specifies the IKE SA hard lifetime for an IKE proposal.

The **undo sa duration** command restores the default IKE SA hard lifetime.

By default, the IKE SA hard lifetime is 86400 seconds.

Format

sa duration *seconds*

undo sa duration

Parameters

Parameter	Description	Value
seconds	Specifies the IKE SA hard lifetime. IKE SA is automatically updated after the hard lifetime expires.	The value is an integer that ranges from 60 to 604800, in seconds.

 Copyright © Huawei Technologies Co., Ltd.

Views

IKE proposal view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the SA lifetime is set, SAs are updated in real time and difficult to decipher, enhancing security.

The IKE SA lifetime is classified as follows:

- Hard lifetime (hard timeout period): specifies the lifetime of an IKE SA.

  When two devices negotiate an IKE SA, the actual hard lifetime is the smaller of the two values configured on the two devices.
- Soft lifetime (soft timeout period): refers to the time after which a new IKE SA is negotiated so that the new IKE SA will be ready before the hard lifetime of the original IKE SA expires.

  Table 12-68 lists the default soft lifetime values.

Table 12-68 Soft lifetime values

IKE Protocol Type	Description
IKEv1	70% of the actual hard SA lifetime
IKEv2	65% to 75% of the actual hard SA lifetime

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

Precautions

IKE negotiation requires DH calculation, which takes a long time. Therefore, you are advised to set the IKE SA hard lifetime to a value longer than 10 minutes to make sure that the update of IKE SAs does not affect secure communication.

During IKEv1 negotiation, the responder cannot initiate IKE SA renegotiation after the IKE SA soft lifetime expires.

Example

Set the IKE SA hard lifetime to 600 seconds for IKE proposal 10.

```
<Huawei> system-view
[Huawei] ike proposal 10
[Huawei-ike-proposal-10] sa duration 600
```

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

12.6.22 display ike proposal (All views)

12.6.158 sa duration (ISAKMP IPSec policy view, IPSec policy template view, IPSec profile view)

Function

The **sa duration** command sets the hard lifetime of IPSec SAs in an IPSec policy or profile.

The **undo sa duration** command restores the default configuration.

By default, the hard lifetime of IPSec SAs is not configured in an IPSec policy or profile. The system uses the global hard lifetime of IPSec SAs.

Format

sa duration { **traffic-based** *kilobytes* | **time-based** *seconds* }

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

Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
traffic-based *kilobytes*	Specifies the traffic-based 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. During IPSec negotiation between a Huawei device and a Cisco device using IKEv1: • If the Huawei device functions as the initiator and the traffic hard lifetime is set to 0, the traffic hard lifetime value pushed by the Cisco device takes effect on the local end. • If the Huawei device functions as the responder and the traffic hard lifetime is set to 0, the value 0 takes effect on the local end.
time-based *seconds*	Specifies the time-based SA hard lifetime. When a large number of IPSec tunnels are established between two devices, you are advised to set the IPSec SA hard lifetime to a value larger than or equivalent to 1800s.	The value is an integer that ranges from 30 to 604800, in seconds.

Views

ISAKMP IPSec policy view, IPSec policy template view, IPSec profile view

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

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 12-69 lists the default soft lifetime values.

Table 12-69 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

The SA lifetime can be configured globally (**12.6.113 ipsec sa global-duration**) or based on an IPSec policy or profile. If no SA lifetime is configured for the IPSec policy or profile, the global lifetime is used. If both the global SA lifetime and lifetime based on the IPSec policy or profile are configured, the latter one takes effect.

 Copyright © Huawei Technologies Co., Ltd.

You only need to specify the SA lifetime for the SA setup through the IKE negotiation. That is, it is invalid to the SA manually set up. The manually set up SA is effective permanently.

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 IPSec SA hard lifetime in IPSec policy **policy1** to 7200 seconds.

```
<Huawei> system-view
[Huawei] ipsec policy policy1 1 isakmp
[Huawei-ipsec-policy-isakmp-policy1-1] sa duration time-based 7200
```

Set the IPSec SA hard lifetime in IPSec policy **policy2** to 20000 KB.

```
<Huawei> system-view
[Huawei] ipsec policy policy2 1 isakmp
[Huawei-ipsec-policy-isakmp-policy2-1] sa duration traffic-based 20000
```

Set the IPSec SA hard lifetime in IPSec profile **profile1** to 7200 seconds.

```
<Huawei> system-view
[Huawei] ipsec profile profile1
[Huawei-ipsec-profile-profile1] sa duration time-based 7200
```

Set the IPSec SA hard lifetime in IPSec profile **profile1** to 20000 KB.

```
<Huawei> system-view
[Huawei] ipsec profile profile1
[Huawei-ipsec-profile-profile1] sa duration traffic-based 20000
```

12.6.159 sa encryption-hex

Function

The **sa encryption-hex** command configures an encryption key for an IPSec SA.

The **undo sa encryption-hex** command cancels the configuration.

By default, the encryption key is not configured for an IPSec SA.

Format

sa encryption-hex { **inbound** | **outbound** } **esp** { **simple** | **cipher** } *hex-string*

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

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
inbound	Sets an encryption key for the inbound IPSec SA. IPSec uses the inbound IPSec SA to process incoming packets.	-
outbound	Sets an encryption key for the outbound IPSec SA. IPSec uses the outbound IPSec SA to process outgoing packets.	-
esp	Sets an encryption key using the ESP protocol. If the IPSec proposal referenced in an IPSec policy uses the ESP protocol, the authentication key is set based on the *esp* keyword.	-
simple	Indicates the encryption key in plain text. The encryption key is displayed in plain text in the configuration file. **NOTICE** If **simple** is selected, the password is saved in the configuration file in plain text. This brings security risks. It is recommended that you select **cipher** to save the password in cipher text.	-
cipher	Indicates the encryption key in cipher text. You can enter an authentication key in plain text or cipher text. The encryption key is displayed in cipher text in the configuration file.	-

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
hex-string	Sets an encryption key for the IPSec SA.	The value is a hexadecimal number. • If DES is used, the key length is 8 bytes. • If 3DES is used, the key length is 24 bytes • If AES-128 is used, the key length is 16 bytes. • If AES-192 is used, the key length is 24 bytes. • If AES-256 is used, the key length is 32 bytes. • If SM4 is used, the key length is 16 bytes.

Views

Manual IPSec policy view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **sa encryption-hex** command applies to manually created IPSec policies only. You do not need to set an encryption key for an IPSec SA established through IKE negotiation, because IKE peers automatically negotiate the encryption key.

Precautions

When configuring manual IPSec policies, you must set encryption keys for the IPSec SAs in **inbound** and **outbound** directions. The inbound encryption key on the local end must be the same as the outbound encryption key on the remote end. The outbound encryption key on the local end must be the same as the inbound encryption key on the remote end.

Example

In IPSec policy **policy1** using ESP and AES-256, set the SPI and encryption key of the inbound IPSec SA to 10000 and 0x1234567890abcdef1234567890abcdef1234567890abcdef1234567890abcdef; set the SPI and encryption key of the outbound IPSec SA to 20000 and 0xabcdefabcdef1234abcdefabcdef1234abcdefabcdef1234abcdefabcdef1234.

```
<Huawei> system-view
[Huawei] ipsec proposal prop1
```

 Copyright © Huawei Technologies Co., Ltd.

```
[Huawei-ipsec-proposal-prop1] quit
[Huawei] ipsec policy policy1 1 manual
[Huawei-ipsec-policy-manual-policy1-1] proposal prop1
[Huawei-ipsec-policy-manual-policy1-1] sa spi inbound esp 10000
[Huawei-ipsec-policy-manual-policy1-1] sa encryption-hex inbound esp cipher
1234567890abcdef1234567890abcdef1234567890abcdef1234567890abcdef
[Huawei-ipsec-policy-manual-policy1-1] sa spi outbound esp 20000
[Huawei-ipsec-policy-manual-policy1-1] sa encryption-hex outbound esp cipher
abcdefabcdef1234abcdefabcdef1234abcdefabcdef1234abcdefabcdef1234
```

12.6.160 sa encryption-hex (SA view)

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.	-

 Copyright © Huawei Technologies Co., Ltd.

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

Usage Scenario

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.

Copyright © Huawei Technologies Co., Ltd.

NOTE

If **sa encryption-hex** command is configured, then the encryption key configured using **sa string-key** command is deleted automatically.

Example

Configure an encryption key in the hexadecimal format for the SA named **sa1**.

```
<Huawei> system-view
[Huawei] ipsec sa sa1
[Huawei-ipsec-sa-sa1] sa encryption-hex inbound esp abcdabcdabcdabcd
```

12.6.161 sa keep-holding-to hard-duration

Function

The **sa keep-holding-to hard-duration** command configures the device to delete the original IPSec SA after the hard lifetime expires during IPSec SA re-negotiation.

The **undo sa keep-holding-to hard-duration** command configures the device to delete the original IPSec SA immediately after it uses the new IPSec SA to transmit data during IPSec SA re-negotiation.

By default, during IPSec SA re-negotiation, the device deletes the original IPSec SA immediately after using the new IPSec SA to transmit data.

Format

sa keep-holding-to hard-duration

undo sa keep-holding-to hard-duration

Parameters

None

Views

ISAKMP IPSec policy view, IPSec policy template view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After a new IPSec SA is negotiated, if the peer device still uses the original IPSec SA to transmit data while the local device deletes the original IPSec SA immediately after using the new IPSec SA to transmit data, the IPSec SAs on the two devices will be different. This will cause IPSec traffic interruption. In this case, you are advised to run the **sa keep-holding-to hard-duration** command to enable the local device to delete the original IPSec SA after the hard lifetime expires.

 Copyright © Huawei Technologies Co., Ltd.

Precautions

This command takes effect only for IPSec SAs established through IKEv1 negotiation.

Example

Configure the device to delete the original IPSec SA after the hard lifetime expires during IPSec SA re-negotiation.

```
<Huawei> system-view
[Huawei] ipsec policy policy1 1 isakmp
[Huawei-ipsec-policy-isakmp-policy1-1] sa keep-holding-to hard-duration
```

Related Topics

12.6.34 display ipsec policy (all views)

12.6.36 display ipsec policy-template (all views)

12.6.162 sa spi

Function

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

The **undo sa spi** command cancels the configuration.

By default, the SPI of an IPSec SA is not configured.

Format

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

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

Parameters

Parameter	Description	Value
inbound	Sets an SPI for the inbound IPSec SA.	-
outbound	Sets an SPI for the outbound IPSec SA.	-
ah	Sets an SPI using the AH protocol. If the IPSec proposal referenced in an IPSec policy uses the AH protocol, the authentication key is set based on the *ah* keyword.	-
esp	Sets an SPI using the ESP protocol. If the IPSec proposal referenced in an IPSec policy uses the ESP protocol, the authentication key is set based on the *esp* keyword.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
spi-number	Sets an SPI for the IPSec SA.	The value is an integer that ranges from 256 to 4294967295.

Views

Manual IPSec policy view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

An IPSec SA is uniquely identified by a triplet, including the SPI, destination IP address, and security protocol number (AH or ESP). The receiver uses the SPI to identify the binding between a data flow and an IPSec SA.

When manually configuring an IPSec policy, you must specify the SPIs for inbound and outbound SAs. The inbound SPI on the local end must be the same as the outbound SPI on the remote end. The outbound SPI on the local end must be the same as the inbound SPI on the remote end.

Precautions

This command applies to manually created IPSec policies only. You do not need to set an SPI for an IPSec SA established through IKE negotiation, because IKE peers automatically negotiate the SPI.

Example

In IPSec policy **policy1** using AH and SHA2-256 on the local device, set the SPI of the inbound IPSec SA to 10000; set the SPI of the outbound IPSec SA to 20000.

```
<Huawei> system-view
[Huawei] ipsec proposal prop1
[Huawei-ipsec-proposal-prop1] transform ah
[Huawei-ipsec-proposal-prop1] ah authentication-algorithm sha2-256
[Huawei-ipsec-proposal-prop1] quit
[Huawei] ipsec policy policy1 1 manual
[Huawei-ipsec-policy-manual-policy1-1] sa spi inbound ah 10000
[Huawei-ipsec-policy-manual-policy1-1] sa spi outbound ah 20000
```

In IPSec policy **policy1** using AH and SHA2-256 on the remote device, set the SPI of the inbound IPSec SA to 20000; set the SPI of the outbound IPSec SA to 10000.

```
<Huawei> system-view
[Huawei] ipsec proposal prop1
[Huawei-ipsec-proposal-prop1] transform ah
[Huawei-ipsec-proposal-prop1] ah authentication-algorithm sha2-256
[Huawei-ipsec-proposal-prop1] quit
[Huawei] ipsec policy policy1 1 manual
```

 Copyright © Huawei Technologies Co., Ltd.

```
[Huawei-ipsec-policy-manual-policy1-1] sa spi inbound ah 20000
[Huawei-ipsec-policy-manual-policy1-1] sa spi outbound ah 10000
```

12.6.163 sa spi (SA view)

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.	-
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

 Copyright © Huawei Technologies Co., Ltd.

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

Set the SPI for the SA named **sa1**.

```
<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
```

12.6.164 sa string-key

Function

The **sa string-key** command configures a character string as an authentication key for an IPSec SA.

The **undo sa string-key** command cancels the configuration.

By default, the authentication key is not configured for an IPSec SA.

Format

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

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

Parameters

Parameter	Description	Value
inbound	Sets an authentication key for the inbound IPSec SA.	-
outbound	Sets an authentication key for the outbound IPSec SA.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
ah	Sets an authentication key using the AH protocol. If the IPSec proposal referenced in an IPSec policy uses the AH protocol, the authentication key is set based on the *ah* keyword.	-
esp	Sets an authentication key using the ESP protocol. If the IPSec proposal referenced in an IPSec policy uses the ESP protocol, the authentication key is set based on the *esp* keyword.	-
simple	Indicates plain text authentication key. Type in an authentication key in plain text. The authentication key is displayed in plain text in the configuration file. **NOTICE** If **simple** is selected, the password is saved in the configuration file in plain text. This brings security risks. It is recommended that you select **cipher** to save the password in cipher text.	-
cipher	Indicates the cipher authentication key. You can enter an authentication key in plain text or cipher text. The authentication key is displayed in cipher text in the configuration file.	-

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
string-key	Sets an authentication key for the IPSec SA.	The value is a string of case-sensitive characters without question marks (?) and spaces. The value is a string of 1 to 255 characters in plain text or 48 to 348 characters in cipher text. **NOTE** To ensure security, the authentication key must meet the minimum complexity requirement. That is, the authentication key must be a combination of three of the following: uppercase letters, lowercase letters, digits, and special characters (such as !, @, #, $, and %).

Views

Manual IPSec policy view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When an authentication algorithm is specified in the IPSec proposal referenced by a manually created IPSec policy, you must configure an authentication key for the inbound/outbound SA. The inbound authentication key on the local end must be the same as the outbound authentication key on the remote end. The outbound authentication key on the local end must be the same as the inbound authentication key on the remote end.

The authentication key can be a hexadecimal number or a character string.

- The **sa string-key** command sets a character string as the authentication key.
- The **sa authentication-hex** command sets an authentication key in hexadecimal notation.

If two keys in different formats are configured, the key configured later takes effect.

Precautions

 Copyright © Huawei Technologies Co., Ltd.

The **sa string-key** command applies to manually created IPSec policies only. You do not need to set an authentication key for an IPSec SA established through IKE negotiation, because IKE peers automatically negotiate the authentication key.

The authentication key on both ends of an IPSec tunnel must use the same format. For example, an IPSec SA cannot be established if the authentication key on one end is a character string but that on the other end is a hexadecimal number.

Example

In IPSec policy **policy1** using AH and SHA2-256 on the local device, set the SPI and authentication key of the inbound IPSec SA to 10000 and **Test@123**; set the SPI and authentication key of the outbound IPSec SA to 20000 and **Test@456**.

```
<Huawei> system-view
[Huawei] ipsec proposal prop1
[Huawei-ipsec-proposal-prop1] transform ah
[Huawei-ipsec-proposal-prop1] ah authentication-algorithm sha2-256
[Huawei-ipsec-proposal-prop1] quit
[Huawei] ipsec policy policy1 1 manual
[Huawei-ipsec-policy-manual-policy1-1] sa spi inbound ah 10000
[Huawei-ipsec-policy-manual-policy1-1] sa string-key inbound ah cipher Test@123
[Huawei-ipsec-policy-manual-policy1-1] sa spi outbound ah 20000
[Huawei-ipsec-policy-manual-policy1-1] sa string-key outbound ah cipher Test@456
```

In IPSec policy **policy1** using AH and SHA2-256 on the remote device, set the SPI and authentication key of the inbound IPSec SA to 20000 and **Test@456**; set the SPI and authentication key of the outbound IPSec SA to 10000 and **Test@123**.

```
<Huawei> system-view
[Huawei] ipsec proposal prop1
[Huawei-ipsec-proposal-prop1] transform ah
[Huawei-ipsec-proposal-prop1] ah authentication-algorithm sha2-256
[Huawei-ipsec-proposal-prop1] quit
[Huawei] ipsec policy policy1 1 manual
[Huawei-ipsec-policy-manual-policy1-1] sa spi inbound ah 20000
[Huawei-ipsec-policy-manual-policy1-1] sa string-key inbound ah cipher Test@456
[Huawei-ipsec-policy-manual-policy1-1] sa spi outbound ah 10000
[Huawei-ipsec-policy-manual-policy1-1] sa string-key outbound ah cipher Test@123
```

12.6.165 sa string-key (SA view)

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** }

 Copyright © Huawei Technologies Co., Ltd.

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 ciphertext used for authentication.	-
string-cipher-key	Specifies the ciphertext 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 simple 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

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

Usage Scenario

AH and ESP can use either Message Digest 5 (MD5), Secure Hash Algorithm 1 (SHA-1) or SHA-2, 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.

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

Set an authentication key in the string format for the SA named **sa1**.

```
<Huawei> system-view
[Huawei] ipsec sa sa1
[Huawei-ipsec-sa-sa1] sa string-key inbound esp Hello-13579
[Huawei-ipsec-sa-sa1] sa string-key outbound esp Huawei-13579
```

12.6.166 sa trigger-mode

Function

The **sa trigger-mode** command configures a mode in which IPSec tunnel setup is triggered.

The **undo sa trigger-mode** command restores the default mode in which IPSec tunnel setup is triggered.

By default, the IPSec tunnel trigger mode is **auto**.

Format

sa trigger-mode { **auto** | **traffic-based** }

undo sa trigger-mode

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
auto	Indicates that IPSec tunnel setup is triggered automatically.	-
traffic-based	Indicates that IPSec tunnel setup is triggered by traffic.	-

Views

ISAKMP IPSec policy view

Default Level

2: Configuration level

Usage Guidelines

If **auto** is specified, IPSec tunnel setup is triggered automatically. If **traffic-based** is specified, an IPSec tunnel is triggered by outgoing data flows matching the IPSec policy.

Example

Set the mode in which IPSec tunnel setup is triggered to **traffic-based**.

```
<Huawei> system-view
[Huawei] ipsec policy test 10 isakmp
[Huawei-ipsec-policy-isakmp-test-10] sa trigger-mode traffic-based
```

12.6.167 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* [**dynamic-source**]

undo security acl

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
acl-number	Specifies the number of an ACL.	The value is an integer that ranges from 3000 to 3999.
dynamic-source	Indicates that the IP address of the applied interface in the IPSec policy replaces the source IP address in its referenced ACL. This parameter is only valid in IPSec policy view.	-

Views

Manual IPSec policy view, ISAKMP IPSec policy view, IPSec policy template view, 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 256. Otherwise, this ACL cannot be referenced in this IPSec policy.

After an IPSec tunnel has been established, if both permit and deny actions are configured in an ACL rule in the IPSec policy template view, the deny action does not take effect.

 Copyright © Huawei Technologies Co., Ltd.

Example

Reference ACL 3100 in a manually created IPSec policy.

```
<Huawei> system-view
[Huawei] acl number 3100
[Huawei-acl-adv-3100] rule permit tcp source 10.1.1.1 0.0.0.0 destination 10.1.1.2 0.0.0.0
[Huawei-acl-adv-3100] quit
[Huawei] ipsec policy policy1 100 manual
[Huawei-ipsec-policy-manual-policy1-100] security acl 3100
```

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
```

12.6.168 service-scheme

Function

The **service-scheme** command specifies a service scheme referenced by an IKE peer.

The **undo service-scheme** command deletes a service scheme referenced by an IKE peer.

By default, an IKE peer does not reference any service scheme.

Format

service-scheme *service-scheme-name*

undo service-scheme

Parameters

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

Views

IKE peer view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

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

 Copyright © Huawei Technologies Co., Ltd.

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. In this case, run the **service-scheme** command to specify a service scheme referenced by an IKE peer. After this command is configured, remote ends are authorized based on network resource information pushed by the server end.

Prerequisites

A service scheme has been created by running the **service-scheme** *service-scheme-name* command.

Example

Configure the service scheme **service** referenced by an IKE peer.

```
<Huawei> system-view
[Huawei] aaa
[Huawei-aaa] service-scheme service
[Huawei-aaa-service-service] quit
[Huawei-aaa] quit
[Huawei] ike peer huawei
[Huawei-ike-peer-huawei] service-scheme service
```

Related Topics

12.6.20 display ike peer (all views)

12.6.169 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

 Copyright © Huawei Technologies Co., Ltd.

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
```

Related Topics

12.6.30 display ipsec efficient-vpn

12.6.170 sim-based-username

Function

The **sim-based-username** command configures the user name and password of the remote device for authentication by the RADIUS server.

The **undo sim-based-username** command deletes the user name and password of the remote device for authentication by the RADIUS server.

By default, the user name and password of the remote device for authentication by the RADIUS server are not configured.

Format

sim-based-username type { **imei** | **imsi** } **password** *password*

undo sim-based-username

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
type { **imei** | **imsi** }	Obtains the corresponding user name by the type. • **imei**: indicates that the type of the user name is International Mobile Equipment Identity (IMEI). • **imsi**: indicates that the type of the user name is International Mobile Subscriber Identity (IMSI).	-
password *password*	Sets the password of the remote device for authentication by the RADIUS server.	The value is a string of case-sensitive characters. It cannot contain question marks (?) or spaces. The *password* is in plain text containing 9 to 32 characters or in cipher text containing 48 to 68 characters. **NOTE** To improve the security, it is recommended that the certificate revocation password contains at least two types of lowercase letters, uppercase letters, digits, and special characters, and contains at least 9 characters.

Views

Efficient VPN policy view

Default Level

2: Configuration level

Usage Guidelines

When the remote device establishes an IKE SA with the RADIUS server, the remote device needs to be authenticated and authorized by the RADIUS server. The remote device needs to send the user name and password to the RADIUS server. The remote device can obtain the user name based on the user name type configured using this command.

 Copyright © Huawei Technologies Co., Ltd.

Example

Set the user name type and password of the remote device for authentication by the RADIUS server to **IMSI** and **Huawei@1234**.

```
<Huawei> system-view
[Huawei] ipsec efficient-vpn evpn mode network-auto-cfg
[Huawei-ipsec-efficient-vpn-evpn] sim-based-username type imsi password Huawei@1234
```

12.6.171 switch-back enable

Function

The **switch-back enable** command enables revertive switching of an IKE peer.

The **undo switch-back enable** command disables revertive switching of an IKE peer.

By default, revertive switching of an IKE peer is disabled.

Format

switch-back enable

undo switch-back enable

Parameters

None

Views

IKE peer view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On a live network, to improve network reliability, the headquarters provides two devices to connect to the branch. On the branch gateway, two IP addresses or domain names are configured for an IKE peer to establish connections with the headquarters. Normally, the branch gateway connects to the primary headquarters gateway. When the primary headquarters gateway becomes unreachable, the branch gateway connects to the secondary headquarters gateway to prevent traffic loss. After the primary headquarters gateway recovers, you need to run the **switch-back enable** command to enable revertive switching to the primary headquarters gateway.

Precautions

The **12.6.134 remote-address (IKE peer view)** command must also be executed to configure an IKE peer to perform redundancy switching according to the NQA test instance status or the BFD session status. The switching function takes effect

 Copyright © Huawei Technologies Co., Ltd.

based on the NQA test instance status change or BFD session status change instead of based on the detection result.

Example

Configure revertive switching of the IKE peer **huawei**.

```
<Huawei> system-view
[Huawei] ike peer huawei
[Huawei-ike-peer-huawei] switch-back enable
```

12.6.172 transform

Function

The **transform** command specifies a security protocol used in an IPSec proposal.

The **undo transform** command restores the default configuration.

By default, an IPSec proposal uses the ESP protocol.

Format

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

undo transform

Parameters

Parameter	Description	Value
ah	Indicates that the IPSec proposal uses the Authentication Header (AH) protocol.	-
ah-esp	Indicates that the IPSec proposal encapsulates packets through ESP, then through AH.	-
esp	Indicates that the IPSec proposal uses the ESP protocol.	-

Views

IPSec proposal view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Three security modes are available and their differences are as follows:

 Copyright © Huawei Technologies Co., Ltd.

- In the AH mode, devices only authenticate packets.
- In the ESP mode, devices provide packet authentication, encryption, or both functions.
- In the AH-ESP mode, devices use the AH protocol to authenticate packets and the ESP protocol to encrypt packets. During IPSec encapsulation, devices encapsulate packets using ESP and then AH. During IPSec decapsulation, devices decapsulate packets using AH and then ESP.

AH prevents data tampering but cannot prevent data from being listened to, 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.

Precautions

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

Example

Set the security protocol used in IPSec proposal **newprop1** to AH.

```
<Huawei> system-view
[Huawei] ipsec proposal newprop1
[Huawei-ipsec-proposal-newprop1] transform ah
```

12.6.173 transform (ipsec-proto-protect-proposal view)

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 2406.

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 proto-protect proposal view

 Copyright © Huawei Technologies Co., Ltd.

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Based on packet encryption and authentication at the IP layer, IPSec ensures the integrity, authenticity, and confidentiality of packets transmitted on networks. IPSec uses two protocols, AH and ESP, for data authentication and encryption.

- AH: provides data origin and integrity authentication.
- ESP: provides data origin and integrity authentication and data encryption.

Configuration Impact

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

NOTE

AH uses the authentication algorithm SHA2-256 by default. ESP uses the authentication algorithm SHA2-256 and the encryption algorithm AES 128 by default.

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

The security protocols on both IPSec peers must be identical.

Example

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

```
<Huawei> system-view
[Huawei] ipsec proto-protect proposal prop1
[Huawei-ipsec-proto-protect-proposal-prop1] transform ah
```

12.6.174 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

 Copyright © Huawei Technologies Co., Ltd.

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. **NOTE** This parameter takes effect only in the ISAKMP IPSec policy view.	-

Views

Manual IPSec policy view, ISAKMP IPSec policy view, IPSec policy template view, Efficient VPN policy view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

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

For a manually created IPSec policy, you must run the **tunnel local** *ipv4-address* command to configure an IP address for the local end before you can create an SA. Only after correct IP addresses are configured for the local end (start point) and remote end (end point), an IPSec tunnel can be established between the two ends.

For the IKE negotiation mode, 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.

 Copyright © Huawei Technologies Co., Ltd.

Precautions

- If an IPSec policy is created manually, **tunnel local** on the local end must be the same as the **tunnel remote** on the remote end.
- If an IPSec policy is created in IKE negotiation mode, the **tunnel local** on the local end must be the same as **12.6.134 remote-address (IKE peer view)** that the remote end references from the IKE peer.
- You do not need to specify the **12.6.174 tunnel local** (local address) for the IKE peer referenced in an IPSec profile, because the local address is the source address of the GRE, mGRE or IPSec virtual tunnel interface. For the IKE peer referenced in an IPSec profile, **12.6.174 tunnel local** does not take effect.
- When applying an IPSec policy to a tunnel interface and running the **12.3.18 source** command to specify an IP address for the interface, you must run the **12.6.174 tunnel local** command to configure a tunnel local address. Otherwise, IKE negotiation will fail.
- In an IPSec hot standby scenario, **tunnel local** must be set to a virtual IP address.

Example

Set the local IP address of the IPSec tunnel to 10.1.1.1 in the manual IPSec policy view.

```
<Huawei> system-view
[Huawei] ipsec policy policy1 100 manual
[Huawei-ipsec-policy-manual-policy1-100] tunnel local 10.1.1.1
```

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

```
<Huawei> system-view
[Huawei] ipsec policy policy1 100 isakmp
[Huawei-ipsec-policy-isakmp-policy1-100] tunnel local applied-interface
```

12.6.175 tunnel remote

Function

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

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

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

Format

tunnel remote *ip-address*

undo tunnel remote

Parameters

Parameter	Description	Value
ip-address	Specifies an IPv4 address for the remote end of an IPSec tunnel.	The value is in dotted decimal notation.

 Copyright © Huawei Technologies Co., Ltd.

Views

Manual IPSec policy view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

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

For a manually created IPSec policy, you must run the **tunnel remote** *ip-address* command to configure an IP address for the remote end before you can create an SA. Only after correct IP addresses are configured for the local end (start point) and remote end (end point), an IPSec tunnel can be established between the two ends.

Precautions

If an IPSec policy is created manually, **tunnel remote** on the local end must be the same as **tunnel local** on the remote end.

Example

Set the remote IP address in IPSec policy **policy1** to 10.1.1.2.

```
<Huawei> system-view
[Huawei] ipsec policy policy1 1 manual
[Huawei-ipsec-policy-manual-policy1-1] tunnel remote 10.1.1.2
```

12.6.176 tunnel pathmtu enable

Function

The **tunnel pathmtu enable** command enables the device to learn the maximum transmission unit (MTU) of packets allowed on an IPSec tunnel.

The **undo tunnel pathmtu enable** command disables the device from learning the MTU of packets allowed on an IPSec tunnel.

By default, the device cannot learn the MTU of packets allowed on an IPSec tunnel.

Format

tunnel pathmtu enable

undo tunnel pathmtu enable

Parameters

None

 Copyright © Huawei Technologies Co., Ltd.

Views

Tunnel interface view, Tunnel-Template interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the local device sends IPSec packets along a created IPSec tunnel, the IPSec packets are discarded if the packet MTU exceeds the MTU allowed on the IPSec tunnel and the local device receives an ICMP Unreachable packet.

The local device uses the MTU in the ICMP Unreachable packet and the Security Parameter Index (SPI) of the SA, and then automatically adjusts the interface MTU to a proper value to allow IPSec packets to pass.

Prerequisites

This command takes effect only when the encapsulation mode of the tunnel interface has been set to **IPSec** or **GRE** using the **tunnel-protocol** command or the **destination** command has been configured on the tunnel interface.

The Don't Fragment (DF) field of the IPSec tunnel has been set to 1 using the **ipsec df-bit set** command, indicating that packet fragmentation is not allowed on the IPSec tunnel.

Precautions

If there is a firewall on the network, this command cannot take effect because the firewall blocks ICMP packets.

If devices have the NAT traverse function enabled, this command cannot take effect because the format of IPSec packets has changed after the NAT traverse and the devices cannot identify the SPI values of SAs.

Example

Enable the device to learn the MTU allowed on an IPSec tunnel on a virtual tunnel interface.

```
<Huawei> system-view
[Huawei] interface tunnel 0/0/1
[Huawei-Tunnel0/0/1] tunnel-protocol ipsec
[Huawei-Tunnel0/0/1] tunnel pathmtu enable
```

12.6.177 user (IKE user table view)

Function

The **user** command configures IKE user information.

The **undo user** command deletes IKE user information.

By default, no IKE user information is configured.

 Copyright © Huawei Technologies Co., Ltd.

Format

user id-type { **any** *any-id* | **fqdn** *remote-fqdn* | **ip** *ip-address* | **user-fqdn** *remote-user-fqdn* } **vpn-instance** *vpn-instance-name*

user id-type { **any** *any-id* | **fqdn** *remote-fqdn* | **ip** *ip-address* | **user-fqdn** *remote-user-fqdn* } **pre-shared-key** *key* [**description** *description*]

undo user id-type { **any** *any-id* | **fqdn** *remote-fqdn* | **ip** *ip-address* | **user-fqdn** *remote-user-fqdn* } **vpn-instance**

undo user id-type { **any** *any-id* | **fqdn** *remote-fqdn* | **ip** *ip-address* | **user-fqdn** *remote-user-fqdn* } **pre-shared-key**

Parameters

Parameter	Description	Value
id-type	Specifies the remote ID type and remote ID of an IKE peer.	-
any *any-id*	Indicates that the remote ID of an IKE peer can be of any type and configures the remote ID.	The value is a string of 1 to 255 case-sensitive characters without question marks (?) and spaces.
fqdn *remote-fqdn*	Specifies the name as the remote ID of an IKE peer and configures the remote ID.	The value is a string of 1 to 255 case-sensitive characters without question marks (?) and spaces.
ip *ip-address*	Specifies the IP address as the remote ID of an IKE peer and configures the remote ID.	The value is in dotted decimal notation.
user-fqdn *remote-user-fqdn*	Specifies the domain name as the remote ID of an IKE peer and configures the remote ID.	The value is a string of 1 to 255 case-sensitive characters without question marks (?) and spaces.
vpn-instance *vpn-instance-name*	Specifies a VPN instance name.	The value is the name of an existing VPN instance.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
pre-shared-key *key*	Specifies a pre-shared key.	The value is a string of 1 to 128 case-sensitive characters in plaintext or 48 to 188 case-sensitive characters in ciphertext. When the value contains the question mark (?) or space, you must enclose the value with double quotation marks ("").
description *description*	Specifies the description of an IKE user.	The value is a string of 1 to 63 case-sensitive characters without question marks (?).

Views

IKE user table view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The device functions as the headquarters gateway, an IPSec policy is created using an IPSec policy template, and the gateway receives IPSec connection requests of different branches. If the pre-shared key is used for identity authentication and all branches use the same ID and pre-shared key, there are security risks. That is, if the ID and pre-shared key of one branch leak, the ID and pre-shared key of all branches leak. The IKE user table can prevent this problem.

The IKE user table records the mapping between remote IDs of IKE peers and pre-shared keys. After an IKE peer references the IKE user table, the device searches for the pre-shared key matching the remote ID of the IKE peer in the IKE user table to complete identity authentication during IKE negotiation. In this manner, branches use different IDs and pre-shared keys for identity authentication.

In addition, on an MPLS 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 the resources on another VPN site only through the insecure Internet. To enhance access security, these hosts can connect to the backbone network of the MPLS VPN through an IPSec tunnel.

After you run this command, the device determines the VPN instance to which site traffic passing through the IPSec tunnel belongs by the user type, isolating traffic from different sites.

Prerequisites

 Copyright © Huawei Technologies Co., Ltd.

The VPN instance has been created using the **ip vpn-instance** command and the route distinguisher (RD) has been configured for the VPN instance using the **route-distinguisher** command.

Precautions

- After an IKE peer references an IKE user table, the pre-shared key configured by this command takes precedence over the pre-shared key configured using the **pre-shared-key** command.
- After an IKE peer references an IKE user table, the VPN instance configured by this command takes precedence over the VPN instance configured using the **sa binding vpn-instance** command.
- If IKEv1 in main mode is used, **id-type** must be set to **ip**. In NAT traversal scenarios, *ip-address* must be the IP address translated by the NAT device.

Example

Configure user information in IKE user table 10, and set the remote ID type, remote ID, and pre-shared key to **IP**, 10.1.1.1, and **Test!123** respectively.

```
<Huawei> system-view
[Huawei] ike user-table 10
[Huawei-ike-user-table-10] user id-type ip 10.1.1.1 pre-shared-key Test!123
```

Configure user information in IKE user table 10, and bind it to VPN instance **vpna**.

```
<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] quit
[Huawei-vpn-instance-vpna] quit
[Huawei] ike user-table 10
[Huawei-ike-user-table-10] user id-type ip 10.1.1.1 vpn-instance vpna
```

Related Topics

12.6.74 ike user-table

12.6.178 user

Function

The **user** command creates an IKE user and displays the IKE user view, or directly displays the view of an existing IKE user.

The **undo user** command deletes the created IKE user.

By default, no IKE user is created in an IKE user table.

Format

user *user-name*

undo user *user-name*

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
user-name	Specifies the name of an IKE user.	The value is a string of 1 to 63 case-sensitive characters without spaces and question marks (?).

Views

IKE user table view

Default Level

2: Configuration level

Usage Guidelines

After the **ike user-table** command is used to create an IKE user table and enter the IKE user table view, run the **user** command to create an IKE user and enter the IKE user view. You can define the pre-shared key, user ID, IP address, DNS server address, and VPN instance in the IKE user view.

Example

Create an IKE user in the IKE user table.

```
<Huawei> system-view
[Huawei] ike user-table 10
[Huawei-ike-user-table-10] user user1
[Huawei-ike-user-table-10-user1]
```

Related Topics

12.6.74 ike user-table

12.6.63 id-type

12.6.127 pre-shared-key (IKE user view)

12.6.181 vpn-instance-traffic (IKE user view)

12.6.27 display ike user-table (all views)

12.6.179 user-table

Function

The **user-table** command references an IKE user table in an IKE peer.

The **undo user-table** command deletes the referenced IKE user table.

By default, the IKE peer does not reference an IKE user table.

 Copyright © Huawei Technologies Co., Ltd.

Format

user-table *user-table-id*

undo user-table

Parameters

Parameter	Description	Value
user-table-id	Specifies the ID of an IKE user table.	The value must be an existing IKE user table ID.

Views

IKE peer view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

An IKE user table records the mapping between remote IDs of IKE peers and pre-shared keys. After an IKE peer references an IKE user table, the device searches for the pre-shared key matching the remote ID of the IKE peer in the IKE user table to complete identity authentication during IKE negotiation. In this manner, branches use different IDs and pre-shared keys.

Prerequisites

An IKE user table has been created using the **ike user-table** command.

Precautions

After an IKE peer references an IKE user table, the pre-shared key configured using the **12.6.127 pre-shared-key (IKE user view)** command takes precedence over that configured using the **12.6.126 pre-shared-key (IKE peer view, Efficient VPN policy view)** command.

Example

Reference IKE user table 10 in IKE peer **peer1**.

```
<Huawei> system-view
[Huawei] ike user-table 10
[Huawei-ike-user-table-10] quit
[Huawei] ike peer peer1
[Huawei-ike-peer-peer1] user-table 10
```

Related Topics

12.6.74 ike user-table

 Copyright © Huawei Technologies Co., Ltd.

12.6.180 version

Function

The **version** command sets the IKE version number of an IKE peer.

The **undo version** command cancels the configuration.

By default, IKEv1 and IKEv2 are enabled.

Format

version { **1** | **2** }

undo version { **1** | **2** }

Parameters

Parameter	Description	Value
1	Indicates that the IKE version number is 1.	-
2	Indicates that the IKE version number is 2.	-

Views

IKE peer view

Default Level

2: Configuration level

Usage Guidelines

IKEv1 and IKEv2 cannot be disabled simultaneously.

If IKEv1 and IKEv2 are enabled simultaneously, the initiator uses IKEv2, and the responder can use IKEv1 or IKEv2.

Example

Configure IKE peer **peer1** to initiate negotiation using IKEv1.

```
<Huawei> system-view
[Huawei] ike peer peer1
[Huawei-ike-peer-peer1] undo version 2
```

12.6.181 vpn-instance-traffic (IKE user view)

Function

The **vpn-instance-traffic** command configures a VPN instance corresponding to user traffic of the IKE user table.

 Copyright © Huawei Technologies Co., Ltd.

The **undo vpn-instance-traffic** command deletes a VPN instance corresponding to user traffic of the IKE user table.

By default, the VPN instance corresponding to user traffic of the IKE user table is not configured.

Format

vpn-instance-traffic { **public** | **name** *vpn-instance-name* }

undo vpn-instance-traffic

Parameters

Parameter	Description	Value
public	Indicates that user traffic of the IKE user table is public network traffic.	-
name *vpn-instance-name*	Specifies the name of a VPN instance.	The value must be an existing VPN instance name.

Views

IKE user view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In a scenario where multiple branches connect to the headquarters, you can run the **sa binding vpn-instance** command to specify the VPN instance that IPSec tunnel traffic belongs to, thereby isolating traffic of different branches. When the device functions as the headquarters gateway and an IPSec policy is created using an IPSec policy template, the headquarters gateway cannot distinguish VPNs of different branches. You can run the **vpn-instance-traffic** command to specify VPNs for different branches.

Prerequisites

1. A VPN instance has been created using the **12.9.35 ip vpn-instance** command.
2. An RD has been configured using the **12.9.50 route-distinguisher** command.

Precautions

After an IKE user table is referenced by an IKE peer, the VPN instance configured by this command takes precedence over the VPN instance configured by the **sa binding vpn-instance** command.

 Copyright © Huawei Technologies Co., Ltd.

Example

Configure a VPN instance named **vrf1** corresponding to user traffic of the IKE user table.

```
<Huawei> system-view
[Huawei] ip vpn-instance vrf1
[Huawei-vpn-instance-vrf1] route-distinguisher 22:1
[Huawei-vpn-instance-vrf1-af-ipv4] quit
[Huawei-vpn-instance-vrf1] quit
[Huawei] ike user-table 10
[Huawei-ike-user-table-10] user user1
[Huawei-ike-user-table-10-user1] vpn-instance-traffic name vrf1
```

Related Topics

12.9.35 ip vpn-instance

12.9.50 route-distinguisher

12.6.27 display ike user-table (all views)

12.6.182 user-fqdn

Function

The **user-fqdn** command configures the user domain name of an allowed peer for IKE negotiation.

The **undo user-fqdn** command deletes the user domain name of the allowed peer.

By default, no user domain name of allowed peer for IKE negotiation is configured.

Format

user-fqdn *fqdn-name*

undo user-fqdn *fqdn-name*

Parameters

Parameter	Description	Value
fqdn-name	Specifies the user domain name of the peer for IKE negotiation.	The value is an existing user domain name of the peer for IKE negotiation.

Views

Identity filter set view

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

Usage Scenario

You can run this command to configure a user domain name in the identity filter set to specify the allowed peer.

Precautions

An IPSec tunnel can be established only when the peer matches one or more attributes in the identity filter set and IPSec negotiation parameters on two ends are the same.

You can run this command in the same view multiple times to specify multiple user domain names.

Example

Set the user domain name of the allowed peer for IKE negotiation to **liming@huawei.com**.

```
<Huawei> system-view
[Huawei] ike identity identity1
[Huawei-ike-identity-identity1] user-fqdn liming@huawei.com
```

Related Topics

12.6.121 match ike-identity

12.7 A2A VPN Configuration Commands

12.7.1 anti-replay time-based enable

Function

The **anti-replay time-based enable** command enables the time-based anti-replay function for the A2A VPN.

The **undo anti-replay time-based enable** command disables the time-based anti-replay function for the A2A VPN.

By default, the time-based anti-replay function is disabled for the A2A VPN.

Format

anti-replay time-based enable

undo anti-replay time-based enable

Parameters

None

 Copyright © Huawei Technologies Co., Ltd.

Views

GDOI group IPSec policy view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To prevent unauthorized users from stealing A2A VPN packets for DoS attacks, the A2A VPN provides the time-based anti-replay function to detect replayed packets (processed packets) according to the time mechanism.

After this function is enabled for the A2A VPN, the KS generates a pseudo timestamp (PTs) based on the GM and sends the pseudo timestamp and time-based anti-replay window (Tw) to GMs. During communication between GMs, the pseudo timestamp and time-based anti-replay window are used to prevent replayed packets. The detailed process is as follows:

1. When sending a packet, GM_1 adds the encryption time t1 to the encrypted packet. The formula for calculating t1 is as follows: t1 = Pseudo timestamp (PTs1) + Packet sending time (ts) - GM_1 registration time (tr1).
2. After receiving the packet, GM_2 generates the time t2, extracts the encryption time t1 from the packet, and compares t1 and t2. The formula for calculating t2 is as follows: t2 = Pseudo timestamp (PTs2) + Time when the packet is received (tsr) - GM_2 registration time (tr2). If the difference between t1 and t2 is within the range (-Tw to +Tw), the packet is accepted; otherwise, the packet is dropped.

Precautions

When the configuration is modified, the KS does not send rekey messages immediately until the TEK SA soft lifetime expires. To make the modified configuration take effect immediately, enter the **12.7.11 gdoi ks rekey** command to manually trigger the KS to send out rekey messages.

Example

Enable the time-based anti-replay function for the A2A VPN.

```
<Huawei> system-view
[Huawei] gdoi ks group gr1
[Huawei-gdoi-group-gr1] ipsec 2
[Huawei-gdoi-group-gr1-ipsec-2] anti-replay time-based enable
```

Related Topics

12.7.2 anti-replay time-based window

12.7.3 display gdoi ks group

12.7.2 anti-replay time-based window

 Copyright © Huawei Technologies Co., Ltd.

Function

The **anti-replay time-based window** command sets the size of the A2A VPN time-based anti-replay window.

The **undo anti-replay time-based window** command restores the size of the A2A VPN time-based anti-replay window to the default value.

The default size of the A2A VPN time-based anti-replay window is 5 seconds.

Format

anti-replay time-based window *seconds*

undo anti-replay time-based window

Parameters

Parameter	Description	Value
seconds	Specifies the size of the A2A VPN time-based anti-replay window.	The value is an integer that ranges from 1 to 100, in seconds.

Views

GDOI group IPSec policy view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the time-based anti-replay function is enabled, you can adjust the time-based anti-replay window size based on the actual scenario. For example, in the case of a large network delay, the service packets received by the receiver are regarded as replayed packets and thus are discarded. In this instance, you can disable the time-based anti-replay function or expand the anti-replay window size to prevent incorrect packet dropping.

Precautions

When the configuration is modified, the KS does not send rekey messages immediately until the TEK SA soft lifetime expires. To make the modified configuration take effect immediately, enter the **12.7.11 gdoi ks rekey** command to manually trigger the KS to send out rekey messages.

Example

Set the size of the A2A VPN time-based anti-replay window to 6 seconds.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> system-view
[Huawei] gdoi ks group gr1
[Huawei-gdoi-group-gr1] ipsec 2
[Huawei-gdoi-group-gr1-ipsec-2] anti-replay time-based window 6
```

Related Topics

12.7.1 anti-replay time-based enable

12.7.3 display gdoi ks group

12.7.3 display gdoi ks group

Function

The **display gdoi ks group** command displays configuration information about a GDOI group of a KS.

Format

display gdoi ks group [**brief** | **name** *group-name*]

Parameters

Parameter	Description	Value
brief	Displays brief configuration information about a given GDOI group.	-
name *group-name*	Displays detailed configuration information about a given GDOI group. If **name** is not specified, the configuration information about all GDOI groups is displayed.	The value must be the name of an existing GDOI group.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

When deploying the A2A VPN, you can run this command to check the configuration information about the GDOI groups of the KS, such as the group ID,

 Copyright © Huawei Technologies Co., Ltd.

encryption algorithm used for rekey messages, signature hash algorithm used for rekey messages, transmission mode of rekey messages, RSA key pair used for rekey messages, retransmission interval of rekey messages, number of times for retransmitting rekey messages, time-based anti-replay function, and anti-replay window size.

Example

Display brief configuration information about a GDOI group.

```
<Huawei> display gdoi ks group brief
Number of GDOI group : 1

GDOI group name                    identity number
------------------------------------------------------------
test                               33
```

Display configuration information about all GDOI groups.

```
<Huawei> display gdoi ks group
================================================
GDOI group: test
================================================
  Group identity number          : 10
  SA mode                        : normal
  Rekey encrypt algorithm        : AES-128
  Rekey sig-hash-algorithm       : SHA2-512
  Rekey transport type           : multicast
  Source address                 : 3.1.1.1
  Rekey destination address      : 239.0.1.2
  Rekey rsa key pair             : keytest
  Rekey lifetime (secs)          : 86400
  Rekey retry interval (secs)    : 10
  Rekey retry limit              : 3
  User-table                     : 10
  Local-id                       : -
  Local-id-type                  : ip
  Group policy numbers           : 1

  GDOI policy seq                : 5
   Proposal name                       : tran1
   Security acl                        : 3001
   SA lifetime (secs)                  : 3600
   Anti-replay time-based              : enable
   Anti-replay time-based window size(secs) : 5
```

Table 12-70 Description of the **display gdoi ks group** command output

Item	Description
Number of GDOI group	Number of GDOI groups.
GDOI group name/GDOI group	GDOI group name. To configure this parameter, run the **12.7.10 gdoi ks group** command.
identity number/Group identity number	GDOI group identity number. To configure this parameter, run the **12.7.13 group identity number** command.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
SA mode	SA mode: • receive-only: The GM sends only plaintext packets but can receive both plaintext and ciphertext packets. • normal: The GM sends and receives only ciphertext packets. To configure this parameter, run the **12.7.38 sa receive-only** command.
Rekey encrypt algorithm	Encryption algorithm used for rekey messages: • DES • 3DES • AES-128 • AES-192 • AES-256 To configure this parameter, run the **12.7.25 rekey encryption-algorithm** command.
Rekey sig-hash-algorithm	Signature hash algorithm used for rekey messages: • SHA1 • SHA2-256 • SHA2-384 • SHA2-512 To configure this parameter, run the **12.7.28 rekey sig-hash-algorithm** command.
Rekey transport type	Transmission mode of rekey messages: • unicast • multicast To configure this parameter, run the **12.7.29 rekey transport-type** command.
Source address	IP address of a KS. To configure this parameter, run the **12.7.40 source address (GDOI Group View)** command.
Rekey destination address	Destination IP address of rekey messages. To configure this parameter, run the **12.7.24 rekey destination address** command.

Copyright © Huawei Technologies Co., Ltd.

Item	Description
Rekey rsa key pair	RSA key pair used for rekey messages. To configure this parameter, run the **12.7.23 rekey authentication public-key rsa** command.
Rekey lifetime (secs)	KEK SA lifetime, in seconds. To configure this parameter, run the **12.7.27 rekey sa duration time-based** command.
Rekey retry interval (secs)	Interval for retransmitting rekey messages, in seconds. To configure this parameter, run the **12.7.26 rekey retry** command.
Rekey retry limit	Number of times for retransmitting rekey messages. To configure this parameter, run the **12.7.26 rekey retry** command.
User-table	IKE user table referenced in the GDOI group. To configure this parameter, run the **12.7.42 user-table (GDOI Group View)** command.
Local-id	Local ID used in A2A VPN negotiation. To configure this parameter, run the **12.7.21 local-id (GDOI Group View)** command.
Local-id-type	Local ID type used in A2A VPN negotiation: • fqdn: The local ID type used in A2A VPN negotiation is in the name format. • ip: The local ID type used in A2A VPN negotiation is in the IP address format. • user-fqdn: The local ID type used in A2A VPN negotiation is in the user +domain name format. To configure this parameter, run the **12.7.20 local-id-type (GDOI Group View)** command.
Group policy numbers	Number of GDOI IPSec policies.
GDOI policy seq	GDOI group IPSec policy sequence number. To configure this parameter, run the **12.7.15 ipsec** command.

Copyright © Huawei Technologies Co., Ltd.

Item	Description
Proposal name	IPSec proposal referenced in GDOI IPSec policies. To configure this parameter, run the **12.7.22 proposal (GDOI group IPSec policy View)** command.
Security acl	ACL referenced in GDOI IPSec policies. To configure this parameter, run the **12.7.39 security acl** command.
SA lifetime (secs)	TEK SA lifetime, in seconds. To configure this parameter, run the **12.7.37 sa duration time-based** command.
Anti-replay time-based	Time-based anti-replay function: • enable: The time-based anti-replay function is enabled. • disable: The time-based anti-replay function is disabled. To configure this parameter, run the **12.7.1 anti-replay time-based enable** command.
Anti-replay time-based window size (secs)	Size of the time-based anti-replay window, in seconds. To configure this parameter, run the **12.7.2 anti-replay time-based window** command.

12.7.4 display gdoi ks members

Function

The **display gdoi ks members** command displays information about GDOI group members of a KS.

Format

display gdoi ks members [**group** *group-name*]

Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
group *group-name*	Displays information about members in a specified GDOI group. If **group** is not specified, the information about members in all GDOI groups is displayed.	The value must be the name of an existing GDOI group.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After a GM registers with the KS successfully, you can run this command to view information about GDOI group members, such as the number of GMs, transmission mode of rekey messages, IP address of the GM, IP address of the KS, and sequence number of rekey messages.

Example

Display information about members in all GDOI groups of the KS.

```
<Huawei> display gdoi ks members
============================================
 GDOI group    : test
 GM number     : 1
 Rekey transport type          : unicast
============================================

  GM ID                      : 10.2.1.1
  Key server ID              : 10.3.1.1
  Current seq of rekey       : 0
  Acked seq of rekey         : 0
  Number of rekey sent       : 0
  Number of rekey unacked    : 0
```

Table 12-71 Description of the **display gdoi ks members** command output

Item	Description
GDOI group	GDOI group name. To configure this parameter, run the **12.7.10 gdoi ks group** command.
GM number	Number of GDOI group members.

Copyright © Huawei Technologies Co., Ltd.

Item	Description
Rekey transport type	Transmission mode of rekey messages: • unicast • multicast To configure this parameter, run the **12.7.29 rekey transport-type** command.
GM ID	IP address of the GM.
Key server ID	IP address of the KS. To configure this parameter, run the **12.7.40 source address (GDOI Group View)** command.
Current seq of rekey	Current sequence number of rekey messages.
Acked seq of rekey	Sequence number of unicast rekey ACK messages.
Number of rekey sent	Number of sent rekey messages.
Number of rekey unacked	Number of unicast rekey ACK messages that are not received.

Related Topics

12.7.31 reset gdoi ks members

12.7.5 display gdoi ks members history record

Function

The **display gdoi ks members history record** command displays historical information about GDOI group members of a KS.

Format

display gdoi ks members history record [**group** *group-name*]

Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
group *group-name*	Displays historical information about members in a specified GDOI group. If **group** is not specified, the historical information about members in all GDOI groups is displayed.	The value must be the name of an existing GDOI group.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

When a GM fails to register with the KS or goes offline abnormally, you can run this command to check the reason for quick fault location.

Example

Display historical information about members in all GDOI groups.

```
<Huawei> display gdoi ks members history record
================================================================================
GDOI GM history record:
remote address                  : 10.2.1.1
source address                  : 10.10.10.1
group name                      : test
group id                        : 33
offline reason                  : Failed to verify rekey ack message of a group member
offline time                    : 2018-05-28 10:06:43

================================================================================
GDOI GM history record:
remote address                  : 10.2.1.2
source address                  : 10.10.10.1
group name                      : test
group id                        : 33
register failure reason         : No TEK
register failure time           : 2018-05-28 11:06:43
```


Copyright © Huawei Technologies Co., Ltd.

Table 12-72 Description of the **display gdoi ks members history record** command output

Item	Description
GDOI GM history record	Historical information about a GM in a GDOI group.
remote address	IP address of the GM.
source address	IP address of the KS.
group name	GDOI group name.
group id	GDOI group ID.
offline reason	Reason why the GM goes offline. Failed to verify rekey ack message of a group member: Failed to verify the rekey ACK message of the GM.
offline time	Time when the GM goes offline.
register failure reason	Reason why the GM fails to register with the KS: • Can not find GDOI group: The GDOI group cannot be found. • Invalid hash_1 payload received: The KS receives an invalid hash payload. • Invalid group id received: The KS receives an invalid group ID. • Number of group members reached maximum: The number of GMs has reached the upper limit. • No KEK: The KEK SA does not exist. • No TEK: The TEK SA does not exist. • No permit rules: All rules in the ACL referenced by the KS are Deny. • Invalid hash_3 payload received: The KS receives an invalid hash payload. • Send sequence failed: Failed to send the sequence number payload of the KEK SA. • Invalid TEK key: The TEK key is invalid. • Invalid KEK key: The KEK key is invalid. • Deletion in progress: The GDOI group is being deleted.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
register failure time	Time when the GM fails to register with the KS.

Related Topics

12.7.32 reset gdoi ks members history record

12.7.6 display gdoi ks rekey statistics

Function

The **display gdoi ks rekey statistics** command displays statistics about the rekey messages on a KS.

Format

display gdoi ks rekey statistics [**group** *group-name*]

Parameters

Parameter	Description	Value
group *group-name*	Displays statistics about the rekey messages of a specified GDOI group. If **group** is not specified, statistics about the rekey messages of all GDOI groups are displayed.	The value must be the name of an existing GDOI group.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

When the KS performs rekey, you can run this command to view statistics about rekey messages received and sent by the KS, which helps you quickly locate faults.

Example

Display statistics about rekey messages of all GDOI groups.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> display gdoi ks rekey statistics
==============================================
GDOI group: test
==============================================
  Rekey transport type          : unicast
  Number of rekey sent          : 28
  Number of rekey retransmitted  : 21
  Number of rekey acked         : 0
  Number of rekey missed        : 13
```

Table 12-73 Description of the **display gdoi ks rekey statistics** command output

Item	Description
GDOI group	GDOI group name. To configure this parameter, run the **12.7.10 gdoi ks group** command.
Rekey transport type	Transmission mode of rekey messages: • unicast • multicast To configure this parameter, run the **12.7.29 rekey transport-type** command.
Number of rekey sent	Number of sent rekey messages.
Number of rekey retransmitted	Number of retransmitted rekey messages.
Number of rekey acked	Number of unicast rekey ACK messages.
Number of rekey missed	Number of discarded unicast rekey ACK messages.

Related Topics

12.7.33 reset gdoi ks rekey statistics

12.7.7 display gdoi ks sa

Function

The **display gdoi ks sa** command displays SA information about the GDOI groups of a KS.

Format

display gdoi ks sa [**group** *group-name*]

Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
group *group-name*	Displays SA information about a specified GDOI group. If **group** is not specified, the SA information about all GDOI groups is displayed.	The value must be the name of an existing GDOI group.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After a GM registers with the KS successfully, you can run this command to view the SA information about the GDOI groups of the KS, such as the group name, encryption algorithm used for rekey messages, signature hash algorithm used for rekey messages, transmission mode of rekey messages, RSA key pair used for rekey messages, KEK SA lifetime, TEK SA lifetime, time-based anti-replay function, and anti-replay window size.

Example

Display SA information about all GDOI groups.

```
<Huawei> display gdoi ks sa
============================================
GDOI group: bzh
============================================
  KEK SA
   SPI : 0x2ba0dacd87f2dd0a573a281e0599c65b
   Rekey transport type        : multicast
   Encrypt algorithm           : 3DES
   Encrypt iv length (bits)    : 64
   Encrypt key length (bits)   : 192
   Signature hash algorithm    : SHA1
   Signature key length (bits) : 4096
   Signature algorithm         : SIG_ALG_RSA
   Rekey current sequence      : 0
   Rekey next sequence         : 4
   SA lifetime (secs)          : 600
   SA remaining lifetime (secs): 104
   Next rekey time (secs)      : 34

  TEK SA
   SPI         : 3327227442 (0xc6517632)
   Security acl : 3001
   Proposal     : ESP-ENCRYPT-AES-256 ESP-AUTH-SHA2-256-128
   Encrypt key length (bits)   : 256
```

 Copyright © Huawei Technologies Co., Ltd.

```
Auth key length (bits)      : 256
Anti-replay (time-based)    : enable
Window size (secs)          : 99
Replay value (secs)         : 102813.30
SA lifetime (secs)          : 3600
SA remaining lifetime (secs): 391
Next rekey time (secs)      : 261
```

Table 12-74 Description of the **display gdoi ks sa** command output

Item	Description
GDOI group	GDOI group name. To configure this parameter, run the **12.7.10 gdoi ks group** command.
KEK SA	Information about the KEK SA.
SPI	SPI value of the KEK SA or TEK SA.
Rekey transport type	Transmission mode of rekey messages: • unicast • multicast To configure this parameter, run the **12.7.29 rekey transport-type** command.
Encrypt algorithm	Encryption algorithm. To configure this parameter, run the **12.7.25 rekey encryption-algorithm** command.
Encrypt iv length (bits)	Length of the encryption IV, in bits.
Encrypt key length (bits)	Length of the encryption key, in bits.
Signature hash algorithm	Signature hash algorithm: • SHA1 • SHA2-256 • SHA2-384 • SHA2-512 To configure this parameter, run the **12.7.28 rekey sig-hash-algorithm** command.
Signature key length (bits)	Length of the signature key, in bits.
Signature algorithm	Signature algorithm.
Rekey current sequence	Sequence number used by the current rekey message.
Rekey next sequence	Sequence number used by the next rekey message.

Copyright © Huawei Technologies Co., Ltd.

Item	Description
SA lifetime (secs)	KEK SA or TEK SA lifetime, in seconds. To configure this parameter, run the **12.7.27 rekey sa duration time-based** or **12.7.37 sa duration time-based** command.
SA remaining lifetime (secs)	Remaining lifetime of the KEK SA or TEK SA, in seconds.
Next rekey time (secs)	Next rekey time, in seconds.
TEK SA	Information about the TEK SA.
Security acl	ACL used in the TEK SA. To configure this parameter, run the **12.7.39 security acl** command.
Proposal	Algorithm of the IPSec proposal. To configure this parameter, run the **12.7.22 proposal (GDOI group IPSec policy View)** command.
Auth key length (bits)	Length of the authentication key, in bits.
Anti-replay (time-based)	Time-based anti-replay function: • enable: The time-based anti-replay function is enabled. • disable: The time-based anti-replay function is disabled. To configure this parameter, run the **12.7.1 anti-replay time-based enable** command.
Window size (secs)	Size of the time-based anti-replay window, in seconds. To configure this parameter, run the **12.7.2 anti-replay time-based window** command.
Replay value (secs)	Replay pseudo timestamp, in seconds.

Related Topics

12.7.30 reset gdoi ks group

12.7.8 display ipsec gdoi-policy

Function

The **display ipsec gdoi-policy** command displays GDOI policy information.

Copyright © Huawei Technologies Co., Ltd.

Format

display ipsec gdoi-policy [*policy-name* [*seq-number*]]

Parameters

Parameter	Description	Value
policy-name	Displays detailed information about the GDOI policy with a specified name. If *policy-name* is not specified, information about all GDOI policies is displayed.	The value must be an existing GDOI policy name.
seq-number	Displays information about the GDOI policy with a specified sequence number.	The value must be an existing GDOI policy sequence number.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After registering with the KS successfully, a GM obtains the TEK and KEK security policies from the KS, such as the data flow to be protected, SA mode, IPSec proposal, and encryption algorithm of rekey messages. You can run this command to view information about security policies or information about the locally-configured security policies.

Example

Display detailed GDOI policy information.

```
<Huawei> display ipsec gdoi-policy
==========================================
Gdoi policy group: "map1"
Using interface: GigabitEthernet1/0/0
==========================================
  Sequence number: 10
  Group identity : 10
  Qos pre-classify: Disable
  Qos group: -
  Key server ID  : 3.1.1.1(active)
  Peer name      : spub
  Local acl      :
```

 Copyright © Huawei Technologies Co., Ltd.

```
  GM reregister  : 2018-06-05 14:34:39
  Rekey received :
  Rekey received cumulative : 0
  Rekey received after register : 0
  Rekey ack sent : 0

  ACL Downloaded From KS 3.1.1.1:
   Protocol: 0/permit
   Flow source      : 10.1.1.0/255.255.255.0/0
   Flow destination : 10.1.2.0/255.255.255.0/0

  TEK POLICY:
   SA mode : normal
   SPI: 2529860581 (0x96ca9be5)
   Encapsulation mode: Tunnel
   Proposal : ESP-ENCRYPT-AES-128 ESP-AUTH-SHA2-256-128
   SA remaining lifetime (secs) : 3206
   Anti-replay (time based) : enable
   Window size (secs): 5
   Reply value (secs): 3689.31

  KEK POLICY:
   Rekey transport type        : multicast
   SPI: 0x2ad569a935d15b75174446fbb0feaf5b
   Received rekey seqno        : 100
   Lifetime (secs)             : 71733
   Encrypt algorithm           : AES
   Encrypt key size            : 128
   Signature hash algorithm    : HMAC_AUTH_SHA2_512
   Signature key length (bits) : 2160
   Signature algorithm         : SIG_ALG_RSA

==========================================
Gdoi policy group: "po1"
Shared interface: LoopBack0
Using interface: GigabitEthernet1/0/1
                 GigabitEthernet1/0/2
==========================================
  Sequence number: 10
  Group identity : 10
  Qos pre-classify: Disable
  Qos group: -
  Key server ID  : 3.1.1.1(active)
  Peer name      : spub
  Local acl      :

  GM reregister  : 2018-06-05 14:34:39
  Rekey received :
  Rekey received cumulative : 0
  Rekey received after register : 0
  Rekey ack sent : 0

  ACL Downloaded From KS 3.1.1.1:
   Protocol: 0/permit
   Flow source      : 10.1.1.0/255.255.255.0/0
   Flow destination : 10.1.2.0/255.255.255.0/0

  TEK POLICY:
   SA mode : normal
   SPI: 2529860581 (0x96ca9be5)
   Encapsulation mode: Tunnel
   Proposal : ESP-ENCRYPT-AES-128 ESP-AUTH-SHA2-256-128
   SA remaining lifetime (secs) : 3206
   Anti-replay (time based) : enable
   Window size (secs): 5
   Reply value (secs): 3689.31

  KEK POLICY:
   Rekey transport type        : multicast
```

 Copyright © Huawei Technologies Co., Ltd.

```
SPI: 0x2ad569a935d15b75174446fbb0feaf5b
Received rekey seqno        : 100
Lifetime (secs)             : 71733
Encrypt algorithm           : AES
Encrypt key size            : 128
Signature hash algorithm    : HMAC_AUTH_SHA2_512
Signature key length (bits) : 2160
Signature algorithm         : SIG_ALG_RSA
```

Table 12-75 Description of the **display ipsec gdoi-policy** command output

Item	Description
Gdoi policy group	Name of the GDOI policy group. To create a GDOI policy, run the **12.7.18 ipsec policy (system view)** command.
Shared interface	Multi-link shared interface. To configure a multi-link shared interface, run the **12.6.103 ipsec policy shared** command.
Using interface	Interface to which a GDOI policy is applied. To apply a GDOI policy to an interface, run the **12.7.19 ipsec policy (interface view)** command.
Sequence number	Sequence number of the applied IPSec policy. To create a GDOI policy, run the **12.7.18 ipsec policy (system view)** command.
Group identity	GDOI group ID.
Qos pre-classify	Whether to pre-extract original packet information: • Enable: Pre-extraction is enabled. • Disable: Pre-extraction is disabled. To enable pre-extraction, run the **12.6.132 qos pre-classify** command.
Qos group	QoS group to which A2A VPN packets belong. To configure a QoS group, run the **12.6.131 qos group** command.
Key server ID	IP address of the KS.
Peer name	Name of the referenced IKE peer. To create an IKE peer, run the **12.6.77 ike-peer** command.
Local acl	Number of a local ACL. To reference an ACL, run the **12.6.167 security acl** command.
GM reregister	Time at which a GM registers with the KS.

Copyright © Huawei Technologies Co., Ltd.

Item	Description
Rekey received	Time at which a GM receives rekey messages.
Rekey received cumulative	Total number of rekey messages received by a GM.
Rekey received after register	Number of rekey messages received by a GM after it registers with the KS.
Rekey ack sent	Number of responses to unicast rekey messages sent by a GM.
ACL Downloaded From KS	ACL downloaded from the KS by the GM.
Protocol	Number of the protocol data flows of which are protected by the SA.
Flow source	Source address of encryption data flows. ● The value 10.0.0.0 indicates the network segment address of the source IP address. ● The value 255.0.0.0 indicates the network mask. ● The value 0/0 indicates the ACL number and port number.
Flow destination	Destination address of encryption data flows. ● The value 10.1.0.0 indicates the network segment address of the destination IP address. ● The value 255.0.0.0 indicates the network mask. ● The value 0/0 indicates the ACL number and port number.
TEK POLICY	Policy for the traffic encryption key.
SA mode	TEK SA mode.
SPI	Security parameter index.
Encapsulation mode	TEK SA encapsulation mode. ● Tunnel: tunnel mode. ● Transport: transport mode.
Proposal	Encryption and authentication algorithms of A2A VPN Security proposal.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
SA remaining lifetime (secs)	Remaining lifetime of the TEK SA in seconds.
Anti-replay (time based)	Time-based anti-replay: • enable: The time-based anti-replay function is enabled. • disable: The time-based anti-replay function is disabled.
Window size (secs)	Size of the time-based anti-replay window, in seconds.
Reply value (secs)	Replay pseudo timestamp, in seconds.
KEK POLICY	Policy for key encryption key.
Rekey transport type	Type of the received rekey message. • unicast • multicast
Received rekey seqno	Received Rekey message sequence number.
Lifetime (secs)	Remaining lifetime of the KEK SA in seconds.
Encrypt algorithm	Encryption algorithm used in a GDOI policy.
Encrypt key size	Private key of the encryption algorithm.
Signature hash algorithm	Hash algorithm used to calculate a signature.
Signature key length (bits)	Private key length of the signature in bits.
Signature algorithm	Signature algorithm used in a GDOI policy.

12.7.9 display ipsec gdoi-sa

Function

The **display ipsec gdoi-sa** command displays GDOI SA information.

Format

display ipsec gdoi-sa [*policy-name* [*seq-number*]]

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
policy-name	Displays the SA established through a specified GDOI policy. If *policy-name* is not specified, all GDOI SA information is displayed.	The value must be an existing GDOI policy name.
seq-number	Specifies the sequence number of the GDOI policy.	The value must be an existing GDOI policy sequence number.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

When the TEK SA and KEK SA are generated by the GM, you can run this command to view information about the TEK SA and KEK SA, such as the data flows to be protected, inbound/outbound packet statistics, SA mode, transmission mode of rekey messages, encryption algorithm of rekey messages, and signature hash algorithm of rekey messages.

Example

Display detailed information about the SA established through a GDOI policy.

```
<Huawei> display ipsec gdoi-sa
==============================
Interface: GigabitEthernet1/0/0
 Path MTU: 1500
==============================
  ---------------------------------
  Gdoi policy name         : "map1"
  Sequence number          : 10
  ---------------------------------
    [TEK SA]
    Protected vrf : 0
    Protocol: 0/permit
    Flow source      : 10.1.1.0/255.255.255.0/0
    Flow destination : 10.1.2.0/255.255.255.0/0

    Inpacket count            : 0
    Inpacket decap count      : 0
    Outpacket count           : 0
    Outpacket encap count     : 0
    Inpacket drop count       : 0
    Outpacket drop count      : 0
    Anti-replay drop count    : 0
```

 Copyright © Huawei Technologies Co., Ltd.

```
  SA mode : normal
  SPI: 99152831 (0x5e8f3bf)
  Encapsulation mode: Tunnel
  Proposal : ESP-ENCRYPT-AES-128 ESP-AUTH-SHA2-256-128
  SA remaining lifetime (secs) : 2873
  Anti-replay (time based) : enable
  Window size (secs): 5
  Replay value (secs): 6342.88

  [KEK POLICY]
  Rekey transport type       : multicast
  SPI: 0x2ad569a935d15b75174446fbb0feaf5b
  Received rekey seqno       : 8
  Lifetime (secs)            : 81811
  Encrypt algorithm          : AES
  Encrypt key size           : 128
  Signature hash algorithm   : HMAC_AUTH_SHA2_512
  Signature key length (bits) : 2160
  Signature algorithm        : SIG_ALG_RSA

==============================
 Shared interface: LoopBack0
 Using interface: GigabitEthernet1/0/1
                  GigabitEthernet1/0/3
==============================
  --------------------------------
  Gdoi policy name        : "map1"
  Sequence number         : 10
  --------------------------------
  [TEK SA]
  Protected vrf : 0
  Protocol: 0/permit
  Flow source      : 10.1.1.0/255.255.255.0/0
  Flow destination : 10.1.2.0/255.255.255.0/0

  Inpacket count           : 0
  Inpacket decap count     : 0
  Outpacket count          : 0
  Outpacket encap count    : 0
  Inpacket drop count      : 0
  Outpacket drop count     : 0
  Anti-replay drop count   : 0

  SA mode : normal
  SPI: 99152831 (0x5e8f3bf)
  Encapsulation mode: Tunnel
  Proposal : ESP-ENCRYPT-AES-128 ESP-AUTH-SHA2-256-128
  SA remaining lifetime (secs) : 2873
  Anti-replay (time based) : enable
  Window size (secs): 5
  Replay value (secs): 6342.88

  [KEK POLICY]
  Rekey transport type       : multicast
  SPI: 0x2ad569a935d15b75174446fbb0feaf5b
  Received rekey seqno       : 8
  Lifetime (secs)            : 81811
  Encrypt algorithm          : AES
  Encrypt key size           : 128
  Signature hash algorithm   : HMAC_AUTH_SHA2_512
  Signature key length (bits) : 2160
  Signature algorithm        : SIG_ALG_RSA
```

 Copyright © Huawei Technologies Co., Ltd.

Table 12-76 Description of the **display ipsec gdoi-sa** command output

Item	Description
Interface	Interface to which a GDOI policy is applied. To apply a GDOI policy to an interface, run the **12.7.19 ipsec policy (interface view)** command.
Path MTU	MTU of the interface.
Shared interface	Multi-link shared interface. To configure a multi-link shared interface, run the **12.6.103 ipsec policy shared** command.
Using interface	Interface to which a GDOI policy is applied. To apply a GDOI policy to an interface, run the **12.7.19 ipsec policy (interface view)** command.
Gdoi policy name	Name of the applied GDOI policy. To create a GDOI policy, run the **12.7.18 ipsec policy (system view)** command.
Sequence number	Sequence number of the applied GDOI policy. To create a GDOI policy, run the **12.7.18 ipsec policy (system view)** command.
TEK SA	SA of the traffic encryption key.
Protected vrf	VPN instance protected by A2A VPN. To specify the VPN instance bound to A2A VPN, run the **sa binding vpn-instance** command.
Protocol	Number of the protocol data flows of which are protected by the SA.
Flow source	Source address of encryption data flows. • The value 10.1.1.0 indicates the network segment address of the source IP address. • The value 255.255.255.0 indicates the network mask. • The value 0/0 indicates the ACL number and port number.

Copyright © Huawei Technologies Co., Ltd.

Item	Description
Flow destination	Destination address of encryption data flows. • The value 10.1.2.0 indicates the network segment address of the destination IP address. • The value 255.255.255.0 indicates the network mask. • The value 0/0 indicates the ACL number and port number.
Inpacket count	Number of incoming Security packets.
Inpacket decap count	Number of times that the device decapsulates incoming packets.
Outpacket count	Number of outgoing Security packets.
Outpacket encap count	Number of times that the device encapsulates outgoing packets.
Inpacket drop count	Number of discarded incoming packets.
Outpacket drop count	Number of discarded outgoing packets.
Anti-replay drop count	Number of packets dropped during anti-replay.
SA mode	TEK SA mode.
SPI	Security parameter index.
Encapsulation mode	TEK SA encapsulation mode. • Tunnel: tunnel mode. • Transport: transport mode.
Proposal	Encryption and authentication algorithms of A2A VPN Security proposal.
SA remaining lifetime (secs)	Remaining lifetime of the TEK SA in seconds.
Anti-replay (time based)	Time-based anti-replay: • enable: The time-based anti-replay function is enabled. • disable: The time-based anti-replay function is disabled.
Window size (secs)	Size of the time-based anti-replay window, in seconds.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Replay value (secs)	Replay pseudo timestamp, in seconds.
KEK POLICY	Policy for the traffic encryption key.
Rekey transport type	Type of the received rekey message. • unicast • multicast
Received rekey seqno	Received Rekey message sequence number.
Lifetime (secs)	Remaining lifetime of the KEK SA in seconds.
Encrypt algorithm	Encryption algorithm used in a GDOI policy.
Encrypt key size	Private key length of the encryption algorithm.
Signature hash algorithm	Hash algorithm used by a signature.
Signature key length (bits)	Private key length of the signature in bits.
Signature algorithm	Signature algorithm used in a GDOI policy.

12.7.10 gdoi ks group

Function

The **gdoi ks group** command creates a GDOI group for a KS and displays the GDOI group view.

The **undo gdoi ks group** command deletes the ID of a GDOI group.

By default, no GDOI group is created for a KS.

Format

gdoi ks group *group-name*

undo gdoi ks group *group-name*

Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
group-name	Specifies the name of a GDOI group.	The value is a string of 1 to 31 case-sensitive characters, with the exception of spaces or question marks (?).

Views

System view

Default Level

2: Configuration level

Usage Guidelines

After registering with the KS successfully, a GM obtains the TEK and KEK policies from the KS that are configured in a GDOI group. For this reason, you need to run the **gdoi ks group** command first to create a GDOI group, and then set parameters for the GDOI group, such as the group ID, group IP address, IKE user table, signature algorithm and key pair of rekey messages, and GDOI IPSec policies.

Example

Create a GDOI group for the KS.

```
<Huawei> system-view
[Huawei] gdoi ks group gr1
[Huawei-gdoi-group-gr1]
```

Related Topics

12.7.3 display gdoi ks group

12.7.11 gdoi ks rekey

Function

The **gdoi ks rekey** command is used to manually trigger a KS to send rekey messages.

Format

gdoi ks rekey group *group-name*

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
group *group-name*	Specifies the name of a GDOI group.	The value must be the name of an existing GDOI group.

Views

User view

Default Level

3: Configuration level

Usage Guidelines

After modifying the configuration in a GDOI group, you can run this command to manually trigger the KS to send rekey messages without waiting for the KEK SA or TEK SA to age out.

Example

Manually trigger the KS to send rekey messages.

```
<Huawei> gdoi ks rekey group gr1
```

12.7.12 gdoi sa direction receive-option

Function

The **gdoi sa direction receive-option** command sets the SA mode to Receive_Option. In this mode, the device can receive both cipher text and plain text packets but can send only cipher text packets.

Format

gdoi sa direction receive-option

Parameters

None

Views

User view

Default Level

1: Monitoring level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

When you deploy A2A VPN on an existing network, a GM that has joined a group such as GM_1 can only send and receive cipher text packets, but the other GMs that have not joined the group can only send and receive plain text packets. In this case, the other GMs will discard encrypted packets from GM_1 because they cannot decrypt them, and GM_1 will discard plain text packets from the other GMs, resulting in service interruption. After you run this command on the GMs, A2A VPN can be deployed in several stages, preventing service interruption.

Example

Set the SA mode to Receive_Option.

```
<Huawei> gdoi sa direction receive-option
```

12.7.13 group identity number

Function

The **group identity number** command configures an ID for a GDOI group.

The **undo group identity number** command deletes the ID of a GDOI group.

By default, a GDOI group has no ID.

Format

group identity number { *group-number* | *ip-address* }

undo group identity number

Parameters

Parameter	Description	Value
group-number	Specifies the GDOI group ID.	The value is an integer that ranges from 0 to 4294967295.
ip-address	Specifies the IP address of the GDOI group.	The value is in dotted decimal notation.

Views

GDOI policy view, GDOI group view

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

Usage Scenario

You can run this command to configure an ID for a GDOI group in the A2A VPN. The KS determines the GDOI group to which a GM is to be added based on the group ID submitted by the GM.

Precautions

You can configure either a group ID or an IP address for a GDOI group at one time. If you run the command multiple times, only the latest configuration takes effect.

When the group ID for a GDOI group is modified, the GDOI group-related TEK SA and KEK SA are deleted. As a result, services between the KS and GM are interrupted until the GM re-registers with the KS after the TEK SA of the GM ages out.

Example

Configure an ID for a GDOI group in the GDOI policy view.
```
<Huawei> system-view
[Huawei] ipsec policy mypolicy 4 gdoi
[Huawei-ipsec-policy-gdoi-mypolicy-4] group identity number 10
```

Configure an ID for a GDOI group in the GDOI group view.
```
<Huawei> system-view
[Huawei] gdoi ks group gr1
[Huawei-gdoi-group-gr1] group identity number 10
```

12.7.14 ike-peer

Function

The **ike-peer** command references an IKE peer.

The **undo ike-peer** command cancels the configuration.

By default, no IKE peer is referenced.

Format

ike-peer *peer-name*

undo ike-peer

Parameters

Parameter	Description	Value
peer-name	Specifies the name of the referenced IKE peer.	The value must be an existing IKE peer name.

 Copyright © Huawei Technologies Co., Ltd.

Views

GDOI policy view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When you configure IKE negotiation, you need to reference an IKE peer in the specified view.

Prerequisites

An IKE peer has been created using the **ike peer** command in the system view.

Example

Reference the IKE peer **mypeer** in the GDOI policy.

```
<Huawei> system-view
[Huawei] ike peer mypeer
[Huawei-ike-peer-mypeer] quit
[Huawei] ipsec policy map2 4 gdoi
[Huawei-ipsec-policy-gdoi-map2-4] ike-peer mypeer
```

Related Topics

12.7.18 ipsec policy (system view)

12.7.15 ipsec

Function

The **ipsec** command creates a GDOI group IPSec policy and displays the GDOI group IPSec policy view.

The **undo ipsec** deletes the created GDOI group IPSec policy.

By default, no GDOI group IPSec policy is created.

Format

ipsec *policy-num*

undo ipsec *policy-num*

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
policy-num	Specifies the sequence number of a GDOI group IPSec policy.	The value is an integer that ranges from 1 to 65,535.

Views

GDOI group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After registering with the KS successfully, a GM receives the TEK policies pushed by the KS. The TEK policies are used for generating TEK SAs on the GMs to encrypt inter-GM data flows. To generate a TEK policy on the KS, you need to run the **ipsec** command to configure a GDOI group IPSec policy.

Follow-up Tasks

You need to set parameters for the GDOI group IPSec policy, for example, referencing the IPSec proposal and security ACL.

Precautions

When a GDOI group IPSec policy is added, the KS does not send rekey messages immediately until the TEK SA soft lifetime expires. To make the modified configuration take effect immediately, enter the **12.7.11 gdoi ks rekey** command to manually trigger the KS to send out rekey messages.

When the GDOI group IPSec policy is deleted, the KS immediately sends out rekey messages.

Example

Create a GDOI group IPSec policy and enter the GDOI group IPSec policy view.

```
<Huawei> system-view
[Huawei] gdoi ks group gr1
[Huawei-gdoi-group-gr1] ipsec 2
[Huawei-gdoi-group-gr1-ipsec-2]
```

Related Topics

12.7.3 display gdoi ks group

Copyright © Huawei Technologies Co., Ltd.

12.7.16 ipsec gdoi anti-replay force 32-bit enable

Function

The **ipsec gdoi anti-replay force 32-bit enable** command enables an A2A VPN Group Member (GM) device to use the least significant 32 bits of the timestamp to add a timestamp to encrypted packets.

The **undo ipsec gdoi anti-replay force 32-bit enable** command disables an A2A VPN GM device from using the least significant 32 bits of the timestamp to add a timestamp to encrypted packets.

By default, an A2A VPN GM device does not use the least significant 32 bits of the timestamp to add a timestamp to encrypted packets.

NOTE

This function is supported in V200R010C10 and later versions.

Format

ipsec gdoi anti-replay force 32-bit enable

undo ipsec gdoi anti-replay force 32-bit enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

When the device functions as an A2A VPN GM device to connect to a non-Huawei device, you need to run the **ipsec gdoi anti-replay force 32-bit enable** command to enable

the Huawei GM device to use the least significant 32 bits to add timestamps to encrypted packets, if the Key Server (KS) advertises 64-bit timestamps of encrypted packets but the non-Huawei GM device supports only 32-bit timestamps of encrypted packets. This command ensures normal interconnection with the non-Huawei device.

Example

Enable an A2A VPN GM device to use the least significant 32 bits of the timestamp to add a timestamp to encrypted packets.

```
<Huawei> system-view
[] ipsec gdoi anti-replay force 32-bit enable
```

 Copyright © Huawei Technologies Co., Ltd.

12.7.17 ipsec gdoi multicast-rekey ip

Function

The **ipsec gdoi multicast-rekey ip** command configures an IP address for multicast Rekey messages.

The **undo ipsec gdoi multicast-rekey ip** command deletes an IP address for multicast Rekey messages.

By default, no IP address is configured for multicast Rekey messages.

Format

ipsec gdoi multicast-rekey ip *ip-address*

undo ipsec gdoi multicast-rekey ip

Parameters

Parameter	Description	Value
ip-address	Specifies an IP address for multicast Rekey messages.	The value ranges from 224.0.1.0 to 239.255.255.255, in dotted decimal notation.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After an IP address for multicast Rekey messages is configured, GMs with this IP address and a UDP port number 848/4500 update TEK SAs or KEK SAs based on the multicast Rekey messages.

Precautions

The IP address for multicast Rekey messages configured on the GM must be the same as that configured on the KS.

After you configure this command, the following commands must be configured; otherwise, the configuration does not take effect.

- Run the **multicast routing-enable** command to enable the multicast routing function.

 Copyright © Huawei Technologies Co., Ltd.

- Run the **pim dm** command to enable the PIM-DM function on an interface.
- Run the **igmp static-group** command to configure a static multicast group on an interface.

Example

Set the IP address for multicast Rekey messages to 225.0.0.1.

```
<Huawei> system-view
[Huawei] ipsec gdoi multicast-rekey ip 225.0.0.1
```

12.7.18 ipsec policy (system view)

Function

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

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

By default, no IPSec policy is configured.

Format

ipsec policy *policy-name seq-number* **gdoi**

undo ipsec policy *policy-name* [*seq-number*]

Parameters

Parameter	Description	Value
policy-name	Specifies the name of an IPSec policy.	The value is a string of 1 to 15 case-sensitive characters without question marks (?) or spaces.
seq-number	Specifies the sequence number of an IPSec policy.	The value is an integer that ranges from 1 to 4. A smaller value indicates a higher IPSec policy priority.
gdoi	Indicates that an IPSec SA is established in GDOI mode.	-

Views

System view

 Copyright © Huawei Technologies Co., Ltd.

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

An IPSec policy is a prerequisite to creating SAs and determines the methods used to protect specified data flows. An IPSec policy is identified by its name and sequence number, and multiple IPSec policies with the same IPSec policy name constitute an IPSec policy group.

On an A2A VPN network with many branches, a large number of multicast services need to be encrypted; therefore, the IPSec policy in GDOI mode is recommended.

Follow-up Procedure

Define negotiated IPSec parameters in the IPSec policy view and run the **ipsec policy (interface view)** command to apply the IPSec policy to an interface.

Example

Create an IPSec policy **policy1** whose sequence number is 3, and set the SA creation mode to GDOI.

```
<Huawei> system-view
[Huawei] ipsec policy policy1 3 gdoi
[Huawei-ipsec-policy-gdoi-policy1-3]
```

Related Topics

12.7.19 ipsec policy (interface view)

12.7.39 security acl

12.7.14 ike-peer

12.7.8 display ipsec gdoi-policy

12.7.19 ipsec policy (interface view)

Function

The **ipsec policy** command applies an IPSec policy group to an interface.

The **undo ipsec policy** command deletes the IPSec policy group from an interface so that it is no longer protected by IPSec.

By default, no IPSec policy is applied to an interface.

Format

ipsec policy *policy-name*

undo ipsec policy

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
policy-name	Specifies the name of the IPSec policy applied to an interface.	The value must be an existing IPSec policy name.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To protect data flows from an A2A VPN network on an interface, you need to apply a GDOI policy group to the interface. If the GDOI policy group is deleted from the interface, the interface no longer provides the encryption protection function.

After a GDOI policy group is applied to an interface, all GDOI policies in the group are applied to the interface to protect different data flows.

When sending a data flow, an interface matches the data flow with the GDOI policies in the GDOI policy group in ascending order of sequence numbers. If the data flow matches an ACL rule in a GDOI policy, the interface processes the data flow according to the GDOI policy; if the data flow does not match an ACL rule, the interface matches the data flow with another GDOI policy; if the data flow does not match any ACL rule in all the GDOI policies, the interface forwards the data flow directly without encryption protection.

Precautions

Only one GDOI policy group can be applied on an interface. A GDOI policy group can be applied to only one interface. To apply a new GDOI policy group to the interface, remove the previous one first.

In a GDOI policy group, if multiple policies are bound to different IKE peers, the remote addresses specified in the IKE peers cannot be the same. Otherwise, IKE negotiation of some GDOI policies fails.

Example

Bind an GDOI policy group named **policy1** to GE 1/0/2.

```
<Huawei> system-view
[Huawei] ipsec policy policy1 1 gdoi
[Huawei-ipsec-policy-isakmp-policy1-1] quit
[Huawei] interface gigabitethernet 1/0/2
[Huawei-Gigabitethernet1/0/2] ipsec policy policy1
```

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

12.7.18 ipsec policy (system view)

12.7.20 local-id-type (GDOI Group View)

Function

The **local-id-type** command sets the local ID type for a GDOI group.

The **undo local-id-type** command restores the default local ID type of a GDOI group.

The default local ID type of a GDOI group is in the IP address format.

Format

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

undo local-id-type

Parameters

Parameter	Description	Value
fqdn	Sets the local ID type used in IKE negotiation to the name format.	-
ip	Sets the local ID type used in IKE negotiation to the IP address format.	-
user-fqdn	Sets the local ID type used in IKE negotiation to the user +domain name format.	-

Views

GDOI group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Identity authentication is a self-protection mechanism for A2A VPN negotiation. It ensures security by confirming the identities of both communication parties. The identity types for the KS and GM can be different. You can use this command to set the identity type of the local end in a GDOI group, which is also called the local ID type.

Precautions

In pre-shared key authentication, the local ID type and local ID set for the local end must be the same as the peer ID type and peer ID set for the peer end.

 Copyright © Huawei Technologies Co., Ltd.

The method of setting the local ID type and local ID varies according to the identity authentication mode, as shown in **Table 12-77**.

Table 12-77 Relationship between the identity authentication mode, local ID type, and local ID

Authentication Mode	IP	FQDN	User-FQDN
Pre-shared key authentication (**pre-share**)	Supported The IP address is set using the **12.7.40 source address (GDOI Group View)** command.	Supported The ID is set using the **12.7.21 local-id (GDOI Group View)** command, indicating that this ID is used for identity authentication.	Supported The ID is set using the **12.7.21 local-id (GDOI Group View)** command, indicating that this ID is used for identity authentication.
RSA signature authentication (**rsa-signature**)	Not supported	Not supported	Not supported

Example

Set the local ID type of a GDOI group to the name format.

```
<Huawei> system-view
[Huawei] gdoi ks group gr1
[Huawei-gdoi-group-gr1] local-id-type fqdn
```

Related Topics

12.7.21 local-id (GDOI Group View)

12.7.3 display gdoi ks group

12.7.21 local-id (GDOI Group View)

Function

The **local-id** command specifies a local ID for a GDOI group.

The **undo local-id** command deletes the local ID of a GDOI group.

By default, no local ID is specified for a GDOI group.

Format

local-id *id*

undo local-id

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
id	Specifies the local ID of a GDOI group.	The value is a string of 1 to 255 case-sensitive characters, with the exception of question marks (?).

Views

GDOI group view

Default Level

2: Configuration level

Usage Guidelines

When using the **12.7.20 local-id-type (GDOI Group View)** command to set the local ID type to FQDN or user-FQDN, you also need to run the **local-id** command to specify a local ID, which is used for identity authentication.

Example

Set the local ID of a GDOI group to **huawei**.

```
<Huawei> system-view
[Huawei] gdoi ks group gr1
[Huawei-gdoi-group-gr1] local-id huawei
```

Related Topics

12.7.20 local-id-type (GDOI Group View)

12.7.3 display gdoi ks group

12.7.22 proposal (GDOI group IPSec policy View)

Function

The **proposal** command references an IPSec proposal in a GDOI group IPSec policy.

The **undo proposal** command cancels the preceding configuration.

By default, no IPSec proposal is referenced in a GDOI group IPSec policy.

Format

proposal *proposal-name*

undo proposal

 Copyright © Huawei Technologies Co., Ltd.

Parameters

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

Views

GDOI group IPSec policy view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After using the **12.7.15 ipsec** command to create a GDOI group IPSec policy, you need to configure an IPSec proposal to define the IPSec protection method, for example, an encryption/authentication algorithm. The IPSec proposal takes effect only after being referenced in the GDOI group IPSec policy. After registering with the KS successfully, a GM obtains the IPSec proposal from the KS for further negotiating TEK SA establishment with other GMs.

Prerequisites

An IPSec proposal has been configured using the **12.6.109 ipsec proposal** command.

Precautions

The A2A VPN supports only the ESP protocol and the tunnel encapsulation mode.

When the IPSec proposal is modified, the KS does not send rekey messages immediately until the TEK SA soft lifetime expires. To make the modified configuration take effect immediately, enter the **12.7.11 gdoi ks rekey** command to manually trigger the KS to send out rekey messages.

When the IPSec proposal is added or deleted, the KS sends rekey messages immediately.

Example

Set an IPSec proposal named **prop1**, and reference this proposal to a GDOI group IPSec policy.

```
<Huawei> system-view
[Huawei] ipsec proposal prop1
[Huawei-ipsec-proposal-prop1] quit
[Huawei] gdoi ks group gr1
[Huawei-gdoi-group-gr1] ipsec 2
[Huawei-gdoi-group-gr1-ipsec-2] proposal prop1
```

Related Topics

12.7.3 display gdoi ks group

 Copyright © Huawei Technologies Co., Ltd.

12.7.23 rekey authentication public-key rsa

Function

The **rekey authentication public-key rsa** command configures an RSA key pair used by rekey messages.

The **undo rekey authentication public-key rsa** command deletes the RSA key pair used by rekey messages.

By default, no RSA key pair is configured for rekey messages.

Format

rekey authentication public-key rsa *key-pair-name*

undo rekey authentication public-key rsa

Parameters

Parameter	Description	Value
key-pair-name	Specifies the RSA key pair name.	The value must be an existing RSA key pair name.

Views

GDOI group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

For security purposes, the KS signs the encrypted rekey messages. That is, the KS uses its own RSA private key to encrypt the data obtained using the hash algorithm from the encrypted rekey messages. After receiving the rekey messages, GMs use the RSA public key, hash algorithm, and encryption algorithm of the KS to decrypt them. The RSA public key, hash algorithm, and encryption algorithm are sent by the KS to registered GMs.

You can run the **rekey authentication public-key rsa** command to configure an RSA key pair used by rekey messages.

Prerequisite

An RSA key pair has been created using the **19.17.106 pki rsa local-key-pair create** command, or an RSA key pair has been imported to the device memory using the **19.17.95 pki import rsa-key-pair** command.

Copyright © Huawei Technologies Co., Ltd.

Precautions

When the configuration is modified, the KS does not send rekey messages immediately until the KEK SA soft lifetime expires. To make the modified configuration take effect immediately, enter the **12.7.11 gdoi ks rekey** command to manually trigger the KS to send out rekey messages.

Example

Configure an RSA key pair used by rekey messages.

```
<Huawei> system-view
[Huawei] pki rsa local-key-pair create keytest modulus 2048 exportable
 Info: The name of the new key-pair will be: keytest
 Generating key-pairs...
.+++
.....+++
[Huawei] gdoi ks group gr1
[Huawei-gdoi-group-gr1] rekey authentication public-key rsa keytest
```

Related Topics

12.7.3 display gdoi ks group

12.7.24 rekey destination address

Function

The **rekey destination address** command configures a destination IP address used by multicast rekey messages.

The **undo rekey destination address** command deletes the destination IP address used by multicast rekey messages.

By default, no destination IP address is configured for multicast rekey messages.

Format

rekey destination address *ip-address*

undo rekey destination address

Parameters

Parameter	Description	Value
ip-address	Specifies the destination IP address used by multicast rekey messages.	The value is in dotted decimal notation in a range from 224.0.0.0 to 239.255.255.255, excluding reserved multicast addresses.

Copyright © Huawei Technologies Co., Ltd.

Views

GDOI group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In multicast rekey mode, a GM registers with the KS and joins a specific multicast group. The KS sends rekey messages to all the GMs that join the group in multicast mode. In this scenario, you need to run the **rekey destination address** command to configure a destination IP address used by rekey messages in advance. Otherwise, the KS cannot send multicast rekey messages.

Precautions

When the configuration is modified, the KS does not send rekey messages immediately until the KEK SA soft lifetime expires. To make the modified configuration take effect immediately, enter the **12.7.11 gdoi ks rekey** command to manually trigger the KS to send out rekey messages.

Example

Set the destination IP address of multicast rekey messages to 239.10.1.1.

```
<Huawei> system-view
[Huawei] gdoi ks group gr1
[Huawei-gdoi-group-gr1] rekey destination address 239.10.1.1
```

Related Topics

12.7.3 display gdoi ks group

12.7.25 rekey encryption-algorithm

Function

The **rekey encryption-algorithm** command configures an encryption algorithm for rekey messages.

The **undo rekey encryption-algorithm** command restores the default encryption algorithm used by rekey messages.

The default encryption algorithm used by rekey messages is AES-256.

Format

rekey encryption-algorithm { **des** | **3des** | **aes-128** | **aes-192** | **aes-256** }

undo rekey encryption-algorithm

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
des	Specifies the 56-bit DES-CBC encryption algorithm.	-
3des	Specifies the 168-bit 3DES-CBC encryption algorithm.	-
aes-128	Specifies the 128-bit AES-CBC encryption algorithm.	-
aes-192	Specifies the 192-bit AES-CBC encryption algorithm.	-
aes-256	Specifies the 256-bit AES-CBC encryption algorithm.	-

Views

GDOI group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

For security purposes, the KS signs the encrypted rekey messages. That is, the KS uses its own RSA private key to encrypt the data obtained using the hash algorithm from the encrypted rekey messages. After receiving the rekey messages, GMs use the RSA public key, hash algorithm, and encryption algorithm of the KS to decrypt them. The RSA public key, hash algorithm, and encryption algorithm are sent by the KS to registered GMs.

You can run the **rekey encryption-algorithm** command to configure the encryption algorithm for rekey messages.

Precautions

The DES and 3DES algorithms are not secure and therefore not recommended.

When the configuration is modified, the KS does not send rekey messages immediately until the KEK SA soft lifetime expires. To make the modified configuration take effect immediately, enter the **12.7.11 gdoi ks rekey** command to manually trigger the KS to send out rekey messages.

Copyright © Huawei Technologies Co., Ltd.

Example

Set the encryption algorithm for rekey messages to AES-192.

```
<Huawei> system-view
[Huawei] gdoi ks group gr1
[Huawei-gdoi-group-gr1] rekey encryption-algorithm aes-192
```

Related Topics

12.7.3 display gdoi ks group

12.7.26 rekey retry

Function

The **rekey retry** command configures the number of retransmissions and retransmission interval for rekey messages.

The **undo rekey retry** command restores the default number of retransmissions and retransmission interval of rekey messages.

By default, the number of retransmissions of rekey messages is 3 and the retransmission interval is 10 seconds.

Format

rekey retry limit *limit* **interval** *interval*

undo rekey retry

Parameters

Parameter	Description	Value
limit *limit*	Specifies the number of times for retransmitting rekey messages.	The value is an integer that ranges from 1 to 6.
interval *interval*	Specifies the interval at which rekey messages are retransmitted.	The value is an integer that ranges from 5 to 20, in seconds.

Views

GDOI group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

 Copyright © Huawei Technologies Co., Ltd.

After a GM registers with the KS successfully, the KS periodically sends rekey messages to the GM to update the TEK and KEK policies. When the network is unstable, the GM fails to receive rekey messages and thereby cannot update these policies in a timely manner, causing service interruption.

To solve this problem, the A2A VPN provides a mechanism for retransmitting rekey messages.

- Unicast rekey

  If the KS does not receive a response from the GM within a specified period after sending a rekey message, the KS retransmits the rekey message until the number of retransmissions reaches the specified value.
- Multicast rekey

  After sending a rekey message, the KS periodically retransmits it until the number of retransmissions reaches the specified value.

You can run the **rekey retry** command to change the number of retransmissions and retransmission interval of rekey messages based on actual scenarios. For example, you can increase the number of retransmissions when network congestion occurs.

Precautions

When the configuration is modified, the KS does not send rekey messages immediately until the KEK SA soft lifetime expires. To make the modified configuration take effect immediately, enter the **12.7.11 gdoi ks rekey** command to manually trigger the KS to send out rekey messages.

Example

Set the number of retransmissions of rekey messages to 4 and the retransmission interval to 8 seconds.

```
<Huawei> system-view
[Huawei] gdoi ks group gr1
[Huawei-gdoi-group-gr1] rekey retry limit 4 interval 8
```

Related Topics

12.7.3 display gdoi ks group

12.7.27 rekey sa duration time-based

Function

The **rekey sa duration time-based** command configures the KEK SA hard lifetime.

The **undo rekey sa duration time-based** command restores the default KEK SA hard lifetime.

The default KEK SA hard lifetime is 86,400 seconds.

Format

rekey sa duration time-based *seconds*

 Copyright © Huawei Technologies Co., Ltd.

undo rekey sa duration time-based

Parameters

Parameter	Description	Value
seconds	Specifies the KEK SA hard lifetime.	The value is an integer that ranges from 600 to 604,800, in seconds.

Views

GDOI group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The KEK SA lifetime is used to periodically update the KEK SA, which reduces the risk of KEK SA cracking and improves security.

The KEK SA lifetime falls into the following types:

- Hard lifetime (hard timeout period): defines the number of seconds until the KEK SA expires.
- Soft lifetime (soft timeout period): defines the number of seconds until the IKE process is informed that the KEK SA is about to expire. This is to provide enough time for the creation of a new KEK SA before the hard lifetime is reached.

When the soft lifetime expires, the KS generates a new KEK SA and sends it to GMs through rekey messages. After receiving the rekey messages, GMs delete the old KEK SA and use the new one when the hard lifetime expires.

The value of the soft lifetime is related to the transmission mode, number of retransmissions, and retransmission interval of rekey messages. **Table 12-78** shows the detailed calculation methods.

Table 12-78 Soft lifetime values

Transmission Mode of Rekey Messages	Soft Lifetime Value
Unicast rekey	Hard lifetime - (30 + (Number of retransmissions + 1) x Retransmission interval + 5 x Number of GMs in the group/50)

 Copyright © Huawei Technologies Co., Ltd.

Transmission Mode of Rekey Messages	Soft Lifetime Value
Multicast rekey	Hard lifetime - (30 + (Number of retransmissions + 1) x Retransmission interval)

Precautions

When the configuration is modified, the KS does not send rekey messages immediately until the KEK SA soft lifetime expires. To make the modified configuration take effect immediately, enter the **12.7.11 gdoi ks rekey** command to manually trigger the KS to send out rekey messages.

Example

Set the KEK SA hard lifetime to 3600 seconds.

```
<Huawei> system-view
[Huawei] gdoi ks group gr1
[Huawei-gdoi-group-gr1] rekey sa duration time-based 3600
```

Related Topics

12.7.3 display gdoi ks group

12.7.28 rekey sig-hash-algorithm

Function

The **rekey sig-hash-algorithm** command configures the signature hash algorithm for rekey messages.

The **undo rekey sig-hash-algorithm** command restores the default signature hash algorithm for rekey messages.

The default signature hash algorithm for rekey messages is SHA2-256.

Format

rekey sig-hash-algorithm { **sha1** | **sha2-256** | **sha2-384** | **sha2-512** }

undo rekey sig-hash-algorithm

Parameters

Parameter	Description	Value
sha1	Sets the signature hash algorithm for rekey messages to SHA1.	-

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
sha2-256	Sets the signature hash algorithm for rekey messages to SHA2-256.	-
sha2-384	Sets the signature hash algorithm for rekey messages to SHA2-384.	-
sha2-512	Sets the signature hash algorithm for rekey messages to SHA2-512.	-

Views

GDOI group view

Default Level

2: Configuration level

Usage Guidelines

For security purposes, the KS signs the encrypted rekey messages. That is, the KS uses its own RSA private key to encrypt the data obtained using the hash algorithm from the encrypted rekey messages. After receiving the rekey messages, GMs use the RSA public key, hash algorithm, and encryption algorithm of the KS to decrypt them. The RSA public key, hash algorithm, and encryption algorithm are sent by the KS to registered GMs.

You can run the **rekey sig-hash-algorithm** command to configure the signature hash algorithm for rekey messages.

Precautions

The SHA1 algorithm is not secure and therefore not recommended.

When the KS connects to a GM, you need to confirm the signature hash algorithm supported by the GM. For example, the GM running a software version earlier than V200R010C00 supports only the SHA1 algorithm.

When the configuration is modified, the KS does not send rekey messages immediately until the KEK SA soft lifetime expires. To make the modified configuration take effect immediately, enter the **12.7.11 gdoi ks rekey** command to manually trigger the KS to send out rekey messages.

Example

Set the signature hash algorithm for rekey messages to SHA2-384.

```
<Huawei> system-view
[Huawei] gdoi ks group gr1
[Huawei-gdoi-group-gr1] rekey sig-hash-algorithm sha2-384
```

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

12.7.3 display gdoi ks group

12.7.29 rekey transport-type

Function

The **rekey transport-type** command configures the transmission mode of rekey messages.

The **undo rekey transport-type** command restores the default transmission mode of rekey messages.

The default transmission mode of rekey messages is multicast.

Format

rekey transport-type { **multicast** | **unicast** }

undo rekey transport-type

Parameters

Parameter	Description	Value
multicast	Sets the transmission mode to multicast.	-
unicast	Sets the transmission mode to unicast.	-

Views

GDOI group view

Default Level

2: Configuration level

Usage Guidelines

After GMs register with the KS, the KS periodically sends new TEK SAs or KEK SAs to GMs through rekey messages to improve security. A rekey message carries parameters such as information about the data flows to be protected, encryption algorithm, key, and SA lifetime.

The KS supports two modes for transmitting rekey messages:

- Multicast mode

  The KS sends rekey messages to GMs in the multicast group using the multicast address as the destination IP address. After successfully registering with the KS, GMs join a specific multicast group. All GMs in the group will receive the rekey messages.

 Copyright © Huawei Technologies Co., Ltd.

In multicast mode, GM entries on the KS do not age. If a GM keeps changing its IP address to register with the KS, the number of GM entries on the KS exceeds the maximum value. As a result, new GMs cannot register with the KS. In this instance, you need to run the **12.7.30 reset gdoi ks group** command to clear GM entries.

- Unicast mode

  The KS sends a rekey message to each GM using the GM address as the destination IP address. After receiving the rekey message, each GM sends an ACK message to the KS. The KS updates the current active GM list based on the received ACK messages and sends rekey messages only to active GMs.

  In unicast mode, the KS sends a rekey message to each GM. If there are too many GMs that may bring heavy load to the KS, the multicast mode is recommended.

Precautions

When the configuration is modified, the KS does not send rekey messages immediately until the KEK SA soft lifetime expires. To make the modified configuration take effect immediately, enter the **12.7.11 gdoi ks rekey** command to manually trigger the KS to send out rekey messages.

Example

Set the transmission mode of rekey messages to unicast.

```
<Huawei> system-view
[Huawei] gdoi ks group gr1
[Huawei-gdoi-group-gr1] rekey transport-type unicast
```

Related Topics

12.7.3 display gdoi ks group

12.7.30 reset gdoi ks group

Function

The **reset gdoi ks group** command clears the TEK SA and KEK SA related to a given GDOI group of a KS.

Format

reset gdoi ks group *group-name*

Parameters

Parameter	Description	Value
group *group-name*	Specifies the name of a GDOI group.	The value must be the name of an existing GDOI group.

 Copyright © Huawei Technologies Co., Ltd.

Views

User view

Default Level

3: Configuration level

Usage Guidelines

After this command is executed, the TEK SA and KEK SA related to a given GDOI group of the KS are deleted. As a result, services between the KS and GM are interrupted until the GM re-registers with the KS after the TEK SA of the GM ages out.

Example

Clear the TEK SA and KEK SA related to a KS GDOI group.

```
<Huawei> reset gdoi ks group gr1
```

Related Topics

12.7.7 display gdoi ks sa

12.7.31 reset gdoi ks members

Function

The **reset gdoi ks members** command clears statistics about GDOI group members of a KS.

Format

reset gdoi ks members group *group-name*

Parameters

Parameter	Description	Value
group *group-name*	Specifies the name of a GDOI group.	The value must be the name of an existing GDOI group.

Views

User view

Default Level

3: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

NOTE

After this command is executed, cleared statistics cannot be restored.

When diagnosing and locating GM registration problems, you can collect statistics only within a given length of time for fault location. You need to run the **reset gdoi ks members** command to clear historical GDOI group member statistics before statistics collection, and then run the **12.7.4 display gdoi ks members** command to view the current statistics about GDOI group members.

Example

Clear statistics about GDOI group members of a KS.

```
<Huawei> reset gdoi ks members group gr1
```

12.7.32 reset gdoi ks members history record

Function

The **reset gdoi ks members history record** command clears historical information about the GDOI group members of a KS.

Format

reset gdoi ks members history record [**group** *group-name*]

Parameters

Parameter	Description	Value
group *group-name*	Specifies the name of a GDOI group. If **group** is not specified, the historical information about members in all GDOI groups is cleared.	The value must be the name of an existing GDOI group.

Views

User view

Default Level

3: Configuration level

Usage Guidelines

NOTE

After this command is executed, cleared statistics cannot be restored.

When diagnosing and locating a GM registration failure or abnormal logout, you can collect statistics only within a given length of time for fault location. You need

 Copyright © Huawei Technologies Co., Ltd.

to run the **reset gdoi ks members history record** command to clear historical statistics before statistics collection, and then run the **12.7.6 display gdoi ks rekey statistics** command to view the current statistics about the rekey messages on the KS.

Example

Clear historical information about the GMs in GDOI group **gr1**.

```
<Huawei> reset gdoi ks members history record group gr1
```

12.7.33 reset gdoi ks rekey statistics

Function

The **reset gdoi ks rekey statistics** command clears statistics about the rekey messages on a KS.

Format

reset gdoi ks rekey statistics [**group** *group-name*]

Parameters

Parameter	Description	Value
group *group-name*	Specifies the name of a GDOI group. If **group** is not specified, statistics about the rekey messages of all GDOI groups are cleared.	The value must be the name of an existing GDOI group.

Views

User view

Default Level

3: Configuration level

Usage Guidelines

NOTE

After this command is executed, cleared statistics cannot be restored.

When diagnosing and locating rekey messages problems, you can collect statistics only within a given length of time for fault location. You need to run the **reset gdoi ks rekey statistics** command to clear historical statistics before statistics collection, and then run the **12.7.6 display gdoi ks rekey statistics** command to view the current statistics about the rekey messages on the KS.

 Copyright © Huawei Technologies Co., Ltd.

Example

Clear statistics about the rekey messages of GDOI group **gr1**.

```
<Huawei> reset gdoi ks rekey statistics group gr1
```

12.7.34 qos group

Function

The **qos group** command configures the QoS group to which the IPSec packets belong.

The **undo qos group** command deletes the QoS group to which the IPSec packets belong.

By default, no QoS group is configured.

Format

qos group *qos-group-value*

undo qos group

Parameters

Parameter	Description	Value
qos-group-value	Specifies the ID of the QoS group.	The value is an integer that ranges from 1 to 99.

Views

Manual IPSec policy view, IPSec policy view, IPSec policy template view, IPSec profile view, Efficient VPN policy view, GDOI policy view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When both an IPSec policy and a QoS policy are used on an interface, you can run this command to specify the QoS group to which the IPSec packets belong to facilitate QoS management.

Precautions

This command takes effect in the packet encapsulation process but not the packet decapsulation process. That is, the command takes effect only for incoming packets.

Follow-up Procedure

 Copyright © Huawei Technologies Co., Ltd.

After QoS for IPSec packets is enabled, run the **if-match qos-group** *qos-group-value* command in the traffic classifier view to configure a matching rule based on the QoS group.

Example

Configure the QoS group to which the IPSec packets belong in the IPSec policy view.

```
<Huawei> system-view
[Huawei] ipsec policy policy1 10 isakmp
[Huawei-ipsec-policy-isakmp-policy1-10] qos group 30
```

Related Topics

12.6.104 ipsec policy (interface view)
12.6.106 ipsec policy-template
12.6.107 ipsec profile (interface view)
12.6.98 ipsec efficient-vpn (system view)

12.7.35 qos pre-classify

Function

The **qos pre-classify** command enables pre-extraction of original IP packets.

The **undo qos pre-classify** command disables pre-extraction of original IP packets.

By default, pre-extraction of original IP packets is disabled.

Format

qos pre-classify

undo qos pre-classify

Parameters

None

Views

Tunnel interface view, Efficient VPN policy view, Manual IPSec policy view, IPSec policy view, IPSec policy template view, IPSec profile view, GDOI policy view, BD view, VBDIF interface view, VPN instance view, Virtual template interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In tunnel mode, QoS parameters such as the packet header and protocol type in original packets are hidden after IP packets are encapsulated through GRE,

 Copyright © Huawei Technologies Co., Ltd.

VXLAN, L2TP, and IPSec. Although GRE, VXLAN, L2TP, and IPSec uses the DSCP field in original packets as the DSCP field in the IP packet header, some QoS solutions require quintuple information. The encryption device can pre-extract quintuple information including the source address, destination address, protocol type, source port number, and destination port number to facilitate refined QoS management on GRE, VXLAN, L2TP, and IPSec packets.

In an A2A VPN solution, the device uses the IP header of original packets as the IP header for encapsulated A2A VPN packets. Therefore, you do not need to configure this command if the device classifies packets based on the source address, destination address, or protocol type only.

Follow-up Procedure

After pre-extraction of original IP packets is enabled, run the **if-match acl** { *acl-number* | *acl-name* } command in the traffic classifier view to configure a matching rule based on the ACL.

Example

Enable pre-extraction of original IP packets in the IPSec policy view.

```
<Huawei> system-view
[Huawei] ipsec policy policy1 10 isakmp
[Huawei-ipsec-policy-isakmp-policy1-10] qos pre-classify
```

Related Topics

12.6.104 ipsec policy (interface view)

12.6.106 ipsec policy-template

12.6.107 ipsec profile (interface view)

12.6.98 ipsec efficient-vpn (system view)

12.7.36 reset ipsec gdoi-sa

Function

The **reset ipsec gdoi-sa** command deletes TEK SAs and KEK SAs of all created GDOI policies.

Format

reset ipsec gdoi-sa [**policy** *policy-name* [*seq-number*]]

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
policy *policy-name* [*seq-number*]	Specifies the name and sequence number of a GDOI policy. The *seq-number* parameter is optional. If *seq-number* is not specified, all the TEK SAs and KEK SAs in the GDOI policy group specified by *policy-name* are deleted. This parameter is specified by running the **12.6.105 ipsec policy (system view)** command.	The value must be an existing GDOI policy name and sequence number.

Views

User view

Default Level

3: Management level

Usage Guidelines

When running the **reset ipsec gdoi-sa** command, pay attention to the following:

- If no parameter is specified, the TEK SAs and KEK SAs of all GDOI policies are deleted.
- If both **policy** and *seq-number* are specified, the TEK SAs and KEK SAs of the GDOI policy with the specified name and sequence is deleted. If only **policy** is specified, all the TEK SAs and KEK SAs in the specified GDOI policy group are deleted.

Example

Delete the TEK SAs and KEK SAs of all GDOI policies.

```
<Huawei> reset ipsec gdoi-sa
```

Delete all the TEK SAs and KEK SAs in the GDOI policy group **policy1**.

```
<Huawei> reset ipsec gdoi-sa policy policy1
```

Delete the TEK SA and KEK SA of the GDOI policy with the name **policy1** and sequence number 4.

```
<Huawei> reset ipsec gdoi-sa policy policy1 4
```

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

12.7.9 display ipsec gdoi-sa

12.7.37 sa duration time-based

Function

The **sa duration time-based** configures the TEK SA hard lifetime.

The **undo sa duration time-based** restores the TEK SA hard lifetime to the default value.

The default TEK SA hard lifetime is 3600 seconds.

Format

sa duration time-based *seconds*

undo sa duration time-based

Parameters

Parameter	Description	Value
seconds	Specifies the hard lifetime of a TEK SA.	The value is an integer that ranges from 600 to 604,800, in seconds.

Views

GDOI IPSec policy view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The TEK SA lifetime is used to update the TEK SA periodically, which reduces the risk of TEK SA cracking and improves security.

The TEK SA lifetime falls into the following types:

- Hard lifetime (hard timeout period): defines the number of seconds until the TEK SA expires.
- Soft lifetime (soft timeout period): defines the number of seconds until the IKE process is informed that the TEK SA is about to expire. This is to provide enough time for the creation of a new TEK SA before the hard lifetime is reached.

 Copyright © Huawei Technologies Co., Ltd.

When the soft lifetime expires, the KS generates a new TEK SA and sends it to GMs through rekey messages. After receiving the rekey messages, GMs use the new TEK SA 30 seconds prior to hard lifetime expiry. When the hard lifetime expires, the old TEK SA is deleted.

The value of the soft lifetime is related to the transmission mode, number of retransmissions, and retransmission interval of rekey messages. **Table 12-79** shows the detailed calculation methods.

Table 12-79 Soft lifetime values

Transmission Mode of Rekey Messages	Soft Lifetime Value
Unicast rekey	Hard lifetime - (90 + (Number of retransmissions + 1) x Retransmission interval + 5 x Number of GMs in the group/50)
Multicast rekey	Hard lifetime - (90 + (Number of retransmissions + 1) x Retransmission interval)

Precautions

When the configuration is modified, the KS does not send rekey messages immediately until the TEK SA soft lifetime expires. To make the modified configuration take effect immediately, enter the **12.7.11 gdoi ks rekey** command to manually trigger the KS to send out rekey messages.

Example

Set the TEK SA hard lifetime to 7200 seconds.

```
<Huawei> system-view
[Huawei] gdoi ks group gr1
[Huawei-gdoi-group-gr1] ipsec 2
[Huawei-gdoi-group-gr1-ipsec-2] sa duration time-based 7200
```

Related Topics

12.7.3 display gdoi ks group

12.7.38 sa receive-only

Function

The **sa receive-only** command sets the SA mode to Receive_Only. In this mode, the GM can send only plaintext packets but can receive both plaintext and ciphertext packets.

The **undo sa receive-only** command restores the default SA mode.

By default, the SA mode is Normal. In this mode, the GM sends and receives only ciphertext packets.

 Copyright © Huawei Technologies Co., Ltd.

Format

sa receive-only

undo sa receive-only

Parameters

None

Views

GDOI group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If SA modes cannot be configured in stages when you deploy the A2A VPN on an existing network (such as the MPLS VPN), services will be interrupted because a GM that joins a group can send and receive only ciphertext packets but the GM that has not joined the group can send and receive only plaintext packets. In this case, you need to set the SA mode on the GM and KS to implement the phased deployment of the A2A VPN.

The procedure is as follows:

1. Set the SA mode to Receive_Only on the KS. The KS will deliver this SA mode to GMs.
2. Deploy GMs on the A2A VPN one by one. The registered GMs work in Receive_Only mode, so they can communicate with the newly deployed GMs that haven't registered with the KS.
3. After all the GMs are deployed, set the SA mode to Receive_Option on the GMs. A GM in Receive_Option mode can still communicate with a GM in Receive_Only mode.
4. After all the GMs are switched to Receive_Option mode, set the SA mode to Normal on the KS.

Precautions

When the SA mode is changed, the KS immediately sends rekey messages.

When the SA mode is switched on the KS, traffic between GMs is interrupted for a short period of time.

Example

Set the SA mode to Receive_Only.

```
<Huawei> system-view
[Huawei] gdoi ks group gr1
[Huawei-gdoi-group-gr1] sa receive-only
```

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

12.7.12 gdoi sa direction receive-option
12.7.3 display gdoi ks group

12.7.39 security acl

Function

The **security acl** command references an ACL.

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

By default, no ACL is referenced.

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

GDOI policy view, GDOI group IPSec policy view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After a GM registers with the KS, the GM obtains security policies including the ACL rules from the KS. The ACL rules configured on the KS determine data flows to be encrypted and data flows to be forwarded in plain text. The GM matches received data flows with the ACL rules obtained from the KS. If the matched ACL rule defines a permit action, the GM encrypts the data flows and forwards them; if the matched ACL rule defines a deny action, the GM forwards the data flows in plain text. If a data flow matches an ACL rule that defines a permit action, but the GM wants to forward the data flow in plain text, you can configure a local ACL rule to define data flows not to be protected. When a device forwards a data flow, it matches the data flow with the local ACL rule first. If the data flow matches the local ACL rule, the device forwards the data flow in plain text. If not, the device matches the data flow with the ACL rules obtained from the KS.

 Copyright © Huawei Technologies Co., Ltd.

Precautions

The ACL rule configured in a GDOI policy can only be set to deny.

If no ACL rule is configured in a GDOI policy or all ACL rules configured in a GDOI policy are set to deny, a GM will fail to register with the KS.

If the KS sends more than 100 ACL rules to a GM, only 100 ACL rules take effect. If more than 100 ACL rules are configured on a GM, only 100 ACL rules take effect.

When configuring an ACL on the KS, you must deploy ACL rules based on the encrypted data flows to prevent some unencrypted packets from being discarded by IPSec verification, for example, rekey packets and IKE packets. When the ACL range is large, you must configure "deny" ACL rules for the packets that are not encrypted and should not be discarded. This ensures that such packets will not be dropped by IPSec verification.

When an ACL rule is modified in the GDOI group IPSec policy, the KS immediately sends rekey messages. If there are multiple GDOI IPSec policies in a GDOI group, the KS immediately sends out rekey messages when deleting the ACL in a GDOI group IPSec policy. If there is only one GDOI group IPSec policy in a GDOI group, the KS fails to send out rekey messages when deleting the ACL in the GDOI group IPSec policy.

Only the following optional parameters are supported for a security ACL rule: **source**, **destination**, **source-port eq**, and **destination-port eq**.

Example

Reference ACL 3101 in a GDOI policy.

```
<Huawei> system-view
[Huawei] acl number 3101
[Huawei-acl-adv-3101] rule deny ip destination 10.1.1.2 0.0.0.0
[Huawei-acl-adv-3101] quit
[Huawei] ipsec policy policy1 4 gdoi
[Huawei-ipsec-policy-gdoi-policy1-4] security acl 3101
```

Reference ACL 3101 in a GDOI group IPSec policy.

```
<Huawei> system-view
[Huawei] acl number 3101
[Huawei-acl-adv-3101] rule permit ip destination 10.1.1.2 0.0.0.0
[Huawei-acl-adv-3101] quit
[Huawei] gdoi ks group gr1
[Huawei-gdoi-group-gr1] ipsec 2
[Huawei-gdoi-group-gr1-ipsec-2] security acl 3101
```

Related Topics

12.7.8 display ipsec gdoi-policy

12.7.3 display gdoi ks group

12.7.40 source address (GDOI Group View)

Function

The **source address** command configures an IP address for a KS.

The **undo source address** command deletes the configured IP address of a KS.

 Copyright © Huawei Technologies Co., Ltd.

By default, no IP address is configured for a KS.

Format

source address *ip-address*

undo source address

Parameters

Parameter	Description	Value
ip-address	Specifies the IP address of a KS.	The value is in dotted decimal notation.

Views

GDOI group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When a GM registers with the KS, the GM carries the specified KS IP address to perform IKE SA negotiation with the KS. If the IP address configured for the KS is different from that carried by the GM, the IKE SA negotiation between the two ends fails, causing a GM registration failure. After the GM registers successfully, the KS sends a rekey message to the GM using the KS IP address as the source IP address of the rekey message.

Precautions

When the configuration is modified, the KS does not send rekey messages immediately until the KEK SA soft lifetime expires. To make the modified configuration take effect immediately, enter the **12.7.11 gdoi ks rekey** command to manually trigger the KS to send out rekey messages.

Example

Set the IP address of a KS to 10.1.1.1.

```
<Huawei> system-view
[Huawei] gdoi ks group gr1
[Huawei-gdoi-group-gr1] source address 1.1.1.1
```

Related Topics

12.7.3 display gdoi ks group

 Copyright © Huawei Technologies Co., Ltd.

12.7.41 tunnel local

Function

The **tunnel local** command configures an IP address for the local end of an A2A VPN tunnel.

The **undo tunnel local** command deletes the IP address of the local end of an A2A VPN tunnel.

By default, no IP address is configured for the local end of an A2A VPN tunnel.

Format

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

undo tunnel local

Parameters

Parameter	Description	Value
ip-address	Specifies the IP address for the local end of an A2A VPN tunnel.	THe value is a valid IPv4 address in dotted decimal notation.
applied-interface	Specifies the primary address of the interface to which the IPSec policy is applied as the IP address for the local end of an A2A VPN tunnel.	-

Views

GDOI policy view

Default Level

2: Configuration level

Usage Guidelines

You can run this command to specify a start point for an A2A VPN tunnel.

For a manually created IPSec policy, run the **tunnel local** *ip-address* command to configure an IP address for the local end before you can create an SA. Only after correct IP addresses are configured for the local end (start point) and remote end (end point), an A2A VPN tunnel can be established between the two ends.

For a GDOI policy, you do not need to configure a local address for A2A VPN because the device will select an appropriate local address based on routing

 Copyright © Huawei Technologies Co., Ltd.

information during SA negotiation. However, you need to configure a local address in the following cases:

- If the IP address of the interface to which an IPSec policy is applied varies or is unknown, run the **tunnel local** *ip-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 A2A VPN tunnel. Otherwise, run the **tunnel local applied-interface** command to specify the IP address of the interface as the IP address for the local end of an A2A VPN 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** *ip-address* command to specify one of these IP addresses as the IP address for the local end of an A2A VPN tunnel. Otherwise, run the **tunnel local applied-interface** command to specify the IP address of the interface as the IP address for the local end of an A2A VPN tunnel.
- If equal-cost routes exist between the local and remote ends, run the **tunnel local** { *ip-address* | **applied-interface** } command to configure an IP address for the local end of an A2A VPN tunnel.

Example

Configure the primary address of the interface to which the GDOI policy is applied as the IP address for the local end.

```
<Huawei> system-view
[Huawei] ipsec policy policy1 3 gdoi
[Huawei-ipsec-policy-gdoi-policy1-3] tunnel local applied-interface
```

Related Topics

12.7.18 ipsec policy (system view)

12.7.42 user-table (GDOI Group View)

Function

The **user-table** command references an IKE user table in a GDOI group.

The **undo user-table** command cancels the reference of an IKE user table.

By default, no IKE user table is referenced in a GDOI group.

Format

user-table *user-table-id*

undo user-table

Parameters

Parameter	Description	Value
user-table-id	Specifies the ID of an IKE user table.	The value must be the ID of an existing IKE user table.

 Copyright © Huawei Technologies Co., Ltd.

Views

GDOI group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When a GM registers with the KS, the KS and GM use pre-shared key authentication to authenticate each other. The initiator uses the pre-shared key to encrypt the data to be transmitted. The receiver uses the same pre-shared key to decrypt the data. If the decryption succeeds, the initiator passes the authentication.

The IKE user table records the mappings between the GM IDs and pre-shared keys. After a GDOI group references an IKE user table, the KS sends the pre-shared key to a GM based on the GM ID. During identity authentication, the KS searches the IKE user table for the pre-shared key corresponding to the GM ID to complete identity authentication.

Prerequisites

An IKE user table has been created using the **12.6.74 ike user-table** command.

Precautions

Each GDOI group can reference only one IKE user table.

Example

Reference IKE user table 10 in a GDOI group.

```
<Huawei> system-view
[Huawei] ike user-table 10
[Huawei-ike-user-table-10] quit
[Huawei] gdoi ks group gr1
[Huawei-gdoi-group-gr1] user-table 10
```

Related Topics

12.7.3 display gdoi ks group

12.8 SSL VPN Configuration Commands

NOTE

The feature is just for beta test, and is not for commercial use. If the feature is required in the test, contact Huawei technical support personnel.

 Copyright © Huawei Technologies Co., Ltd.

12.8.1 background-color

Function

The **background-color** command configures the background color of the virtual gateway web GUI.

The **undo background-color** command restores the default setting.

The RGB color model of the default background color on the virtual gateway web GUI is **#F6F6F6**.

Format

background-color *color-value*

undo background-color

Parameters

Parameter	Description	Value
color-value	Background color of the virtual gateway web GUI.	The RGB color model is used. The value format is *#H*, in which *H* is a 3-digit or 6-digit hexadecimal number. Each digit ranges from 0 to F.

Views

Virtual gateway view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The device supports personalized GUI elements. Enterprise users can customize elements on the web GUI of a virtual gateway to meet diversified enterprise requirements.

Run the **background-color** command to configure the background color on the virtual gateway web GUI.

Precautions

If you run the **background-color** command multiple times in the same virtual gateway view, only the latest configuration takes effect.

 Copyright © Huawei Technologies Co., Ltd.

Example

Set the RGB color model of the background color of the virtual gateway web GUI to **#EE0000**.

```
<Huawei> system-view
[Huawei] sslvpn gateway users
[Huawei-sslvpn-users] background-color #EE0000
```

Related Topics

12.8.21 max-user

12.8.2 banner-color

Function

The **banner-color** command configures the banner color of the virtual gateway web GUI.

The **undo banner-color** command restores the default setting.

The RGB color model of the default banner color on the virtual gateway web GUI is **#EEEEEE**.

Format

banner-color *color-value*

undo banner-color

Parameters

Parameter	Description	Value
color-value	Banner color of the virtual gateway web GUI.	The RGB color model is used. The value format is *#H*, in which *H* is a 3-digit or 6-digit hexadecimal number. Each digit ranges from 0 to F.

Views

Virtual gateway view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

 Copyright © Huawei Technologies Co., Ltd.

The device supports personalized GUI elements. Enterprise users can customize elements on the web GUI of a virtual gateway to meet diversified enterprise requirements.

Run the **banner-color** command to configure the banner color on the virtual gateway web GUI.

Precautions

If you run the **banner-color** command multiple times in the same virtual gateway view, only the latest configuration takes effect.

Example

Set the RGB color model of the banner color of the virtual gateway web GUI to **#000011**.

```
<Huawei> system-view
[Huawei] sslvpn gateway users
[Huawei-sslvpn-users] banner-color #000011
```

Related Topics

12.8.21 max-user

12.8.3 bind acl

Function

The **bind acl** command binds an ACL to the IP forwarding service.

The **undo bind acl** command unbinds an ACL from the IP forwarding service.

By default, no ACL is bound to the IP forwarding service.

Format

bind acl *acl-number*

undo bind acl

Parameters

Parameter	Description	Value
acl-number	ACL number that you want to bind to the IP forwarding service.	The value is an integer ranging from 3000 to 3999.

Views

IP forwarding service view

 Copyright © Huawei Technologies Co., Ltd.

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The SSL VPN gateway allows remote terminals to communicate with internal servers at the network layer. For example, remote terminals and internal servers implement file sharing.

Remote users are not allowed to access confidential data on the intranet. After an ACL is bound to the IP forwarding service, the SSL VPN gateway filters remote users' IP packets based on this ACL to limit the remote users access rights. For example, if you want remote users to access only internal server 1.1.1.1, bind an ACL to the IP forwarding service to permit only the IP packets destined for 1.1.1.1 and discard other IP packets.

Prerequisites

The ACL that you want to bind to the IP forwarding service has been created.

Precaution

If you run the **bind acl** command multiple times in the same IP forwarding service view, only the latest configuration takes effect.

Example

Bind an ACL to the IP forwarding service.

```
<Huawei> system-view
[Huawei] sslvpn gateway users
[Huawei-sslvpn-users] service-type ip-forwarding resource ifres1
[Huawei-sslvpn-users-if-res-ifres1] bind acl 3001
```

Related Topics

12.8.21 max-user
12.8.28 service-type resource

12.8.4 bind domain

Function

The **bind domain** command binds an AAA domain to a virtual gateway.

The **undo bind domain** command unbinds an AAA domain from a virtual gateway.

By default, no AAA domain is bound to a virtual gateway.

Format

bind domain *domain-name*

undo bind domain

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
domain-name	Name of an AAA domain.	The value is the name of an existing AAA domain.

Views

Virtual gateway view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To prevent unauthorized remote users from accessing internal resources and protect intranet security, each virtual gateway must authenticate login remote users. After being bound to an AAA domain, a virtual gateway performs AAA authentication for all login remote users. Only the authenticated remote users are allowed to access internal resources.

Prerequisites

The AAA domain that you want to bind to the virtual gateway has been created.

Precautions

The virtual gateway supports only two authentication methods: local authentication and RADIUS authentication.

If you need to modify the bound AAA domain after the basic SSL VPN functions are enabled, use the **undo enable** command to disable the basic SSL VPN functions first.

Example

Bind the AAA domain **admin** to the virtual gateway **users**.

```
<Huawei> system-view
[Huawei] sslvpn gateway users
[Huawei-sslvpn-users] bind domain admin
```

Related Topics

12.8.21 max-user

12.8.5 bind ip-pool

Function

The **bind ip-pool** command binds an IP address pool to the IP forwarding service.

 Copyright © Huawei Technologies Co., Ltd.

The **undo bind ip-pool** command unbinds an IP address pool from the IP forwarding service.

By default, no IP address pool is bound to the IP forwarding service.

Format

bind ip-pool *pool-name*

undo bind ip-pool

Parameters

Parameter	Description	Value
pool-name	IP address pool that you want to bind to the IP forwarding service.	The value is the name of an existing ip address pool.

Views

IP forwarding service view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The IP forwarding function allows remote terminals to communicate with internal servers at the network layer.

When a remote user starts the IP forwarding service, the remote host automatically downloads the client software on the web page. The client software then installs a virtual network adapter on the remote host. The client software is responsible for setting up an SSL connection between the terminal and gateway, requesting an IP address for the virtual network adapter, and creating a route with the virtual network adapter as outbound interface.

After an IP address pool is bound to the IP forwarding service, an IP address is allocated from the IP address pool to the virtual network adapter.

Prerequisites

The IP address pool that you want to bind to the IP forwarding service has been created.

Precautions

If you want to configure the rental period of an IP address pool, the rental period must be longer than the maximum online duration of the SSL VPN remote user.

 Copyright © Huawei Technologies Co., Ltd.

If you run the **bind ip-pool** command multiple times in the same IP forwarding service view, only the latest configuration takes effect.

Example

Bind the IP address pool **pool1** to the IP forwarding service.

```
<Huawei> system-view
[Huawei] sslvpn gateway users
[Huawei-sslvpn-users] service-type ip-forwarding resource ifres1
[Huawei-sslvpn-users-if-res-ifres1] bind ip-pool pool1
```

Related Topics

12.8.21 max-user

12.8.28 service-type resource

8.3.83 ip pool (system view)

12.8.6 cut user

Function

The **cut user** command forcibly disconnects remote users from a virtual gateway.

Format

cut user { **name** *user-name* | **id** *user-id* | **all** }

Parameters

Parameter	Description	Value
name *user-name*	Specifies the name of the remote user that you want to disconnect from a virtual gateway.	The value is the name of an existing remote user.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
id *user-id*	Specifies the ID of the remote user that you want to disconnect from a virtual gateway. After a user goes online, the virtual gateway automatically allocates an ID for the remote user. To view the IDs of all online remote users, run the **display sslvpn gateway access-user** command.	The value is an integer and the value range depends on device types. • AR100&AR120&AR150&AR160&AR200 series: 0 to 9 • AR1200 series, AR2201-48FE, AR2202-48FE, AR2204: 0 to 49 • AR2220E, AR2220, AR2240 (using SRU40 or SRU60), AR3200 (using SRU40 or SRU60) series: 0 to 99 • AR2204XE, AR2204XE-DC, AR2240 (using SRU80, or SRU100E, SRU200, or SRU200E, or SRU400), AR3200 (using SRU80, or SRU100E, SRU200, or SRU200E, or SRU400), AR3600 (using SRUX5) series: 0 to 199
all	Disconnects all remote users from a virtual gateway.	-

Views

Virtual gateway view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can disconnect a remote user by specifying the remote user's name or ID or disconnect all remote users from a virtual gateway. The virtual gateway still stores information about the disconnected remote users.

Follow-up Procedure

Copyright © Huawei Technologies Co., Ltd.

Run the **display sslvpn gateway access-user** command to view remote users' status.

Example

Disconnect the user **jackson** from the virtual gateway.

```
<Huawei> system-view
[Huawei] sslvpn gateway users
[Huawei-sslvpn-users] cut user name jackson
```

Related Topics

12.8.21 max-user

12.8.9 display sslvpn gateway access-user

12.8.7 description

Function

The **description** command configures the description of a service on a virtual gateway.

The **undo description** command deletes the service description on a virtual gateway.

By default, the services on a virtual gateway do not have description.

Format

description *description*

undo description

Parameters

Parameter	Description	Value
description	Service description on a virtual gateway.	The value is a string of 1 to 80 case-sensitive characters without spaces or the following characters: < > [ ]. If the string is enclosed in double quotation marks (" "), the string can contain spaces.

Views

Web proxy service view, port forwarding service view, or IP forwarding service view

 Copyright © Huawei Technologies Co., Ltd.

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **description** command configures the service description on a virtual gateway, such as, the usage or use scenario of a service. The service description is used to differentiate services.

Precautions

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

Example

Configure the description for the port forwarding service.

```
<Huawei> system-view
[Huawei] sslvpn gateway users
[Huawei-sslvpn-users] service-type port-forwarding resource pres1
[Huawei-sslvpn-users-pf-res-presl] description this service is used to access the ftp server
```

Related Topics

12.8.21 max-user

12.8.28 service-type resource

12.8.8 display sslvpn gateway

Function

The **display sslvpn gateway** command displays virtual gateway information.

Format

display sslvpn gateway [*gateway-name*]

Parameters

Parameter	Description	Value
gateway-name	Displays information about a specified virtual gateway. If this parameter is not specified, the system displays information about all virtual gateways.	The value is the name of an existing virtual gateway.

 Copyright © Huawei Technologies Co., Ltd.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

None

Example

Display information about the virtual gateway **users**.

```
<Huawei> display sslvpn gateway users
 ------------------------------------------------------------------------------
 Gateway name               :   users
 Status                   :   enable
 Intranet interface         :   Ethernet1/0/0
 Intranet IP              :   10.1.17.1
 Domain                   :   default
 Max-user                 :   200
 Max-onlinetime(minute)     :   120
 Web-proxy resources        :   2
 Port-forwarding resources  :   1
 Ip-forwarding  resources   :   1
 Total online users         :   15
 ------------------------------------------------------------------------
```

Table 12-80 Description of the display sslvpn gateway command output

Item	Description
Gateway name	Virtual gateway name. To configure the virtual gateway name, run the **sslvpn gateway** *gateway-name* command.
Status	Status of the virtual gateway: • enable • disable To enable basic functions of a virtual gateway, run the **enable** command.
Intranet interface	Intranet interface of the virtual gateway. To configure an intranet interface of a virtual gateway, run the **intranet interface** *interface-type interface-number* command.
Intranet IP	IP address of the intranet interface.
Domain	AAA domain bound to the virtual gateway. To bind a domain to a virtual gateway, run the **bind domain** *domain-name* command.

Copyright © Huawei Technologies Co., Ltd.

Item	Description
Max-user	Maximum number of online remote users allowed by the virtual gateway. To set the maximum number of online remote users allowed by a virtual gateway, run the **max-user** *number* command. The maximum number of online remote users is limited by the maximum numbers of online remote users provided by the device. The actual maximum number of online remote users is the smallest value between the maximum numbers configured by the administrator and provided by the device.
Max-onlinetime(minute)	Maximum online duration of a remote user allowed by the virtual gateway. To set the maximum online duration of a remote user allowed by a virtual gateway, run the **max-online-time** *number* command.
Web-proxy resources	Number of web proxy resources.
Port-forwarding resources	Number of port forwarding resources.
Ip-forwarding resources	Number of IP forwarding resources.
Total online users	Total number of online remote users.

12.8.9 display sslvpn gateway access-user

Function

The **display sslvpn gateway access-user** command displays remote access user information on a virtual gateway.

Format

display sslvpn gateway *gateway-name* **access-user** [*user-name*]

Parameters

Parameter	Description	Value
gateway-name	Indicates the virtual gateway name.	The value is the name of an existing virtual gateway.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
user-name	Displays details about the specified remote user on the virtual gateway.	The value is a string of 1 to 64 case-insensitive characters. It cannot contain a space or question mark (?).

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

To view information about online remote users on the virtual gateway, namely, access remote user information, run the **display sslvpn gateway access-user** command.

Example

Display information about all remote access users on a virtual gateway.

```
<Huawei> display sslvpn gateway gate0 access-user
Total access-user number of this gateway: 1
  ------------------------------------------------------------------------------
  User name                      User ID          Auth method
  ------------------------------------------------------------------------------
  admin@domain1                    0                LOCAL
  ------------------------------------------------------------------------------
```

Display information about the remote user **fag**.

```
<Huawei> display sslvpn gateway gate0 access-user fag
  ------------------------------------------------------------------------------
  User name                 :   admin@domain1
  User ID                   :   0
  Auth Method               :   LOCAL
  Max-onlinetime(minute)    :   120
  Current-onlinetime(minute) :   25
  ------------------------------------------------------------------------------
```

Table 12-81 Description of the display sslvpn gateway command output

Item	Description
User name	User name of the remote access user.
User ID	User ID of the remote access user.

Copyright © Huawei Technologies Co., Ltd.

Item	Description
Auth Method	Authentication method of the remote access user: • LOCAL: local authentication • RADIUS: RADIUS authentication
Max-onlinetime(minute)	Maximum online duration of the remote user. To set the maximum online duration of a remote user allowed by a virtual gateway, run the **max-online-time** *number* command.
Current-onlinetime(minute)	Current online duration of the remote user.

Related Topics

12.8.21 max-user

12.8.10 display sslvpn gateway resource

Function

The **display sslvpn gateway resource** command displays resource information on a virtual gateway.

Format

display sslvpn gateway *gateway-name* **resource class** { **web-proxy** | **port-forwarding** | **ip-forwarding** }

Parameters

Parameter	Description	Value
gateway-name	Displays resource information on a virtual gateway.	The value is the name of an existing virtual gateway.
class web-proxy	Displays resource information of the web proxy service.	-
class port-forwarding	Displays resource information of the port forwarding service.	-
class ip-forwarding	Displays resource information of the IP forwarding service.	-

Copyright © Huawei Technologies Co., Ltd.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

To view resource information on a virtual gateway, run the **display sslvpn gateway resource** command.

Example

Display web proxy resource information on the virtual gateway **users**.

```
<Huawei> display sslvpn gateway users resource class web-proxy
The total number of resources is : 2
  ------------------------------------------------------------------------------
  Resource name               Url                      Type
  ------------------------------------------------------------------------------
  liyue                    http://192.168.1.65/      web-proxy
  test                     http://192.168.1.65/      web-proxy
  ------------------------------------------------------------------------------
```

Display port forwarding resource information on the virtual gateway **users**.

```
<Huawei> display sslvpn gateway users resource class port-forwarding

The total number of resources is : 1
  ------------------------------------------------------------------------------
  Resource name               Server          Port     Type
  ------------------------------------------------------------------------------
  liyue                    192.168.1.65       3389     port-forwarding
  ------------------------------------------------------------------------------
```

Display IP forwarding resource information on the virtual gateway **users**.

```
<Huawei> display sslvpn gateway users resource class ip-forwarding
  ------------------------------------------------------------------------------
  Resource name       :  liyue
  Pool name           :  liyue
  Route-mode          :  full
  Acl                 :  3001
  Type                :  ip-forwarding
  ------------------------------------------------------------------------------
```

Table 12-82 Description of the display sslvpn gateway resource command output

Item	Description
The total number of resources	Number of resources on the virtual gateway
Resource name	Resource name. To configure a resource name, run the **service-type** { **web-proxy** | **port-forwarding** | **ip-forwarding** } **resource** *resource-name* command.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Url	URLs in the web proxy service. To configure a URL of an internal web server, run the **link** *url* [**web-tunnel**] command.
Type	Resource type: • web-proxy: web proxy service • port-forwarding: port forwarding service • ip-forwarding: IP forwarding service To configure an SSL VPN service, run the **service-type** { **web-proxy** | **port-forwarding** | **ip-forwarding** } **resource** *resource-name* command.
Server Port	IP address for the port forwarding service. Port number for the port forwarding service. To configure the IP address and port number for the port forwarding service, run the **server ip-address** *ip-address* **port** *port-number* command.
Pool name	IP address pool name bound to the IP forwarding service. To bind an IP address pool to the IP forwarding service, run the **bind ip-pool** *pool-name* command.
Route-mode	Routing mode used by the IP forwarding service: • full • split To configure a routing mode used by the IP forwarding service, run the **route-mode** { **full** | **split** } command.
Acl	ACL number bound to the IP forwarding service. To bind an ACL to the IP forwarding service, run the **bind acl** *acl-number* command.

12.8.11 display sslvpn user statistics

Function

The **display sslvpn user statistics** command displays history statistics on remote users.

Format

display sslvpn user statistics

Parameters

None

Copyright © Huawei Technologies Co., Ltd.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run this command to view history statistics on remote users.

Example

Display history statistics on remote users.

```
<Huawei> display sslvpn user statistics
  ------------------------------------------------------------------------------
  Maximum of total online users in history      :    0
  Begin time of total online users             :    2013-10-18 20:22:05
  Maximum time of total online users           :    2013-10-18 20:22:05
  ------------------------------------------------------------------------------
```

Table 12-83 Description of the **display sslvpn user statistics** command output

Item	Description
Maximum of total online users in history	Maximum number of total online remote users in the history.
Begin time of total online users	Time when collection of statistics on online remote users begins.
Maximum time of total online users	Time when the total number of online remote users reaches the maximum value.

Related Topics

12.8.23 reset sslvpn user statistics

12.8.12 display sslvpn server port

Function

The **display sslvpn server port** command displays information about the listening port number used by the SSL VPN service.

Format

display sslvpn server port

Parameters

None

 Copyright © Huawei Technologies Co., Ltd.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

None

Example

Display information about the listening port number used by the SSL VPN service.

```
<Huawei> display sslvpn server port
 sslvpn server port : 443    (default:443)
```

Table 12-84 Description of the display sslvpn server port command output

Item	Description
sslvpn server port	Listening port number used by the SSL VPN service.
default	Default listening port number used by the SSL VPN service.

Related Topics

12.8.30 sslvpn server port

12.8.13 enable

Function

The **enable** command enables the basic SSL VPN functions for a virtual gateway.

The **undo enable** command disables the basic SSL VPN functions for a virtual gateway.

By default, the basic SSL VPN functions are disabled.

Format

enable

undo enable

Parameters

None

 Copyright © Huawei Technologies Co., Ltd.

Views

Virtual gateway view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To use a device as an SSL VPN gateway, you must configure and enable the basic SSL VPN functions.

Pay attention to the following points when using the basic SSL VPN functions:

- After you configure the basic SSL VPN functions, you must use the **enable** command to make the function effective.
- If you disable the basic SSL VPN functions using the **undo enable** command, all online users are forcibly disconnected from the virtual gateway.

Prerequisites

The configurations of basic SSL VPN functions have been complete on the virtual gateway. The configurations of basic SSL VPN functions include:

- Intranet interfaces
- AAA domain

Example

Enable the basic SSL VPN functions on the virtual gateway **users**.

```
<Huawei> system-view
[Huawei] sslvpn gateway users
[Huawei-sslvpn-users] enable
```

Related Topics

12.8.21 max-user

12.8.14 intranet interface

Function

The **intranet interface** command configures an intranet interface for a virtual gateway.

The **undo intranet interface** command deletes the intranet interface from a virtual gateway.

By default, no intranet interface exists on a virtual gateway.

Format

intranet interface *interface-type interface-number*

 Copyright © Huawei Technologies Co., Ltd.

undo intranet interface

Parameters

Parameter	Description	Value
interface-type interface-number	Type and number of the intranet interface.	The *interface-type* value is a Layer 3 interface type; the *interface-number* value depends on the interface type and slot ID.

Views

Virtual gateway view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The intranet hosts or servers connect to the intranet interfaces of the SSL VPN gateway. When configuring a virtual gateway, the administrator needs to set the interface connecting the SSL VPN gateway to the internal server to the intranet interface of the virtual gateway. The interface enables the communication between the virtual gateway and the internal server.

Precautions

The intranet interface must be a Layer 3 interface and have an IP address.

If you need to modify the intranet interface after the basic SSL VPN functions are enabled, use the **undo enable** command to disable the basic SSL VPN functions first.

Example

Configure the intranet interface for the virtual gateway **users**.

```
<Huawei> system-view
[Huawei] sslvpn gateway users
[Huawei-sslvpn-users] intranet interface gigabitethernet 2/0/0
```

Related Topics

12.8.21 max-user

Copyright © Huawei Technologies Co., Ltd.

12.8.15 link

Function

The **link** command configures a URL of an internal web server and a mode in which the web proxy service is implemented.

The **undo link** command deletes a URL of an internal web server and a mode in which the web proxy service is implemented.

By default, the URL of an internal web server is not configured on a virtual gateway and URL rewriting mode is used.

Format

link *url* [**web-tunnel**]

undo link

Parameters

Parameter	Description	Value
url	Specifies the URL of an internal web server.	The value is a string of 1 to 200 case-sensitive characters. The string cannot contain the following characters: < > [ ]. **NOTE** • A URL supports the IP address and domain name formats. • An HTTP port number can also be specified in the URL. If no port number is specified, the URL uses the default port number 80.
web-tunnel	Indicates that users access the internal web server in web-tunnel mode.	-

Views

Web proxy service view

Default Level

2: Configuration level

Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

Usage Scenario

The web proxy service is based on the HTTPS protocol. Users access the internal web server through the SSL VPN gateway. The SSL VPN gateway functions as a proxy that forwards data between users and the internal web server. This function helps ensure that access to the internal web server is secure.

The URL for the internal web server must be specified so that remote users can access the web server.

The web proxy service can be implemented in the following modes:

- URL rewriting: this mode is often used.

  The internal website resource URL displayed by the SSL VPN gateway to remote users is a rewritten URL. After remote users click the website resource URL, the SSL VPN gateway changes the URL to the URL pointing to the SSL VPN gateway. The SSL VPN gateway must rewrite the URL on each page responded by the internal web server to remote users and retain other contents unchanged.
- Web-tunnel: this mode is implemented through port forwarding.

  After a remote user logs in to the SSL VPN gateway, the Java plug-in is automatically installed on the remote terminal, and the internal website resource URL displayed to the remote user is the actual intranet URL. After the user clicks the URL, the Java plug-in automatically adds a header containing a destination address (address of the SSL VPN gateway) to the packet, and sends the packet to the SSL VPN gateway using HTTP request. The SSL VPN gateway converts the packet to the original HTTP request and sends it to the internal web server.

Precautions

Only one URL can be configured for a web proxy service. If there are multiple internal web servers, multiple web proxy services can be configured.

If you run the **link** command multiple times in the same web proxy service view, only the latest configuration takes effect.

Example

Configure a URL for an internal web server.

```
<Huawei> system-view
[Huawei] sslvpn gateway users
[Huawei-sslvpn-users] service-type web-proxy resource wpres1
[Huawei-sslvpn-users-wp-res-wpres1] link http://10.0.0.1/
```

Related Topics

12.8.21 max-user

12.8.28 service-type resource

 Copyright © Huawei Technologies Co., Ltd.

12.8.16 login-help

Function

The **login-help** command configures the help information on the bottom of the virtual gateway web GUI.

The **undo login-help** command restores the default setting.

The default help information on the bottom of the virtual gateway web GUI is **Copyright © Huawei Technologies Co., Ltd. 2012. All rights reserved.**

Format

login-help *help-info*

undo login-help

Parameters

Parameter	Description	Value
help-info	Help information on the bottom of the virtual gateway web GUI.	The value is a string of 1 to 200 case-sensitive characters without spaces or the following characters: < > [ ]. If the string is enclosed in double quotation marks (" "), the string can contain spaces. **NOTE** The Unicode can be used to represent Chinese characters or special characters.

Views

Virtual gateway view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The device supports personalized GUI elements. Enterprise users can customize elements on the web GUI of a virtual gateway to meet diversified enterprise requirements.

An enterprise may want to display the enterprise address and phone number to customers. To meet this requirement, the administrator can display the information as the help information on the bottom of the virtual gateway web GUI.

Precautions

If you run the **login-help** command multiple times in the same virtual gateway view, only the latest configuration takes effect.

Example

Set the help information on the bottom of the virtual gateway web GUI to **Tel:123456**.

```
<Huawei> system-view
[Huawei] sslvpn gateway users
[Huawei-sslvpn-users] login-help Tel:123456
```

Related Topics

12.8.21 max-user

12.8.17 login-message

Function

The **login-message** command configures the greeting on the virtual gateway web GUI.

The **undo login-message** command restores the default setting.

The default greeting on the virtual gateway web GUI is **Welcome to login:**.

Format

login-message *welcome-info*

undo login-message

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
welcome-info	Greeting on the virtual gateway web GUI.	The value is a string of 1 to 128 case-sensitive characters without spaces or the following characters: < > [ ]. If the string is enclosed in double quotation marks (" "), the string can contain spaces. **NOTE** The Unicode can be used to represent Chinese characters or special characters.

Views

Virtual gateway view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The device supports personalized GUI elements. Enterprise users can customize elements on the web GUI of a virtual gateway to meet diversified enterprise requirements.

An enterprise may require the virtual gateway web GUI to display specified greetings for specified customers or holidays. Run the **login-message** command to configure the greeting on the virtual gateway web GUI.

Precautions

If you run the **login-message** command multiple times in the same virtual gateway view, only the latest configuration takes effect.

Example

Set the greeting on the virtual gateway web GUI to **Welcome**.

```
<Huawei> system-view
[Huawei] sslvpn gateway users
[Huawei-sslvpn-users] login-message Welcome
```

Set the greeting on the virtual gateway web GUI to **Welcome**. (Unicode indicates Chinese Characters.)

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> system-view
[Huawei] sslvpn gateway users
[Huawei-sslvpn-users] login-message %u6B22%u8FCE%u8BBF%u95EE%u672C%u516C%u53F8
```

Related Topics

12.8.21 max-user

12.8.18 login-photo

Function

The **login-photo** command configures the background picture in the login dialog box of the virtual gateway web GUI.

The **undo login-photo** command deletes the configured background picture from the login dialog box of the virtual gateway web GUI.

By default, the background picture in the login dialog box of the virtual gateway web GUI is light gray.

Format

login-photo *login-photo-file*

undo login-photo

Parameters

Parameter	Description	Value
login-photo-file	Background picture in the login dialog box of the virtual gateway web GUI. **NOTE** The background picture must be a GIF file of a maximum of 6 KB.	The value is a string of 1 to 64 characters in the format of *[path] [file-name]*.

Views

Virtual gateway view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Copyright © Huawei Technologies Co., Ltd.

The device supports personalized GUI elements. Enterprise users can customize elements on the web GUI of a virtual gateway to meet diversified enterprise requirements.

Run the **login-photo** command to change the background picture in the login dialog box of the virtual gateway web GUI.

Precautions

- The recommended picture pixels are 35 x 35.
- If you run the **login-photo** command multiple times in the same virtual gateway view, only the latest configuration takes effect.

Example

Set the background picture in the login dialog box of the virtual gateway web GUI to **Login.gif**.

```
<Huawei> system-view
[Huawei] sslvpn gateway users
[Huawei-sslvpn-users] login-photo flash:/Login.gif
```

Related Topics

12.8.21 max-user

12.8.19 logo

Function

The **logo** command configures the enterprise logo on the enterprise gateway web GUI.

The **undo logo** command deletes the configured enterprise logo from the enterprise gateway web GUI.

Format

logo *logo-file*

undo logo

Parameters

Parameter	Description	Value
logo-file	File name of the enterprise logo on the enterprise gateway web GUI.	The value is a string of 1 to 64 characters in the format of *[path] [file-name]*. **NOTE** The enterprise logo must be a GIF file of a maximum of 6 KB.

 Copyright © Huawei Technologies Co., Ltd.

Views

Virtual gateway view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The device supports personalized GUI elements. Enterprise users can customize elements on the web GUI of a virtual gateway to meet diversified enterprise requirements.

Generally, enterprises have their own logos. If an enterprise requires the virtual gateway web GUI to display the enterprise logo, run the **logo** command to configure the enterprise logo on the enterprise gateway web GUI.

Precautions

- The recommended picture pixels are 50 x 50.
- If you run the **logo** command multiple times in the same virtual gateway view, only the latest configuration takes effect.

Example

Set the enterprise logo on the enterprise gateway web GUI to **iHappy.gif**.

```
<Huawei> system-view
[Huawei] sslvpn gateway users
[Huawei-sslvpn-users] logo flash:/iHappy.gif
```

Related Topics

12.8.21 max-user

12.8.20 max-online-time

Function

The **max-online-time** command configures the maximum online duration of a remote user allowed by the virtual gateway.

The **undo max-online-time** command restores the default duration.

By default, the maximum online duration of remote users allowed by a virtual gateway is 120 minutes.

Format

max-online-time *number*

undo max-online-time

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
number	Maximum online duration of a remote user allowed by the virtual gateway.	The value is an integer ranging from 5 to 480, in minutes.

Views

Virtual gateway view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If an online remote user does not use services for a long time, the remote user still occupies resources. To avoid a waste of resources, configure the maximum online duration for remote users. A remote user whose online duration exceeds the limit is logged off forcibly. The virtual gateway still stores information about the disconnected remote users.

Follow-up Procedure

Run the **display sslvpn gateway access-user** command to view the maximum online duration of remote users.

Example

Configure the maximum online duration of a remote user allowed by the virtual gateway.

```
<Huawei> system-view
[Huawei] sslvpn gateway users
[Huawei-sslvpn-users] max-online-time 200
```

Related Topics

12.8.21 max-user

12.8.9 display sslvpn gateway access-user

12.8.21 max-user

Function

The **max-user** command configures the maximum number of online users allowed by the virtual gateway.

The **undo max-user** command restores the default value.

 Copyright © Huawei Technologies Co., Ltd.

By default, the maximum number of online users allowed by the virtual gateway is:

- AR120&AR150&AR160&AR200 series: 10
- AR1200 series, AR2201-48FE, AR2202-48FE, AR2204: 50
- AR2220, AR2220E, AR2240 (using SRU40 or SRU60), AR3200 (using SRU40 or SRU60) series: 100
- AR2204XE, AR2204XE-DC, AR2240 (using SRU80, SRU100E, SRU200, SRU200E, SRU400), AR3200 (using SRU80, SRU100E, SRU200, SRU200E, SRU400), AR3600 (using SRU5X) series: 200

The maximum number of online remote users is limited by the maximum numbers of online remote users provided by the device. The actual maximum number of online remote users is the smallest value between the maximum numbers configured by the administrator and provided by the device.

Format

max-user *number*

undo max-user

Parameters

Parameter	Description	Value
number	Maximum number of online users allowed by the virtual gateway.	The value is an integer and the value range depends on device types. • AR100&AR120&AR150&AR160&AR200 series: 0 to 10 • AR1200 series, AR2201-48FE, AR2202-48FE, AR2204: 0 to 50 • AR2220, AR2220E, AR2240 (using SRU40 or SRU60), AR3200 (using SRU40 or SRU60) series: 0 to 100 • AR2204XE, AR2204XE-DC, AR2240 (using SRU80, SRU100E, SRU200, SRU200E, or SRU400), AR3200 (using SRU80, SRU100E, SRU200, SRU200E, or SRU400), AR3600 (using SRU5X) series: 0 to 200

Views

Virtual gateway view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **max-user** command limits the number of online remote users. When the number of online remote users on the virtual gateway exceeds the limit, no more remote user can log in.

Precautions

 Copyright © Huawei Technologies Co., Ltd.

When you configure the maximum number of online remote users for multiple virtual gateways, the sum of the maximum numbers cannot exceed the maximum number supported by the device.

Example

Set the maximum number of online users on the virtual gateway **users** to 10.

```
<Huawei> system-view
[Huawei] sslvpn gateway users
[Huawei-sslvpn-users] max-user 10
```

Related Topics

12.8.21 max-user

12.8.22 organization

Function

The **organization** command configures the enterprise name on the enterprise gateway web GUI.

The **undo organization** command restores the default setting.

The default enterprise name on the virtual gateway web GUI is **SSL VPN**.

Format

organization *organization-name*

undo organization

Parameters

Parameter	Description	Value
organization-name	Enterprise name on the enterprise gateway web GUI.	The value is a string of 1 to 200 case-sensitive characters without spaces or the following characters: < > [ ]. If the string is enclosed in double quotation marks (" "), the string can contain spaces. **NOTE** The Unicode can be used to represent Chinese characters or special characters.

 Copyright © Huawei Technologies Co., Ltd.

Views

Virtual gateway view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The device supports personalized GUI elements. Enterprise users can customize elements on the web GUI of a virtual gateway to meet diversified enterprise requirements.

Generally, enterprises have their own names. If an enterprise requires the virtual gateway web GUI to display the enterprise name, run the **organization** command to configure the enterprise name on the enterprise gateway web GUI.

Precautions

If you run the **organization** command multiple times in the same virtual gateway view, only the latest configuration takes effect.

Example

Set the enterprise name on the enterprise gateway web GUI to **iHappy**.

```
<Huawei> system-view
[Huawei] sslvpn gateway users
[Huawei-sslvpn-users] organization iHappy
```

Related Topics

12.8.21 max-user

12.8.23 reset sslvpn user statistics

Function

The **reset sslvpn user statistics** command clears history statistics on remote users.

Format

reset sslvpn user statistics

Parameters

None

Views

User view

 Copyright © Huawei Technologies Co., Ltd.

Default Level

3: Management level

Usage Guidelines

You can run this command to clear history statistics on remote users.

NOTICE

Statistics cannot be restored after being cleared. Therefore, confirm the action before you run the command.

Example

Clear history statistics on remote users.

```
<Huawei> reset sslvpn user statistics
```

Related Topics

12.8.11 display sslvpn user statistics

12.8.24 route-mode

Function

The **route-mode** command configures a routing mode for the IP forwarding service.

The **undo route-mode** command restores the default routing mode.

By default, the routing mode is full.

Format

route-mode { **full** | **split** }

undo route-mode

Parameters

Parameter	Description	Value
full	Sets the routing mode to full.	-
split	Sets the routing mode to split.	-

Copyright © Huawei Technologies Co., Ltd.

Views

IP forwarding service view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The SSL VPN gateway allows remote terminals to communicate with internal servers at the network layer. For example, remote terminals and internal servers implement file sharing.

The IP forwarding service can be implemented in the following modes:

- Full routing mode

  The SSL VPN gateway adds a default route with the next hop address as the virtual network adapter's IP address (intranet IP address allocated to the virtual network adapter by the SSL VPN gateway) to the routing table of a remote terminal. The remote terminal can communicate with servers on the specified network segment through the SSL VPN gateway.
- Split routing mode

  The SSL VPN gateway adds the route in split mode to the routing table of a remote terminal. The remote terminal can communicate with only servers on the specified internal network segment. This mode controls internal servers that remote terminals can communicate in a fine-grained manner.

Precaution

If you run the **route-mode** command multiple times in the same IP forwarding service view, only the latest configuration takes effect.

Follow-up Procedure

If you choose the Split mode, you must use the **route-split** command to specify the network segment that users can access.

Example

Set the routing mode to Split.

```
<Huawei> system-view
[Huawei] sslvpn gateway users
[Huawei-sslvpn-users] service-type ip-forwarding resource ifres1
[Huawei-sslvpn-users-if-res-ifres1] route-mode split
```

Related Topics

12.8.21 max-user

12.8.28 service-type resource

12.8.25 route-split

 Copyright © Huawei Technologies Co., Ltd.

12.8.25 route-split

Function

The **route-split** command specifies the accessible network segment for remote users when the split routing mode is used.

The **undo route-split** command cancels the configuration.

By default, no accessible network segment is specified.

Format

route-split ip address *ip-address* **mask** { *mask-length* | *mask* }

undo route-split ip address *ip-address* **mask** { *mask-length* | *mask* }

Parameters

Parameter	Description	Value
ip address *ip-address*	Specifies the destination IP address of the route to the internal network segment. This is a private IP address.	The value is in dotted decimal notation.
mask *mask-length*	Specifies the mask length of the route to the internal network segment.	The value is an integer ranging from 1 to 32.
mask *mask*	Specifies the mask of the route to the internal network segment.	The value is in dotted decimal notation.

Views

IP forwarding service view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The SSL VPN gateway allows remote terminals to communicate with internal servers at the network layer. For example, remote terminals and internal servers implement file sharing.

The IP forwarding service can be implemented in full routing mode and split routing mode. In split routing mode, the SSL VPN gateway adds the route in split

 Copyright © Huawei Technologies Co., Ltd.

mode to the routing table of a remote terminal. The remote terminal can communicate with only servers on the specified internal network segment. This mode controls internal servers that remote terminals can communicate in a fine-grained manner.

The **route-split** command limits the network segment that users can access by specifying the route destination IP address and mask.

Prerequisites

The **route-mode** command has been executed to set the routing mode to Split.

Precautions

A maximum of 10 user routes in Split routing mode can be configured in the same IP forwarding service view.

Example

Specify the network segment that users can access.

```
<Huawei> system-view
[Huawei] sslvpn gateway users
[Huawei-sslvpn-users] service-type ip-forwarding resource ifres1
[Huawei-sslvpn-users-if-res-ifres1] route-mode split
[Huawei-sslvpn-users-if-res-ifres1] route-split ip address 1.1.1.0 mask 24
```

Related Topics

12.8.21 max-user

12.8.28 service-type resource

12.8.24 route-mode

12.8.26 server ip-address

Function

The **server ip-address** command configures the IP address and port number for the port forwarding service.

The **undo server ip-address** command deletes the IP address and port number for the port forwarding service.

By default, no IP address or port number is configured for the port forwarding service.

Format

server ip-address *ip-address* **port** *port-number*

undo server ip-address

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
ip-address	IP address for the port forwarding service.	The value is in dotted decimal notation.
port *port-number*	Port number for the port forwarding service.	The value is an integer ranging from 1 to 65535.

Views

Port forwarding service view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The port forwarding function allows applications to access internal servers using TCP. Remote users can access the TCP-based services on the internal network. The typical port forwarding services include Telnet login, desktop sharing, and mailing. The IP address and port number of the internal application server must be specified so that remote users can access the application server.

Precautions

The IP address and port number specified in a command must match.

If you run the **server ip-address** command with different IP addresses and port numbers multiple times in the same port forwarding service view, only the latest configuration takes effect.

Example

Specify the IP address and port number for the port forwarding service.

```
<Huawei> system-view
[Huawei] sslvpn gateway users
[Huawei-sslvpn-users] service-type port-forwarding resource wpres1
[Huawei-sslvpn-users-pf-res-wpres1] server ip-address 1.1.1.1 port 23
```

Related Topics

12.8.21 max-user

12.8.28 service-type resource

12.8.27 server name

 Copyright © Huawei Technologies Co., Ltd.

12.8.27 server name

Function

The **server name** command configures the domain name and port number for the port forwarding service.

The **undo server name** command deletes the domain name and port number for the port forwarding service.

By default, the domain name and port number are not configured for the port forwarding service.

Format

server name *name* **port** *port-number*

undo server name

Parameters

Parameter	Description	Value
name	Specifies the domain name for the port forwarding service.	The value is a string of 1 to 200 case-sensitive characters without spaces or the following characters: < > [ ]. If the string is enclosed in double quotation marks (" "), the string can contain spaces.
port *port-number*	Specifies the port number for the port forwarding service.	The value is an integer ranging from 1 to 65535.

Views

Port forwarding service view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The port forwarding function allows applications to access internal servers using TCP. Users can access the TCP-based services on the internal network. The typical port forwarding services include Telnet login, desktop sharing, and mailing.

 Copyright © Huawei Technologies Co., Ltd.

Compared with an IP address, the domain name is easy to remember. When configuring the port forwarding service, the administrator can specify the domain name and port number of the internal server that can be accessed.

Prerequisites

The SSL VPN gateway has been configured as the DNS client.

Precautions

When you run this command to configure the domain name and port number for the port forwarding service, the domain name and port number must correspond to each other.

If you run the **server name** command with different values of the *name* or *port-number* parameter multiple times in the same port forwarding service view, only the latest configuration takes effect.

Example

Configure the domain name and port number for the port forwarding service.

```
<Huawei> system-view
[Huawei] sslvpn gateway users
[Huawei-sslvpn-users] service-type port-forwarding resource wpres1
[Huawei-sslvpn-users-pf-res-wpres1] server name www.iHappy.com.cn port 23
```

Related Topics

12.8.21 max-user

12.8.28 service-type resource

12.8.26 server ip-address

12.8.28 service-type resource

Function

The **service-type resource** command creates a service on the virtual gateway and enters the service view or enters an existing service view.

The **undo service-type resource** command deletes a service from the virtual gateway.

By default, no service exists on a virtual gateway.

Format

service-type { **web-proxy** | **port-forwarding** | **ip-forwarding** } **resource** *resource-name*

undo service-type { **web-proxy** | **port-forwarding** | **ip-forwarding** } **resource** *resource-name*

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
web-proxy	Indicates a web proxy service.	-
port-forwarding	Indicates a port forwarding service.	-
ip-forwarding	Indicates an IP forwarding service.	-
resource-name	Indicates the service name.	The value is a string of 1 to 31 case-sensitive characters without spaces When double quotation marks are used around the string, spaces are allowed in the string.

Views

Virtual gateway view

Default Level

2: Configuration level

Usage Guidelines

The device supports three service types as an SSL VPN gateway: web proxy, port forwarding, and IP forwarding.

The services on the SSL VPN gateway are created and configured in the virtual gateway view.

Example

Create the web proxy service **wpres1** and enter its view.

```
<Huawei> system-view
[Huawei] sslvpn gateway users
[Huawei-sslvpn-users] service-type web-proxy resource wpres1
[Huawei-sslvpn-users-wp-res-wpres1]
```

Related Topics

12.8.21 max-user

Copyright © Huawei Technologies Co., Ltd.

12.8.29 sslvpn gateway

Function

The **sslvpn gateway** command creates a virtual gateway and enters its view or enters an existing virtual gateway view.

The **undo sslvpn gateway** command deletes a virtual gateway.

By default, no virtual gateway exists.

Format

sslvpn gateway *gateway-name*

undo sslvpn gateway *gateway-name*

Parameters

Parameter	Description	Value
gateway-name	Indicates the virtual gateway name.	The value is a string of 1 to 31 case-sensitive characters without spaces. The string cannot contain the following characters: ? < > [ ].

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Based on the HTTPS protocol, SSL VPN uses the data encryption, user identify authentication, and message integrity check mechanisms of the SSL protocol to ensure secure remote access to enterprises' intranets.

An SSL VPN gateway can function as multiple virtual gateways, and the administrator manage users and configures services for each virtual gateway. To deploy the SSL VPN function on a device, the administrator creates multiple virtual gateways on the device, and configures the basic SSL VPN functions, SSL VPN services, and personalized web GUI and manage SSL VPN users on each virtual gateway.

Precautions

The numbers of virtual gateways that can be created on devices are as follows:

 Copyright © Huawei Technologies Co., Ltd.

- AR100&AR120&AR150&AR160&AR200 series: 1
- AR1200 series, AR2201-48FE, AR2202-48FE, AR2204: 2
- AR2220, AR2220E, AR2240 (using SRU40 or SRU60), AR3200 (using SRU40 or SRU60) series: 4
- AR2204XE, AR2204XE-DC, AR2240 (using SRU80, SRU100, SRU100E, SRU200, or SRU200E, or SRU400), AR3200 (using SRU80, SRU100, SRU100E, SRU200, or SRU200E, or SRU400) series, AR3600 (using SRUX5): 8

Example

Create the virtual gateway **users**.

```
<Huawei> system-view
[Huawei] sslvpn gateway users
[Huawei-sslvpn-users]
```

Related Topics

12.8.28 service-type resource

12.8.30 sslvpn server port

Function

The **sslvpn server port** command configures the listening port number of the SSL VPN service.

The **undo sslvpn server port** command restores the default setting.

The default listening port number of the SSL VPN service is 443.

Format

sslvpn server port *port*

undo sslvpn server port

Parameters

Parameter	Description	Value
port	Listening port number of the SSL VPN service.	The value is an integer that can be 443 or range from 1025 to 51200.

Views

System view

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

Usage Scenario

The default listening port number of the SSL VPN service is 443. When port 443 is used by another service, such as web-based network management service, run the **sslvpn server port** command to configure another listening port number for the SSL VPN service.

Precautions

- Before configuring the listening port number of the SSL VPN service, the administrator must ensure that all virtual gateways on the SSL VPN gateway are disabled. To disable a virtual gateway, run the **undo enable** command in the virtual gateway view.
- After the administrator changes the listening port number, users must enter the URL containing the new port number to log in to the SSL VPN gateway.

  For example, the URL of the SSL VPN gateway is https://1.1.1.1/gateway1. When the listening port number is changed to 1025, remote users must enter the URL https://1.1.1.1:1025/gateway1.

Example

Set the listening port number of the SSL VPN service to 1025.

```
<Huawei> system-view
[Huawei] sslvpn server port 1025
```

12.8.31 table-color

Function

The **table-color** command configures the table header color of the virtual gateway web GUI.

The **undo table-color** command restores the default setting.

The RGB color model of the default table header color on the virtual gateway web GUI is **#CDCDCD**.

Format

table-color *color-value*

undo table-color

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
color-value	Table header color of the virtual gateway web GUI.	The RGB color model is used. The value format is *#H*, in which *H* is a 3-digit or 6-digit hexadecimal number. Each digit ranges from 0 to F.

Views

Virtual gateway view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The device supports personalized GUI elements. Enterprise users can customize elements on the web GUI of a virtual gateway to meet diversified enterprise requirements.

Run the **table-color** command to configure the table header color on the virtual gateway web GUI.

Precautions

If you run the **table-color** command multiple times in the same virtual gateway view, only the latest configuration takes effect.

Example

Set the RGB color model of the table header color of the virtual gateway web GUI to **#00EEFF**.

```
<Huawei> system-view
[Huawei] sslvpn gateway users
[Huawei-sslvpn-users] table-color #00EEFF
```

Related Topics

12.8.21 max-user

Copyright © Huawei Technologies Co., Ltd.

12.8.32 text-color

Function

The **text-color** command configures the text color of the virtual gateway web GUI.

The **undo text-color** command restores the default setting.

The RGB color model of the default text color on the virtual gateway web GUI is **#333333**.

Format

text-color *color-value*

undo text-color

Parameters

Parameter	Description	Value
color-value	Text color of the virtual gateway web GUI.	The RGB color model is used. The value format is *#H*, in which *H* is a 3-digit or 6-digit hexadecimal number. Each digit ranges from 0 to F.

Views

Virtual gateway view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The device supports personalized GUI elements. Enterprise users can customize elements on the web GUI of a virtual gateway to meet diversified enterprise requirements.

Run the **text-color** command to configure the text color on the virtual gateway web GUI.

Precautions

If you run the **text-color** command multiple times in the same virtual gateway view, only the latest configuration takes effect.

 Copyright © Huawei Technologies Co., Ltd.

Example

Set the RGB color model of the text color of the virtual gateway web GUI to **#00EEFF**.

```
<Huawei> system-view
[Huawei] sslvpn gateway users
[Huawei-sslvpn-users] text-color #00EEFF
```

Related Topics

12.8.21 max-user

12.9 BGP/MPLS IP VPN Configuration Commands

NOTE

The AR100&AR120&AR150&AR160&AR200 series do not supports BGP/MPLS IP VPN, only supports MCE.

12.9.1 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.

NOTE

The AR100&AR120&AR150&AR160&AR200 series do not support this command.

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

 Copyright © Huawei Technologies Co., Ltd.

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 ASBR in VPN Option B networking needs to apply a tunnel policy to VPNv4 routes learned from PEs.
- The RR on the backbone network of a VPN needs to apply a tunnel policy to VPNv4 routes learned from PEs.
- The PE in VPN Option C networking needs to apply a tunnel policy to received BGP labeled routes.

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 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
```

Related Topics

12.9.63 tunnel-policy (system view)

 Copyright © Huawei Technologies Co., Ltd.

12.9.2 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 label allocation mode is one label per route, that is, each route of the VPN instance address family destined for the remote PE is assigned a label.

NOTE

The AR100&AR120&AR150&AR160&AR200 series do not support this command.

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.

By default, each route of the VPN instance IPv4 or IPv6 address family is assigned a specified label. To change the label allocation mode to one label per instance, run the **apply-label per-instance** command. For example, a PE is configured with two VPN instances that have 20000 routes in total. By default, the PE will allocate 20000 MPLS labels to the routes. After the **apply-label per-instance** command is configured for the two VPN instances, the PE will allocate only two labels for the two VPN instances.

When a large number of routes of the VPN instance IPv4 or IPv6 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.

 Copyright © Huawei Technologies Co., Ltd.

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.

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
```

Related Topics

12.9.35 ip vpn-instance

12.9.14 display ip vpn-instance

12.9.36 ipv4-family (VPN instance view)

12.9.50 route-distinguisher

12.9.3 apply-label per-nexthop

Function

The **apply-label per-nexthop** command enables the ASBR to allocate labels for IPv4 VPN routes based on the next hop.

The **undo apply-label per-nexthop** command disables the ASBR from allocating labels for IPv4 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 VPNv4 or VPNv6 route.

NOTE

The AR100&AR120&AR150&AR160&AR200 series do not support this command.

Format

apply-label per-nexthop

 Copyright © Huawei Technologies Co., Ltd.

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 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 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.

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

Configuration Impact

After next-hop-based label allocation is enabled or disabled, the label allocated by the ASBR or SPE 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
```

Related Topics

12.9.2 apply-label per-instance

 Copyright © Huawei Technologies Co., Ltd.

12.9.4 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 label allocation mode is one label per route, that is, each route of the VPN instance address family destined for the remote PE is assigned a label.

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

When only a small number of VPN routes exists on the PE and MPLS label resources are sufficient, you can run the **apply-label per-route** command to improve system security. In this way, downstream devices can load balance VPN traffic based on the inner labels of packets.

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.

 Copyright © Huawei Technologies Co., Ltd.

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
```

Related Topics

12.9.36 ipv4-family (VPN instance view)

12.9.37 ipv6-family (VPN instance view)

12.9.50 route-distinguisher

12.9.5 apply lsp vpn

Function

The **apply lsp vpn** command enables a specified LSP to forward VPN packets that meet the PBR filtering conditions.

The **undo apply lsp vpn** command disables a specified LSP from forwarding VPN packets that meet the PBR filtering conditions.

By default, the PBR is not used for forwarding VPN packets.

Format

apply lsp vpn *vpn-instance-name ce-address* [*pe-address* [*p-address* | *interface-type* | **secondary**]]

undo apply lsp vpn *vpn-instance-name ce-address*

Parameters

Parameter	Description	Value
vpn-instance-name	Specifies the VPN instance name.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
ce-address	Specifies the IP address of the destination CE.	The address is in dotted decimal notation.
pe-address	Specifies the IP address of the peer PE that resides on the LSP.	The address is in dotted decimal notation.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
p-address	Specifies the IP address of the P. *p-address* and *pe-address* together specify the next P through which the LSP passes.	The address is in dotted decimal notation.
interface-type interface-number	Specifies, together with *pe-address*, the next outbound interface of an LSP.	-
secondary	Indicates the backup LSP generated through LDP fast reroute (FRR). When **secondary** is not configured, only the primary LSP forwards packets. When **secondary** is configured, only the backup LSP forwards packets.	-

Views

Policy-Based-Route view

Default Level

2: Configuration level

Usage Guidelines

After configuring a PBR to the PE address and the P address, if there is no reachable LSP to them, the PBR is ineffective.

Example

Configure the LSP destined for the CE with IP address 20.1.1.1 to forward the VPN packets that match ACL 3000.

```
<Huawei> system-view
[Huawei] policy-based-route map1 permit node 10
[Huawei-policy-based-route-map1-10] if-match acl 3000
[Huawei-policy-based-route-map1-10] apply lsp vpn vpn1 20.1.1.1
```

12.9.6 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* }

 Copyright © Huawei Technologies Co., Ltd.

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.

 Copyright © Huawei Technologies Co., Ltd.

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
```

12.9.7 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.

 Copyright © Huawei Technologies Co., Ltd.

Example

Specify the description of a VPN instance named vpn1.

```
<Huawei> system-view
[Huawei] ip vpn-instance vpn1
[Huawei-vpn-instance-vpn1] description OnlyForAB
```

Related Topics

12.9.14 display ip vpn-instance

12.9.8 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, the description of a tunnel interface is "HUAWEI, AR Series, Tunnel *interface-number* Interface".

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.

 Copyright © Huawei Technologies Co., Ltd.

Example

Configure the description of Tunnel 0/0/1.
<Huawei> **system-view**
[Huawei] **interface tunnel 0/0/1**
[Huawei-Tunnel0/0/1] **description This is a tunnel from 10.1.1.1 to 10.2.2.2**

Delete the description of Tunnel 0/0/1.
<Huawei> **system-view**
[Huawei] **interface tunnel 0/0/1**
[Huawei-Tunnel0/0/1] **undo description**

Related Topics

12.9.32 interface tunnel
12.9.16 display interface tunnel

12.9.9 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.

NOTE

The AR100&AR120&AR150&AR160&AR200 series do not support this command.

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

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

After using the **12.9.63 tunnel-policy (system view)** command to create a tunnel policy, you can run the **description** command to configure a description of the tunnel policy to facilitate later query.

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
```

12.9.10 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 tunnel or IPSec tunnel, 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 value is in dotted decimal notation.

Views

Tunnel interface view

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

Usage Scenario

When configuring a GRE, IPv4 over IPv6, IPSec, MPLS TE, 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, IPSec, MPLS TE, IPv4 over IPv6, or IPv6 over IPv4 of manual mode using the **tunnel-protocol** command.

Precautions

Two or more GRE tunnel interfaces in a system can have the same source address and same destination address. The system uses GRE keys to identify these GRE tunnel interfaces. Normally, two tunnel interfaces in a system cannot have the same encapsulation mode, source address, and destination address.

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

On the IPSec, IPv6 over IPv4, IPv4 over IPv6, or GRE tunnel, the destination address of the local tunnel interface is the source address of the remote tunnel interface by the **source** command, and the source address of the local tunnel interface is the destination address of the remote tunnel interface.

Example

Set the destination address of the GRE tunnel Tunnel 0/0/1 to 10.1.1.1.

```
<Huawei> system-view
[Huawei] interface tunnel 0/0/1
[Huawei-Tunnel0/0/1] tunnel-protocol gre
[Huawei-Tunnel0/0/1] destination 10.1.1.1
```

Set the destination address of the GRE tunnel Tunnel 0/0/0 to 10.1.1.1 that belongs to vpn1.

```
<Huawei> system-view
[Huawei] interface tunnel 0/0/0
[Huawei-Tunnel0/0/0] tunnel-protocol gre
[Huawei-Tunnel0/0/0] destination vpn-instance vpn1 10.1.1.1
```

Related Topics

12.9.32 interface tunnel

12.9.55 source

12.9.64 tunnel-protocol

 Copyright © Huawei Technologies Co., Ltd.

12.9.11 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 route
    IPv6-family            : label per route
```

Table 12-85 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.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
label per route	The default label allocation mode is label per route.

12.9.12 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
```

 Copyright © Huawei Technologies Co., Ltd.

```
OSPF          11             3          1            0          5
IS-IS        106             0          1            0          5
RIP           98             0          1            1          5
BGP            2             0          1            1          5
MSR            0             0          0            0          0
------------------------------------------------------------------------------
VPN instance name: VPN1
         DenyAdd TryAddInDelState NotifyDelAll NotifyDelFinish NotifyAddRoute
DIRECT         0                0            0               0             0
STATIC         0                0            0               0             0
UNR            0                0            0               0             0
OSPF          11                3            1               0             5
IS-IS        106                0            1               0             5
RIP           98                0            1               1             5
BGP            2                0            1               1             5
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: 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          11                3            1               0             5
IS-IS        106                0            1               0             5
RIP           98                0            1               1             5
BGP            2                0            1               1             5
MSR            0                0            0               0             0
```

Table 12-86 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.

12.9.13 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       11               3           1              0              5
IS-IS       106               0           1              0              5
RIPng        98               0           1              1              5
BGP           2               0           1              1              5
------------------------------------------------------------------------------
IPv6 VPN instance name: VPN123
        DenyAdd TryAddInDelState NotifyDelAll NotifyDelFinish NotifyAddRoute
DIRECT        0               0           0              0              0
STATIC        0               0           0              0              0
UNR           0               0           0              0              0
OSPFv3       11               3           1              0              5
IS-IS       106               0           1              0              5
RIPng        98               0           1              1              5
BGP           2               0           1              1              5
```

Display the statistics of the prefix limit of the IPv6 VPN instance named **vrf1**.

```
<Huawei> display ipv6 prefix-limit vpn-instance vrf1 statistics
------------------------------------------------------------------------------
```

 Copyright © Huawei Technologies Co., Ltd.

```
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        11               3           1              0             5
IS-IS        106               0           1              0             5
RIPng         98               0           1              1             5
BGP            2               0           1              1             5
```

Table 12-87 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.
NotifyAddRoute	Number of times that the RIB notifies the protocol of re-adding routes.

12.9.14 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.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
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 are iterated (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      : 3
 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
```

 Copyright © Huawei Technologies Co., Ltd.

Table 12-88 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.
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 : GigabitEthernet1/0/0
 Address family ipv4
  Create date : 2012/12/3 15:36:20
  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
```

 Copyright © Huawei Technologies Co., Ltd.

```
Address family ipv6
 Create date : Create date : 2012/12/3 15:36:40
 Up time : 6 days, 04 hours, 41 minutes and 57 seconds
 Log Interval : 5
```

Table 12-89 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.
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

Copyright © Huawei Technologies Co., Ltd.

Item	Description
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.
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.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
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.
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.

Copyright © Huawei Technologies Co., Ltd.

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, 6
  Interface Number : 1
  Interface list : GigabitEthernet1/0/0
```

Table 12-90 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
```

Table 12-91 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.

Related Topics

12.9.35 ip vpn-instance
12.9.7 description (VPN instance view)
12.9.33 ip binding vpn-instance

Copyright © Huawei Technologies Co., Ltd.

12.9.50 route-distinguisher
12.9.69 vpn-target
12.9.2 apply-label per-instance
12.9.30 import route-policy
12.9.26 export route-policy
12.9.65 tnl-policy
12.9.51 routing-table limit
12.9.48 prefix limit
12.9.38 limit-log-interval

12.9.15 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.	-

Copyright © Huawei Technologies Co., Ltd.

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
```

Table 12-92 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.
VPN-Instance Name and ID	Name and ID of the VPN instance.

Related Topics

12.9.35 ip vpn-instance

12.9.69 vpn-target

 Copyright © Huawei Technologies Co., Ltd.

12.9.16 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

None

Example

Display the details of the tunnel interface.

```
<Huawei> display interface tunnel 0/0/2
Tunnel0/0/2 current state : UP
Line protocol current state : UP
```

 Copyright © Huawei Technologies Co., Ltd.

```
Description:HUAWEI, AR Series, Tunnel0/0/2 Interface
Route Port,The Maximum Transmit Unit is 1500
Internet protocol processing : disabled
Encapsulation is TUNNEL, loopback not set
Tunnel source 10.10.10.1 (GigabitEthernet0/0/1), destination 10.1.1.1
Tunnel protocol/transport GRE/IP, key disabled
keepalive disabled
Checksumming of packets disabled
Current system time: 2012-08-09 18:53:47
    300 seconds input rate 0 bits/sec, 0 packets/sec
    300 seconds output rate 0 bits/sec, 0 packets/sec
    15 seconds input rate 0 bits/sec, 0 packets/sec
    15 seconds output rate 0 bits/sec, 0 packets/sec
    0 packets input,  0 bytes
    0 input error
    0 packets output,  0 bytes
    0 output error
    Input bandwidth utilization  : 0%
    Output bandwidth utilization : 0%
```

Table 12-93 Description of the display interface tunnel command output

Item	Description
Tunnel0/0/2 current state	Physical layer status of the Tunnel0/0/2 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 of the Tunnel0/0/2 interface: ● UP: The link layer protocol of the tunnel interface works normally. ● DOWN: The link layer protocol of the tunnel interface is abnormal.
Description	Description of the tunnel interface.
Route Port,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 protocol processing: disabled	IP protocol is disabled.
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 10.10.10.1 (GigabitEthernet0/0/1)	The source address of the tunnel is 10.10.10.1. That is, the IP address of the GigabitEthernet 0/0/1 interface sending packets at the source side is 10.10.10.1.
destination	Destination address of the tunnel.

 Copyright © Huawei Technologies Co., Ltd.

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. ● IPSec: indicates tunnel mode of IPSec to protect data stream. ● MPLS: encapsulates packets into MPLS packets. ● IPv6 over IPv4: encapsulates IPv6 packets into IPv4 packets. ● IPv4 over IPv6: encapsulates IPv4 packets into IPv6 packets. ● SVPN: encapsulates packets into SVPN 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 disabled	The keepalive function of GRE is not enabled.
Checksumming of packets disabled	The check sum function of GRE is not enabled.
300 seconds input rate 0 bits/sec, 0 packets/sec	Rate of bits and packets received on the interface in the last 300 seconds. **NOTE** If the tunnel encapsulation protocol is SVPN, this field is not supported.
300 seconds output rate 0 bits/sec, 0 packets/sec	Rate of bits and packets sent through the interface in the last 300 seconds. **NOTE** If the tunnel encapsulation protocol is SVPN, this field is not supported.
15 seconds input rate 0 bits/sec, 0 packets/sec	Rate of bits and packets received on the interface during the last query period.
15 seconds output rate 0 bits/sec, 0 packets/sec	Rate of bits and packets sent through the interface during the last query period.
0 packets input, 0 bytes 0 input error	Total packets and bytes received on the interface and the total number of defective packets.
0 packets output, 0 bytes 0 output error	Total packets and bytes sent through the interface and the total number of defective packets.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Input bandwidth utilization	Input bandwidth usage.
Output bandwidth utilization	Output bandwidth usage.

Related Topics

12.3.11 keepalive

12.9.17 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.

NOTE

The AR100&AR120&AR150&AR160&AR200 series do not support this command.

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 iterated 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 iterated 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.

 Copyright © Huawei Technologies Co., Ltd.

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 12-94 Description of the **display l3vpn vpn-list tunnel-policy** command output

Item	Description
Codes	Comments
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

12.9.18 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

 Copyright © Huawei Technologies Co., Ltd.

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 12-95 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

12.9.19 display snmp-agent trap feature-name l3vpn all

Function

The **display snmp-agent trap feature-name l3vpn all** command displays whether the trap function is enabled for the L3VPN module and the excessive trap flag.

Format

display snmp-agent trap feature-name l3vpn all

Parameters

None

Views

All views

 Copyright © Huawei Technologies Co., Ltd.

Default Level

1: Monitoring level

Usage Guidelines

The **display snmp-agent trap feature-name l3vpn all** command displays the following information:

- Trap names supported by the L3VPN module. The trap names are the same as the trap names specified by the **snmp-agent trap enable feature-name l3vpn** command. Each trap name corresponds to a network element abnormality.
- Trap status of the L3VPN module. You can check whether the trap is reported based on the trap name.

Example

Display whether the trap function is enabled for the L3VPN module and the excessive trap flag.

```
<Huawei> display snmp-agent trap feature-name l3vpn all
------------------------------------------------------------------------------
Feature name: l3vpn
Trap number : 6
------------------------------------------------------------------------------
Trap name                      Default switch status   Current switch status
L3VPN_MIB_TRAP_VRF_UP          off                     off
L3VPN_MIB_TRAP_VRF_DOWN        off                     off
L3VPN_MIB_TRAP_THRESH_CLEARED  off                     off
L3VPN_MIB_TRAP_THRESH_EXCEED   off                     off
L3VPN_MIB_TRAP_MID_THRESH_EXCEED
                               off                     off
L3VPN_MIB_TRAP_TUNNEL_UPDOWN_EVENT
                               off                     off
```

Table 12-96 Description of the display snmp-agent trap feature-name l3vpn all command output

Item	Description
Feature name	Name of the module.
Trap number	Number of trap messages.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Trap name	Types of trap messages: • L3VPN_MIB_TRAP_MID_THRESH_EXCEED: The number of VPN routes exceeds the maximum number of route prefixes allowed. • L3VPN_MIB_TRAP_THRESH_CLEARED: The number of VPN routes falls below the threshold. • L3VPN_MIB_TRAP_THRESH_EXCEED: The number of VPN routes exceeds the threshold. • L3VPN_MIB_TRAP_TUNNEL_UPDOWN_EVENT: The status of the tunnel used by a VPN changed. • L3VPN_MIB_TRAP_VRF_DOWN: a trap message indicating a VRF Down event. • L3VPN_MIB_TRAP_VRF_UP: a trap message indicating a VRF Up event.
Default switch status	Default status of a trap message: • on: indicates that the trap function is enabled by default. • off: indicates that the trap function is disabled by default.
Current switch status	Status of a trap message: • on: indicates that the trap function is enabled. • off: indicates that the trap function is disabled.

Related Topics

12.9.54 snmp-agent trap enable feature-name l3vpn

12.9.20 display traffic-statistics vpn-instance

Function

The **display traffic-statistics vpn-instance** command displays the traffic statistics about the specified VPN instance.

NOTE

The AR100&AR120&AR150&AR160&AR200 series do not support this command.

 Copyright © Huawei Technologies Co., Ltd.

Format

display traffic-statistics vpn-instance *vpn-instance-name*

Parameters

Parameter	Description	Value
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

Run this command to view the statistics about traffic of the specified VPN instance.

Example

Display the statistics about the VPN instance named **vpna**.

```
<Huawei> display traffic-statistics vpn-instance vpna
 vpn-instance name: vpna
 Statistics last cleared: 0000-00-00 00:00:00
 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
 Input:
   Unicast: 0 packets, Multicast: 0 packets
   Broadcast: 0 packets
 Output:
   Unicast: 0 packets, Multicast: 0 packets
   Broadcast: 0 packets
```

Table 12-97 Description of the **display traffic-statistics vpn-instance** command output

Item	Description
vpn-instance name	Name of a VPN instance
Statistics last cleared	Time when statistics are cleared last time
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	Total number of received bytes and packets

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Output	Total number of sent bytes and packets
Unicast	Number of unicast packets
Multicast	Number of multicast packets
Broadcast	Number of broadcast packets

Related Topics

12.9.49 reset traffic-statistics vpn-instance

12.9.21 display tunnel-info

Function

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

NOTE

The AR100&AR120&AR150&AR160&AR200 series do not support this command.

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 interface boards.	-

Views

All views

Default Level

1: Monitoring level

Copyright © Huawei Technologies Co., Ltd.

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 detail 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 router.

Example

View information about the GRE tunnel.

```
<Huawei> display tunnel-info tunnel-id 10003
Tunnel ID:                0x10003
Tunnel Token:               3
Type:                   gre
Destination:              10.1.1.1
Out Slot:                 0
Instance ID:               0
Interface:                Tunnel0/0/1
```

Table 12-98 Description of the display tunnel-info 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, 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 router sends packets.
Instance ID	VPN instance ID (0 indicates that a tunnel is a public network tunnel).
Interface	Local tunnel interface.

Display all tunnel information.

```
<Huawei> display tunnel-info all
* -> Allocated VC Token
Tunnel ID          Type               Destination          Token
------------------------------------------------------------------------------
0x1800800          lsp                3.3.3.3              0
0x1800801          lsp                2.2.2.2              1
0x41804bb8          lsp                192.168.2.0           3000
```

Display tunnel statistics.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> display tunnel-info statistics
LSP/32bit LSP :                    3/3
GRE :                              0
CRLSP :                            2
LOCAL IFNET :                      0
MPLS LOCAL IFNET :                 0
VPN QOS LSP :                      0
Reserved :                         0
```

Table 12-99 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.

Display tunnel statistics in the order of interface boards.

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

Table 12-100 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.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
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.

12.9.22 display tunnel-policy

Function

The **display tunnel-policy** command displays the configurations of tunnel policies.

NOTE

The AR100&AR120&AR150&AR160&AR200 series do not support this command.

Format

display tunnel-policy [*tunnel-policy-name*]

Parameters

Parameter	Description	Value
tunnel-policy-name	Specifies the name of tunnel policy. If *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:          2
```

 Copyright © Huawei Technologies Co., Ltd.

```
Sel-Seq tunnel policy num:              1
Binding tunnel policy num:              1
Invalid tunnel policy num:              0
Tunnel Policy Name  Select-Seq                    Load balance No
------------------------------------------------------------------------------
po2                 CR-LSP LSP                    1

Tunnel Policy Name  Destination     Tunnel Intf               Ignore-dest-check   Down switch
------------------------------------------------------------------------------------------------
po1                 1.1.1.1         Tunnel0/0/2               Disable             Disable
```

Table 12-101 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:2
Tunnel Policy Name                Destination     Tunnel Intf      Ignore-dest-check   Down Switch
-------------------------------------------------------------------------------------------------------
tep                               2.2.2.2         Tunnel0/0/2      Enable              Disable
                                                  Tunnel0/0/3
                                  3.3.3.3         Tunnel0/0/2      Enable              Disable
                                                  Tunnel0/0/3
```

 Copyright © Huawei Technologies Co., Ltd.

Table 12-102 Description of the display tunnel-policy tunnel-policy-name command output

Item	Description
The number of binding	Number of the bound destination addresses.

Related Topics

12.9.63 tunnel-policy (system view)

12.9.23 display tunnel-policy-config

Function

The **display tunnel-policy-config** command displays the configuration of tunnel policies.

NOTE

The AR100&AR120&AR150&AR160&AR200 series do not support this command.

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.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> display tunnel-policy-config
#
tunnel-policy sel-1
 tunnel select-seq cr-lsp lsp load-balance-number 1
#
tunnel-policy bind-1 tunnel binding destination 1.1.1.1 te Tunnel0/0/1 down-switch
#
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
```

Related Topics

12.9.63 tunnel-policy (system view)

12.9.24 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.

NOTE

The AR100&AR120&AR150&AR160&AR200 series do not support this command.

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

 Copyright © Huawei Technologies Co., Ltd.

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 200 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
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 12-103 Description of the **display tunnel-policy subscriber statistics** command output

Item	Description
The specified tunnel policy does not exist. Total 200 applications subscribed the tunnel policy.	The tunnel policy does not exist and is used by 200 applications.
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.

12.9.25 display tunnel-selector

Function

The **display tunnel-selector** command displays the configurations of tunnel selectors of a system.

 Copyright © Huawei Technologies Co., Ltd.

NOTE

The AR100&AR120&AR150&AR160&AR200 series do not support this command.

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 12-104 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

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

12.9.59 tunnel-selector (system view)

12.9.26 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**

 Copyright © Huawei Technologies Co., Ltd.

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
```

Related Topics

12.9.30 import route-policy

12.9.27 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.

 Copyright © Huawei Technologies Co., Ltd.

NOTE

The AR100&AR120&AR150&AR160&AR200 series do not support this command.

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 32 case-sensitive characters without spaces. The value must start with a letter (case sensitive).
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 in the following scenarios:

- The ASBR or SPE in inter-AS VPN Option B or HVPN networking needs to apply a tunnel policy to VPNv4 routes to, for example, have the VPNv4 routes iterated to MPLS TE tunnels.
- The PE in inter-AS VPN Option C networking needs to apply a tunnel policy to BGP-IPv4 labeled routes to, for example, have the BGP-IPv4 labeled routes iterated 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.

 Copyright © Huawei Technologies Co., Ltd.

Prerequisite

The **12.9.59 tunnel-selector (system view)** 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 **12.9.1 apply tunnel-policy (tunnel-selector view)** 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
```

Related Topics

19.7.4 acl (system view)
19.7.3 acl name
12.9.1 apply tunnel-policy (tunnel-selector view)
9.9.47 ip ip-prefix
12.9.59 tunnel-selector (system view)

12.9.28 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*

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
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

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** command is configured but the **ip ip-prefix aa** command is not configured, all routes will be permitted.
- 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.

Configuration Impact

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] tunnel-selector policy permit node 10
[Huawei-tunnel-selector] if-match ip-prefix p1
```

 Copyright © Huawei Technologies Co., Ltd.

12.9.29 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
```

Related Topics

9.9.48 ip ipv6-prefix

 Copyright © Huawei Technologies Co., Ltd.

12.9.30 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.

 Copyright © Huawei Technologies Co., Ltd.

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
```

Related Topics

12.9.26 export route-policy

12.9.31 ingress-lsp trigger

Function

The **ingress-lsp trigger** command specifies a routing policy to control the creation of ingress LSPs based on labeled BGP IPv4 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

The AR100&AR120&AR150&AR160&AR200 series do not support this command.

Format

ingress-lsp trigger route-policy *route-policy-name*

 Copyright © Huawei Technologies Co., Ltd.

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.

Configuration Impact

If the **ingress-lsp trigger** command is run more than once, the latest configuration overrides the previous ones.

Follow-up Procedure

If the routing policy specified in the **ingress-lsp trigger** command does not exist, you need to configure the routing policy by using the **route-policy** command.

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
```

Related Topics

9.9.53 route-policy

 Copyright © Huawei Technologies Co., Ltd.

12.9.32 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*

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
interface-number	Specifies the number of the tunnel interface with format "slot/subslot/number".	The slot, subslot, or interface number is an integer. The value range of the slot or subslot number varies according to the device type. The value of the interface number ranges. • AR100&AR120&AR150&AR160&AR200 series: 0 to 255 • AR1200 series, AR2201-48FE, AR2202-48FE, AR2204, AR2204E, AR2204E-D: 0 to 255 • AR2220, AR2220E: 0 to 1023 • AR2204XE, AR2204XE-DC, AR2240 (using SRU40, SRU60, or SRU80), AR2240C, AR3200 (using SRU40, SRU60, or SRU80) series: 0 to 2047 • AR2240 (using SRU200, or SRU200E, or SRU400), AR3200 (using SRU200, or SRU200E, or SRU400) series: 0 to 4095 • AR3600 (using SRUX5) series: 0 to 4095

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

 Copyright © Huawei Technologies Co., Ltd.

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
- IPSec
- 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

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, IPSec, IPv4 over IPv6, or IPv6 over IPv4 tunnel, run the **source** and **destination** commands.

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

If a tunnel is being used, services transmitted over the tunnel will be affected after the tunnel interface is deleted. Exercise caution when running the **undo interface tunnel** command.

Example

Create a tunnel interface.

```
<Huawei> system-view
[Huawei] interface tunnel 0/0/1
[Huawei-Tunnel0/0/1]
```

12.9.33 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.

 Copyright © Huawei Technologies Co., Ltd.

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 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

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

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.

Binding an interface to a VPN instance or deleting the binding will result in the deletion of the IP address of the interface, Layer 3 features, and IP-related routing protocols. 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.

 Copyright © Huawei Technologies Co., Ltd.

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
Info: All IPv4 related configurations on this interface are removed!
Info: All IPv6 related configurations on this interface are removed!
```

Related Topics

12.9.14 display ip vpn-instance

12.9.34 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

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

Usage Scenario

When there are private network routes generated by multiple types of routing protocols in a VPN instance enabled with the IPv4 address family, the **ip frr** command can be used to enable IP FRR to immediately switch traffic among routes and ensure the normal forwarding of traffic if certain routes are faulty. The following example shows how IP FRR works:

There are two routes to 1.1.1.1. One is a BGP route with priority 150, and the other one is a static route with priority 60. When IP FRR is not enabled, the static route is preferred. After IP FRR is enabled, the static route functions as the primary route, and the BGP route functions as the backup route. If the static route fails, the system immediately switches traffic to the BGP route to ensure the normal forwarding of traffic.

Precautions

The **ip frr** command must be used together with the **apply backup-interface** and **apply backup-nexthop** commands.

Only one route-policy can be configured every time you use the **ip frr** command. If you run the command multiple times, only the latest configuration takes effect. The configuration in the system view is independent of the configuration in the VPN instance view.

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 gigabitethernet 1/0/0
[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
```

12.9.35 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*

 Copyright © Huawei Technologies Co., Ltd.

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.

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 and consumes resources on the PE.

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.

After the **undo ip vpn-instance** command is used to delete a VPN instance, all configurations of this VPN instance are deleted.

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 or IPv6 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.

 Copyright © Huawei Technologies Co., Ltd.

- 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]
```

Related Topics

12.9.50 route-distinguisher

12.9.36 ipv4-family (VPN instance view)

12.9.37 ipv6-family (VPN instance view)

12.9.69 vpn-target

12.9.14 display ip vpn-instance

12.9.36 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

 Copyright © Huawei Technologies Co., Ltd.

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 and perform VPN configurations in the address family view if you want to have IPv4 VPN routes advertised and IPv4 VPN data forwarded.

Follow-up Procedure

Run the **route-distinguisher** command to configure an RD for the IPv4 address family of the VPN instance. VPN configurations can be performed in the IPv4 address family view only after an RD is configured for the IPv4 address family of the VPN instance.

Precautions

Configurations of the commands run in the VPN instance view, except the **description** 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]
```

12.9.37 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

 Copyright © Huawei Technologies Co., Ltd.

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]
```

Related Topics

12.9.35 ip vpn-instance

12.9.38 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

 Copyright © Huawei Technologies Co., Ltd.

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 address family of a VPN instance reach the maximum, no more routes can be added to the routing table of the IPv4 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
```

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

12.9.51 routing-table limit
12.9.48 prefix limit
12.9.14 display ip vpn-instance
9.10.9 display ip routing-table limit

12.9.39 lsp-trigger bgp-label-route

Function

The **lsp-trigger bgp-label-route** command enables LDP to allocate labels to labeled BGP routes on the public network.

The **undo lsp-trigger bgp-label-route** command restores the default setting.

By default, LDP does not allocate labels to labeled BGP routes on the public network.

NOTE

The AR100&AR120&AR150&AR160&AR200 does not support this command.

Format

lsp-trigger bgp-label-route [**ip-prefix** *ip-prefix-name*]

undo lsp-trigger bgp-label-route

Parameters

Parameter	Description	Value
ip-prefix *ip-prefix-name*	Specifies the name of the IP prefix list that triggers the labeled BGP routes on the public network to set up LDP LSPs.	The value is an existing IP prefix list name.

Views

MPLS view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Both the **lsp-trigger bgp-label-route** command and the **lsp-trigger** command can be used to configure policies to trigger the establishment of LDP LSPs. The former command is used for labeled BGP routes on the public network, and the latter command is used for static routes and IGP routes.

 Copyright © Huawei Technologies Co., Ltd.

NOTE

Modifying the LSP-triggering policy during the LDP GR period is invalid.

Prerequisites

MPLS has been enabled globally using the **mpls (system view)** command.

Precautions

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 public-network labeled BGP routes trigger LDP LSP establishment.

Example

Trigger the establishment of LDP LSPs according to labeled BGP routes on the public network.

```
<Huawei> system-view
[Huawei] mpls
[Huawei-mpls] lsp-trigger bgp-label-route
```

Related Topics

11.1.67 lsp-trigger

12.9.40 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.

NOTE

The AR100&AR120&AR150&AR160&AR200 series do not support this command.

Format

mpls te reserved-for-binding

undo mpls te reserved-for-binding

Parameters

None

Views

Tunnel interface view

 Copyright © Huawei Technologies Co., Ltd.

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 iterated 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 Tunnel0/0/1 for VPN binding.

```
<Huawei> system-view
[Huawei] interface tunnel 0/0/1
[Huawei-Tunnel0/0/1] tunnel-protocol mpls te
[Huawei-Tunnel0/0/1] mpls te reserved-for-binding
```

Delete the configuration of a tunnel that is reserved for VPN binding.

```
<Huawei> system-view
[Huawei] interface tunnel 0/0/1
[Huawei-Tunnel0/0/1] undo mpls te reserved-for-binding
```

Related Topics

12.9.58 tunnel binding

12.9.41 mtu (tunnel interface view)

Function

The **mtu** command sets the Maximum Transmission Unit (MTU) of a tunnel interface.

The **undo mtu** command restores the default value.

By default, the MTU is 1500 bytes on a tunnel interface.

 Copyright © Huawei Technologies Co., Ltd.

Format

mtu *mtu*

undo mtu

Parameters

Parameter	Description	Value
mtu	Specifies the MTU of a tunnel interface.	An integer ranging from 128 to 9202, in bytes.

Views

Tunnel interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The size of data frames is limited at the network layer. Any time the IP layer receives an IP packet to be sent, it checks to which local interface the packet needs to be sent and obtains the MTU configured on the interface. Then the IP layer compares the MTU with the packet length. If the packet length is longer than the MTU, the IP layer fragments the packet into smaller packets, which are shorter than or equal to the MTU.

If unfragmentation is configured, some packets may be discarded during data transmission at the IP layer. To ensure jumbo packets are not dropped during transmission, you need to configure forcible fragmentation. In this case, you can run the **mtu** command to set the size of a fragment.

Precautions

Set the MTU for a tunnel interface based on actual networking. The default value is recommended. If a small MTU is used but the packet size is large, packets may be divided into many fragments. Then the packets are discarded by QoS queues. If a large MTU is used, packets may be transmitted at a low rate.

If IPv6 is run on a tunnel interface and the MTU set using the **mtu** command on the interface is smaller than 1280, IPv6 works abnormally on this interface. To prevent this problem, set the MTU of a tunnel interface to a value greater than or equal to 1280 if IPv6 runs on the tunnel interface.

After running the **mtu** command, run the **shutdown** and then **undo shutdown** commands on the interface. The set MTU then can take effect.

On a network with IPv4 over IPv6 tunnels, if a tunnel interface is Down, the MTU value of the tunnel interface 64000 does not take effect. After the tunnel interface goes Up, the system dynamically refreshes the MTU value of the tunnel interface

 Copyright © Huawei Technologies Co., Ltd.

based on the Path_MTU of the tunnel and IPv6 MTU of the tunnel outbound interface. If the Path_MTU does not exist, the system adopts the MTU of the tunnel outbound interface as the MTU of the tunnel interface.

On a network with Ethernet over GRE tunnels, the MTU configured on a tunnel interface takes effect for Layer 3 traffic but not Layer 2 traffic.

The **mtu** *mtu* command configuration on a TE tunnel interface takes effect for packets sent by hosts only in the following scenarios:

- In an L3VPN over TE scenario, if the length of a packet that a host sends exceeds the configured MTU value, the packet is fragmented based on the MTU value at the IP layer before being forwarded.
- In a TE tunnel scenario, the length of a tunnel detection packet must be less than the configured MTU value.

Example

Set the MTU of Tunnel 0/0/1 to 1492.

```
<Huawei> system-view
[Huawei] interface tunnel 0/0/1
[Huawei-Tunnel0/0/1] mtu 1492
[Huawei-Tunnel0/0/1] shutdown
[Huawei-Tunnel0/0/1] undo shutdown
```

Related Topics

12.9.16 display interface tunnel

12.9.42 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.

NOTE

The AR100&AR120&AR150&AR160&AR200 series do not support this command.

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*

 Copyright © Huawei Technologies Co., Ltd.

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.
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

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

 Copyright © Huawei Technologies Co., Ltd.

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
```

Related Topics

12.9.44 peer upe

9.8.24 default-route imported

12.9.43 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-VPNv4 address family.

NOTE

The AR100&AR120&AR150&AR160&AR200 series do not support this command.

Format

peer { *group-name* | *ipv4-address* } **mpls-local-ifnet disable**

undo peer { *group-name* | *ipv4-address* } **mpls-local-ifnet disable**

 Copyright © Huawei Technologies Co., Ltd.

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

In the IPv4 VPN Option C scenario, EBGP peer relationships are established between BGP peers. The BGP peers can be endpoint PEs in the VPN Option C 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, traffic is iterated 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
```

12.9.44 peer upe

Function

The **peer upe** command specifies a BGP peer or peer group as UPE of HoVPN.

 Copyright © Huawei Technologies Co., Ltd.

The **undo peer upe** command cancels the configuration.

NOTE

The AR100&AR120&AR150&AR160&AR200 series do not support this command.

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.
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

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.

 Copyright © Huawei Technologies Co., Ltd.

- 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.

The BGP peer relationship is interrupted after you run the **peer upe** command. So, confirm the action before you use the command.

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
```

Related Topics

9.8.135 peer route-policy

12.9.42 peer default-originate vpn-instance

12.9.45 peer soo

Function

The **peer soo** command configures the Source 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**

 Copyright © Huawei Technologies Co., Ltd.

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.

Copyright © Huawei Technologies Co., Ltd.

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 or 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. As a result, different sites of the same VPN cannot communicate. The **peer substitute-**

 Copyright © Huawei Technologies Co., Ltd.

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
```

Related Topics

12.9.46 peer substitute-as

12.9.46 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* } **substitute-as**

undo peer { *group-name* | *ipv4-address* } **substitute-as**

 Copyright © Huawei Technologies Co., Ltd.

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.

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

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 **9.8.101 peer as-number** command to create a peer or configure an AS number for a specified peer group.

Precautions

Enabling BGP AS number substitution may cause route loops in a CE multi-homing network. The **peer soo** command must be run to prevent a routing loop in a VPN site.

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
```

 Copyright © Huawei Technologies Co., Ltd.

```
[Huawei-bgp-vpn1] peer 10.1.1.2 as-number 200
[Huawei-bgp-vpn1] peer 10.1.1.2 substitute-as
```

Related Topics

12.9.45 peer soo

12.9.47 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.

NOTE

The AR100&AR120&AR150&AR160&AR200 series do not support this command.

Format

policy vpn-target

undo policy vpn-target

Parameters

None

Views

BGP-VPNv4 address family view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In the networking of BGP/MPLS IP VPN, 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
- 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.

 Copyright © Huawei Technologies Co., Ltd.

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
```

12.9.48 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. **NOTE** The maximum number of unicast prefixes allowed on a PE is determined by the license but is not specified through the **prefix limit** command. The total number of VPN route prefixes and public network route prefixes cannot exceed *number*. If the total number exceeds *number*, the route management module denies the subsequent route prefixes and generates an alarm.	The value is an integer, and the minimum value is 1. The maximum number is determined by the license file.

 Copyright © Huawei Technologies Co., Ltd.

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.

Prerequisites

 Copyright © Huawei Technologies Co., Ltd.

The **12.9.50 route-distinguisher** command has been executed to set the RD of the VPN instance.

Precautions

After the command is run, the excess route prefixes of the current VPN instance address family will be discarded.

If the number of route prefixes exceeds the set limit and the **undo prefix limit** command is run, the system will receive the route prefixes from routing tables generated by protocols to create a private network routing table.

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.

When the number of prefixes exceeds the upper limit, the **prefix limit** command with **simply-alert** specified enables the device to display only alarms and allows the device to add prefixes to the routing table.

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
```

Related Topics

9.8.134 peer route-limit

12.9.51 routing-table limit

12.9.14 display ip vpn-instance

9.10.9 display ip routing-table limit

12.9.49 reset traffic-statistics vpn-instance

Function

The **reset traffic-statistics vpn-instance** command clears traffic statistics about the specified VPN instance.

NOTE

The AR100&AR120&AR150&AR160&AR200 series do not support this command.

 Copyright © Huawei Technologies Co., Ltd.

Format

reset traffic-statistics vpn-instance { **name** *vpn-instance-name* | **all** }

Parameters

Parameter	Description	Value
name *vpn-instance-name*	Specifies the name of a VPN instance.	The value is the name of an existing VPN instance.
all	Clears the traffic statistics about all VPN instances.	-

Views

User view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Run this command to clear L3VPN traffic statistics when you need to collect new traffic statistics.

Precautions

Statistics cannot be restored after being cleared. Therefore, use this command with caution.

Example

Clear statistics about traffic of the VPN instance with the name of **vpn1**.

```
<Huawei> reset traffic-statistics vpn-instance name vpn1
```

Clear statistics about traffic of all the VPN instances.

```
<Huawei> reset traffic-statistics vpn-instance all
Warning: Traffic-statistics information will be cleared! Continue? [Y/N]:y
```

Related Topics

12.9.20 display traffic-statistics vpn-instance

12.9.50 route-distinguisher

Function

The **route-distinguisher** command configures a route distinguisher (RD) for a VPN instance address family.

 Copyright © Huawei Technologies Co., Ltd.

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

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After you create a VPN instance and enable the address family, run this command to configure an RD for the VPN instance address family.

 Copyright © Huawei Technologies Co., Ltd.

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 VPN IPv4 or IPv6 route.

Precautions

Execution of this command will also enable the IPv4 address family.

When the CE is dual-homed, the RDs on the PEs must be globally unique to ensure routing.

Once the RD is configured for the VPN instance address family, it cannot be modified or deleted. To change an RD, you need to delete the VPN instance identified by the RD or disable the VPN instance address family. Then, reconfigure the VPN instance and its RD.

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
```

Related Topics

12.9.35 ip vpn-instance

12.9.14 display ip vpn-instance

12.9.51 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

 Copyright © Huawei Technologies Co., Ltd.

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.

Prerequisites

1. The **ip vpn-instance** command has been executed to create a VPN instance and enter the VPN instance view.

 Copyright © Huawei Technologies Co., Ltd.

2. The **ipv4-family** command has been executed to 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

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.

Follow-up Procedure

When the number of routes reaches the upper limit, run the **undo routing-table limit** command to allow the system to receive routes from routing tables of various protocols and to establish a private IP routing table.

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
```

Related Topics

9.8.134 peer route-limit

12.9.48 prefix limit

12.9.14 display ip vpn-instance

9.10.9 display ip routing-table limit

12.9.52 rr-filter

Function

The **rr-filter** command creates a reflection policy for the route reflectors.

The **undo rr-filter** command removes the configuration.

 Copyright © Huawei Technologies Co., Ltd.

NOTE

The AR100&AR120&AR150&AR160&AR200 series do not support this command.

By default, no reflection policy for a route reflectors 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 or BGP-MDT 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.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> system-view
[Huawei] bgp 100
[Huawei-bgp] ipv4-family vpnv4
[Huawei-bgp-af-vpnv4] rr-filter 10
```

12.9.53 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 an L3VPN service, 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.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> system-view
[Huawei] ip vpn-instance vrf1
[Huawei-vpn-instance-vrf1] service-id 123
```

12.9.54 snmp-agent trap enable feature-name l3vpn

Function

The **snmp-agent trap enable feature-name l3vpn** command enables the trap function for the L3VPN module.

The **undo snmp-agent trap enable feature-name l3vpn** command disables the trap function for the L3VPN module.

By default, the trap function for the L3VPN module is disabled.

Format

snmp-agent trap enable feature-name l3vpn [**trap-name** { **l3vpn_mib_trap_mid_thresh_exceed** | **l3vpn_mib_trap_thresh_cleared** | **l3vpn_mib_trap_thresh_exceed** | **l3vpn_mib_trap_tunnel_updown_event** | **l3vpn_mib_trap_vrf_down** | **l3vpn_mib_trap_vrf_up** }]

undo snmp-agent trap enable feature-name l3vpn [**trap-name** { **l3vpn_mib_trap_mid_thresh_exceed** | **l3vpn_mib_trap_thresh_cleared** | **l3vpn_mib_trap_thresh_exceed** | **l3vpn_mib_trap_tunnel_updown_event** | **l3vpn_mib_trap_vrf_down** | **l3vpn_mib_trap_vrf_up** }]

Parameters

Parameter	Description	Value
trap-name	Enables the traps of L3VPN events of specified types.	-
l3vpn_mib_trap_mid_thresh_exceed	Enables the trap of the event indicating that the number of private route prefixes exceeds the middle threshold which is set by the **prefix limit** command.	-
l3vpn_mib_trap_thresh_cleared	Enables the trap of the event indicating that the number of private route prefixes falls below the threshold which is set by the **prefix limit** command.	-
l3vpn_mib_trap_thresh_exceed	Enables the trap of the event indicating that the number of private route prefixes exceeds the upper limit which is set by the **prefix limit** command.	-

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
l3vpn_mib_trap_tunnel_updown_event	Enables the trap of the event indicating that the status of the tunnel used by a VPN changed.	-
l3vpn_mib_trap_vrf_down	Enables the trap of VRF Down event.	-
l3vpn_mib_trap_vrf_up	Enables the trap of VRF Up event.	-

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

The Simple Network Management Protocol (SNMP) is a standard network management protocol widely used on TCP/IP networks. It uses a central computer (a network management station) that runs network management software to manage network elements. The management agent on the network element automatically reports traps to the network management station. After that, the network administrator immediately takes measures to resolve the problem.

The **snmp-agent trap enable feature-name l3vpn** command enables the trap function for L3VPN modules.

Precautions

To enable the trap function of one or more types of trap messages, specify **trap-name**.

Example

Enable the trap of VRF Down event in the system view.

```
<Huawei> system-view
[Huawei] snmp-agent trap enable feature-name l3vpn trap-name l3vpn_mib_trap_vrf_down
```

Disable the trap of VRF Down event in the system view.

```
<Huawei> system-view
[Huawei] undo snmp-agent trap enable feature-name l3vpn trap-name l3vpn_mib_trap_vrf_down
```

Related Topics

12.9.19 display snmp-agent trap feature-name l3vpn all

 Copyright © Huawei Technologies Co., Ltd.

12.9.55 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 { [**vpn-instance** *vpn-instance-name*] *source-ip-address* | *interface-type interface-number* }

undo source

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Specifies the name of the VPN instance that the source address of a tunnel belongs to. **NOTE** You can specify the parameter only when the encapsulation mode of a tunnel interface is set to IPSec or mGRE.	The value is the name of an existing VPN instance.
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.	-

Views

Tunnel interface view, Tunnel-Template interface view

Copyright © Huawei Technologies Co., Ltd.

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When configuring a tunnel, you must 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, IPSec, 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.

IPv6 over IPv4, IPv4 over IPv6, and GRE tunnels are bidirectional tunnels. The source address of the local tunnel interface is the destination address of the remote tunnel interface by the **destination** command, and the destination address of the local tunnel interface is the source address of the remote tunnel interface.

Two or more tunnel interfaces that use the same encapsulation protocol cannot be configured with the same source and destination addresses. Two or more GRE tunnel interfaces in a system can have the same source address and same destination address. The system uses GRE keys to identify these GRE tunnel interfaces. When two or more tunnel interfaces on a P2MP tunnel are configured with the same source address, run the **gre key** command to set the key number of each tunnel interface.

You can also specify VPN instance parameters while specifying the source address for an IPSec tunnel or an mGRE tunnel in IPSec/mGRE over VPN scenarios.

Example

Set the tunnel type of Tunnel0/0/1 to IPv6 over IPv4 manual tunnel and configure the source IP address of Tunnel0/0/1 as 10.1.1.1.

```
<Huawei> system-view
[Huawei] interface tunnel 0/0/1
[Huawei-Tunnel0/0/1] tunnel-protocol ipv6-ipv4
[Huawei-Tunnel0/0/1] source 10.1.1.1
```

Configure Tunnel0/0/2 of mGRE and use Loopback0 address as the interface address.

```
<Huawei> system-view
[Huawei] interface loopback 0
[Huawei-LoopBack0] ip address 10.2.1.1 32
[Huawei-LoopBack0] quit
[Huawei] interface tunnel 0/0/2
[Huawei-Tunnel0/0/2] tunnel-protocol gre p2mp
[Huawei-Tunnel0/0/2] source loopback 0
```

 Copyright © Huawei Technologies Co., Ltd.

12.9.56 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.

NOTE

The AR100&AR120&AR150&AR160&AR200 series do not support this command.

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.

 Copyright © Huawei Technologies Co., Ltd.

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       ?
```

BGP supernet routes include BGP supernet labeled routes and BGP supernet unicast routes. In V2R3C00 or earlier, a BGP device does not advertise received BGP supernet labeled routes. After the BGP device is upgraded to a later version, the BGP device can advertise received BGP supernet labeled routes to other BGP peers. This advertisement may change the traffic path on the network before and after the upgrade. To ensure that the traffic path remains unchanged, run the **supernet label-route advertise disable** command to disable the BGP device from advertising BGP supernet labeled routes.

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
```

12.9.57 traffic-statistics enable

Function

The **traffic-statistics enable** command enables traffic statistics for a VPN instance family.

The **undo traffic-statistics enable** command disables traffic statistics for a VPN instance family.

By default, traffic statistics is disabled for a VPN instance family.

NOTE

The AR100&AR120&AR150&AR160&AR200 series do not support this command.

Format

traffic-statistics enable

undo traffic-statistics enable

Parameters

None

 Copyright © Huawei Technologies Co., Ltd.

Views

VPN instance view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If you want to collect statistics about the traffic received or sent by a VPN instance family as a basis for VPN traffic monitoring or accounting, run the **traffic-statistics enable** command to enable traffic statistics for the VPN instance family.

Follow-up Procedure

After running the **traffic-statistics enable** command, you can use the **display traffic-statistics vpn-instance** command to view statistics about the traffic of the VPN instance family.

The **reset traffic-statistics vpn-instance** command can be used to clear the collected traffic statistics.

Example

Enable traffic statistics for the family of a VPN instance named **vpna**.

```
<Huawei> system-view
[Huawei] ip vpn-instance vpna
[Huawei-vpn-instance-vpna] traffic-statistics enable
```

Related Topics

12.9.20 display traffic-statistics vpn-instance

12.9.49 reset traffic-statistics vpn-instance

12.9.58 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.

NOTE

The AR100&AR120&AR150&AR160&AR200 series do not support this command.

Format

tunnel binding destination *dest-ip-address* **te** { **tunnel** *interface-number* } &<1-16> [**ignore-destination-check**] [**down-switch**]

 Copyright © Huawei Technologies Co., Ltd.

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 iteration 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, and then GRE, 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.

 Copyright © Huawei Technologies Co., Ltd.

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 iterated to the bound MPLS TE tunnel.

Example

Bind the IP address of the remote PE, 10.2.2.9, to the local tunnel interface Tunnel0/0/1 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 0/0/1
```

Related Topics

12.9.40 mpls te reserved-for-binding

12.9.63 tunnel-policy (system view)

12.9.61 tunnel select-seq

12.9.59 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.

NOTE

The AR100&AR120&AR150&AR160&AR200 series do not support this command.

Format

tunnel-selector *tunnel-selector-name* { **permit** | **deny** } **node** *node*

undo tunnel-selector *tunnel-selector-name* [**node** *node*]

 Copyright © Huawei Technologies Co., Ltd.

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.
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 ASBR in the VPN Option B networking needs to apply a tunnel policy to VPNv4 routes that are received from PEs although VPN instances are not configured on it.
- The SPE in the HoVPN networking needs to apply a tunnel policy to VPNv4 routes that are received from UPEs.

 Copyright © Huawei Technologies Co., Ltd.

- The PE in the VPN Option C networking needs to apply a tunnel policy to BGP labeled routes advertised to remote PEs.

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 **12.9.1 apply tunnel-policy (tunnel-selector view)** command.

In addition, the system will have routes iterated to expected tunnels only after applying a tunnel selector. The **12.9.60 tunnel-selector (BGP view)** 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 be iterated 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]
```

Related Topics

12.9.25 display tunnel-selector

12.9.60 tunnel-selector (BGP 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 routes are only iterated to LSPs.

NOTE

The AR100&AR120&AR150&AR160&AR200 series do not support this command.

Format

tunnel-selector *tunnel-selector-name*

undo tunnel-selector

 Copyright © Huawei Technologies Co., Ltd.

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 view, BGP-IPv4 unicast address family view or 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 ASBR in the VPN Option B networking needs to apply a tunnel policy to VPNv4 routes that are received from PEs although VPN instances are not configured on it.
- The SPE in the HVPN networking needs to apply a tunnel policy to VPNv4 routes that are received from UPEs.
- The PE in the VPN Option C networking needs to apply a tunnel policy to BGP labeled routes advertised to remote PEs.

Prerequisites

The **12.9.59 tunnel-selector (system view)** 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 be iterated to tunnels.

Example

Apply a tunnel selector to BGP labeled routes.

```
<Huawei> system-view
[Huawei] bgp 100
[Huawei-bgp] ipv4-family unicast
[Huawei-bgp-af-ipv4] tunnel-selector tps
```

 Copyright © Huawei Technologies Co., Ltd.

12.9.61 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.

NOTE

The AR100&AR120&AR150&AR160&AR200 series do not support this command.

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.	-
lsp	Specifies the LDP LSPs, BGP LSP or static LSPs.	-
cr-lsp	Specifies the CR-LSP tunnel.	-
load-balance-number	Specifies the number of tunnels taking part in load balancing.	• The value of this parameter can only range from 1 to 4 on the AR1200 series, AR2201-48FE, AR2202-48FE, AR2204E, AR2204E-D, and AR2204. • The value of this parameter can only range from 1 to 8 on the AR2220, AR2220E, AR2240, AR2240C, AR3200, and AR3600 series.

Views

Tunnel policy view

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

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.

Example

Configure a tunnel policy that only LDP LSPs, BGP LSP or static LSPs can be used. Set the number of tunnels taking part in load balancing to 2.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> system-view
[Huawei] tunnel-policy l2
[Huawei-tunnel-policy-l2] tunnel select-seq lsp load-balance-number 2
```

Related Topics

12.9.58 tunnel binding

12.9.63 tunnel-policy (system view)

12.9.62 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.

 Copyright © Huawei Technologies Co., Ltd.

Example

Indicates that a nonexistent tunnel policy can be specified in a command.

```
<Huawei> system-view
[Huawei] tunnel-policy nonexistent-config-check disable
```

12.9.63 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.

NOTE

The AR100&AR120&AR150&AR160&AR200 series do not support this command.

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:

 Copyright © Huawei Technologies Co., Ltd.

- 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 iteration 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]
```

Related Topics

12.9.22 display tunnel-policy

12.9.58 tunnel binding

12.9.61 tunnel select-seq

12.9.64 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** [**p2mp**] | **ipsec** | **ipv6-ipv4** [**6to4** | **auto-tunnel** | **isatap**] | **ipv4-ipv6** | **mpls te** | **svpn** [**p2p** | **p2mp**] | **none** }

undo tunnel-protocol

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
gre	Indicates that the GRE tunnel protocol is configured on a tunnel interface.	-
gre p2mp	Indicates that the mGRE tunnel protocol is configured on a tunnel interface. If this parameter is not used, the tunnel protocol configured on a tunnel interface is a traditional point-to-point GRE.	-
ipsec	Indicates that the IPSec tunnel protocol is configured on a tunnel interface.	-
ipv4-ipv6	Indicates that the IPv4 to IPv6 tunnel protocol is configured on a tunnel interface.	-
ipv6-ipv4	Configures the tunnel protocol of the tunnel interface as ipv6-ipv4 and uses a manual IPv6 over IPv4 tunnel.	-
ipv6-ipv4 6to4	Indicates that the IPv6 to IPv4 tunnel protocol is configured on a tunnel interface using 6to4.	-
ipv6-ipv4 auto-tunnel	Configures the tunnel protocol of the tunnel interface as ipv6-ipv4 and uses an automatic IPv6 over IPv4 tunnel.	-
ipv6-ipv4 isatap	Indicates that the IPv6 to IPv4 tunnel protocol is configured on a tunnel interface using isatap.	-
mpls te	Indicates that the MPLS TE tunnel protocol is configured on a tunnel interface. **NOTE** The AR100&AR120&AR150&AR160&AR200 does not support this parameter.	-
svpn [**p2p** | **p2mp**]	Indicates that the SVPN tunnel protocol is configured on a tunnel interface. • **p2p**: indicates the P2P SVPN tunnel protocol. • **p2mp**: indicates the P2MP SVPN tunnel protocol.	-
none	Indicates that no tunnel protocol is configured on a tunnel interface.	-

Views

Tunnel interface view, Tunnel-Template interface view

 Copyright © Huawei Technologies Co., Ltd.

NOTE

The tunnel template interface view supports the **ipsec** and **none** parameters only.

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. When the **p2mp** parameter is specified following **gre**, you can set the tunnel encapsulation mode to P2MP GRE. The destination address of a P2MP GRE tunnel does not need to be manually configured. Instead, the destination address of this tunnel can either be defined by a protocol (for example, NHRP in a DSVPN scenario) or be dynamically learned.
- IPSec: protects the security of data transmitted on the Internet by establishing tunnels using the IPSec protocol.
- 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.
- SVPN: binds multiple WAN access lines to provide high bandwidth and highly reliable networks for customers.
  - When the SVPN mode is set to Hub-Spoke, specify **p2p** on the Spoke and **p2mp** on the hub when configuring a tunnel protocol.
  - When the SVPN mode is set to Lone Ranger, you must not specify **p2p** or **p2mp**.

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. When an SVPN proposal is bound to a tunnel interface, you cannot modify the tunnel encapsulation mode.

 Copyright © Huawei Technologies Co., Ltd.

Example

Set the tunnel encapsulation mode of Tunnel0/0/2 to mGRE.

```
<Huawei> system-view
[Huawei] interface tunnel 0/0/2
[Huawei-Tunnel0/0/2] tunnel-protocol gre p2mp
```

Set the tunnel encapsulation mode of Tunnel0/0/2 to GRE.

```
<Huawei> system-view
[Huawei] interface tunnel 0/0/2
[Huawei-Tunnel0/0/2] tunnel-protocol gre
```

Related Topics

12.9.32 interface tunnel

12.9.65 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.

NOTE

The AR100&AR120&AR150&AR160&AR200 series do not support this command.

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

 Copyright © Huawei Technologies Co., Ltd.

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 iterated to tunnels based on the default tunnel policy. If the iteration 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
```

Related Topics

12.9.63 tunnel-policy (system view)

 Copyright © Huawei Technologies Co., Ltd.

12.9.14 display ip vpn-instance

12.9.66 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.

Format

transit-vpn

undo transit-vpn

Parameters

None.

Views

VPN instance view or VPN instance IPv4 address family view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

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 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
```

 Copyright © Huawei Technologies Co., Ltd.

```
[Huawei-vpn-instance-vpna] ipv4-family
[Huawei-vpn-instance-vpna-af-ipv4] route-distinguisher 100:1
[Huawei-vpn-instance-vpna-af-ipv4] transit-vpn
```

12.9.67 undo vpn frr all

Function

Using the **undo vpn frr all** command, you can disable VPN FRR in all the VPN instances.

NOTE

The AR100&AR120&AR150&AR160&AR200 series do not support this command.

Format

undo vpn frr all

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

When running the **undo vpn frr all** command in the system view, you can disable VPN FRR in all the VPN instances.

Example

Disable VPN FRR of all the VPN instances in the system view.

```
<Huawei> system-view
[Huawei] undo vpn frr all
```

Related Topics

12.9.70 vpn frr

12.9.68 vpn-route cross multipath

Function

The **vpn-route cross multipath** command adds multiple VPNv4 routes to a VPN instance with a different RD from these routes' RDs.

 Copyright © Huawei Technologies Co., Ltd.

The **undo vpn-route cross multipath** command restores the default configuration.

By default, if the RDs of multiple VPNv4 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

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 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 routes to a VPN instance with a different RD from these routes' RDs. The number of VPNv4 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 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 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
```

 Copyright © Huawei Technologies Co., Ltd.

```
[Huawei-bgp] ipv4-family vpn-instance vrf1
[Huawei-bgp-vrf1] vpn-route cross multipath
```

12.9.69 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**] }

 Copyright © Huawei Technologies Co., Ltd.

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.	-
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

 Copyright © Huawei Technologies Co., Ltd.

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 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 route can be added to the routing table of the local VPN instance enabled with the IPv4 or IPv6 address family.

Prerequisites

The **12.9.50 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
```

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

12.9.14 display ip vpn-instance

12.9.70 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.

NOTE

The AR100&AR120&AR150&AR160&AR200 series do not support this command.

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, VPN instance IPv6 address family view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If a PE is connected to two other PEs, running the **vpn frr** command in the VPN instance address family view of the PE enables VPN FRR and improves network reliability. After VPN FRR is configured, traffic can switch to the secondary LSP immediately after the primary LSP becomes faulty.

The **undo vpn frr all** command is run in the system view, and the **undo vpn frr** command is run in the VPN instance view.

 Copyright © Huawei Technologies Co., Ltd.

NOTE

When running the **undo vpn frr all** command in the system view, you can disable VPN FRR in all the VPN instances.

Prerequisites

The **12.9.50 route-distinguisher** command has been executed to set the RD of the VPN instance.

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 2.2.2.9
[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
```

Related Topics

12.9.67 undo vpn frr all

12.10 EVPN Configuration Commands

NOTE

Only the AR100, AR120, AR150, AR160 (except AR161EW, AR161EW-M1, AR169EW, AR169EGW-L), AR200, AR1200series, AR2220E support EVPN.

12.10.1 advertise l2vpn evpn

Function

The **advertise l2vpn evpn** command enables a VPN instance to advertise IP routes to a BGP EVPN address family.

The **undo advertise l2vpn evpn** command restores the default configuration.

By default, a VPN instance is disabled from advertising IP routes to a BGP EVPN address family.

Format

advertise l2vpn evpn

undo advertise l2vpn evpn

Parameters

None

 Copyright © Huawei Technologies Co., Ltd.

Views

BGP-VPN instance IPv4 address family view

Default Level

2: Configuration level

Usage Guidelines

If IP prefix routes are used to establish tunnels between VXLAN tunnel endpoints (VTEPs) and advertise host routes, run the **advertise l2vpn evpn** command in the BGP-VPN instance IPv4 address family view to enable a VPN instance to advertise IP routes to the BGP EVPN address family. This configuration allows the host routes collected by the VPN instance to be sent to the BGP EVPN address family and then sent to the remote VTEPs through EVPN BGP peer relationships.

Example

Enable a VPN instance named **vpna** to advertise IP routes to the BGP EVPN address family.

```
<Huawei> system-view
[Huawei] bgp 100
[Huawei-bgp] ipv4-family vpn-instance vpna
[Huawei-bgp-vpna] advertise l2vpn evpn
```

12.10.2 display bgp evpn routing-table

Function

The **display bgp evpn routing-table** command displays information about EVPN routes.

Format

display bgp evpn all routing-table [**statistics**]

display bgp evpn { **all** | **route-distinguisher** *route-distinguisher* } **routing-table** { **inclusive-route** [*inclusive-route*] | **mac-route** [*mac-route*] | **prefix-route** [*prefix-route*] }

Parameters

Parameter	Description	Value
all	Displays information about EVPN routes of all EVPN instances.	-
statistics	Displays statistics about EVPN routes.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
route-distinguisher *route-distinguisher*	Displays information about EVPN routes with a specified route distinguisher (RD).	RD has the following four formats: ● 16-bit AS number:32-bit user-defined number. For example, 101:3. The AS number is an integer ranging from 0 to 65535, and the user-defined number is an integer ranging from 0 to 4294967295. The AS number and user-defined number cannot be both 0s. 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, and 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. ● 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.
inclusive-route	Displays information about inclusive multicast routes.	-
inclusive-route	Specifies an inclusive multicast route.	The value is in the format of M:L:X.X.X.X, where: ● M is fixed at 0. ● X.X.X.X indicates the source address configured for the device originating the route. ● L indicates the mask length of the source address configured for the device originating the route.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
mac-route	Displays information about MAC advertisement routes.	-
mac-route	Specifies a MAC advertisement route.	The value is in the format of E:M:H-H-H:L:X.X.X.X, where: ● E indicates the ID of the VLAN to which the MAC address belongs. ● M is fixed at 48, indicating the length of the MAC address. ● H-H-H indicates the MAC address. Each H represents a 4-bit hexadecimal number. The system prefixes the number with zeros if fewer than four bits are entered. For example, if you enter e0, 00e0 is displayed. ● L is fixed at 32, indicating the mask length of the IP address corresponding to the MAC address. ● X.X.X.X indicates the IP address corresponding to the MAC address.
prefix-route	Displays information about IP prefix routes.	-
prefix-route	Specifies an IP prefix route.	The value is in the format of L:X.X.X.X:M, where: ● L is fixed at 0. ● X.X.X.X indicates the IP address of host routes. ● M indicates the mask length of host routes.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Information about specified EVPN routes can be displayed by specifying different parameters.

Copyright © Huawei Technologies Co., Ltd.

Example

Display information about all EVPN routes.

```
<Huawei> display bgp evpn all routing-table
Local AS number :100

 BGP Local router ID is 1.1.1.1
 Status codes: * - valid, > - best, d - damped,
               h - history,  i - internal, s - suppressed, S - Stale
               Origin : i - IGP, e - EGP, ? - incomplete


 EVPN address family:
 Number of Mac Routes : 2
 Route Distinguisher: 1:1


       Network(EthTagId/MacAddrLen/MacAddr/IpAddrLen/IpAddr)  NextHop
 *>     0:48:a4dc-be0f-99a6:0:0.0.0.0                        9.9.9.9
 *>     0:48:a4dc-be0f-99a6:32:9.9.9.9                       9.9.9.9

 VPN-Instance vpn1, Router ID 1.1.1.1:

 Total Number of Routes: 1
     Network            NextHop        MED        LocPrf    PrefVal Path/Ogn

  i  9.9.9.9/32         9.9.9.9                   100        0      ?

 EVPN address family:
 Number of Inclusive Multicast Routes : 1
 Route Distinguisher: 1:1


       Network(EthTagId/IpAddrLen/OriginalIp)               NextHop
 *>     0:32:9.9.9.9                                      9.9.9.9

 EVPN address family:
 Number of Ip Prefix Routes : 1
 Route Distinguisher: 1:1


       Network(EthTagId/IpPrefix/IpPrefixLen)               NextHop
 *>     0:9.9.9.0:24                                      9.9.9.9

 VPN-Instance vpn1, Router ID 1.1.1.1:

 Total Number of Routes: 1
     Network            NextHop        MED        LocPrf    PrefVal Path/Ogn

  i  9.9.9.0/24         9.9.9.9        0          100        0       ?
```

Table 12-105 Description of the **display bgp evpn all routing-table** command output

Item	Description
Local AS number	Local AS number of the EVPN routes
BGP Local router ID	Router ID of the local BGP device
Number of Mac Routes	Number of MAC advertisement routes
Route Distinguisher	RD of the EVPN routes

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Network	Reachable address
NextHop	Next hop address
VPN-Instance	VPN instance name
Router ID	ID of a router
Total Number of Routes	Total number of EVPN routes
MED	Metric of the EVPN routes
LocPrf	Local preference of the EVPN routes
PrefVal	Preferred value of a routing protocol
Path/Ogn	Path and Origin attributes of the AS of the EVPN routes
Number of Inclusive Multicast Routes	Number of inclusive multicast routes
Number of Ip Prefix Routes	Number of IP prefix routes

12.10.3 display bgp evpn update-peer-group

Function

The **display bgp evpn update-peer-group** command displays information about BGP update peer-groups in the EVPN address family.

Format

display bgp evpn update-peer-group [**index** *update-peer-group-index*]

Parameters

Parameter	Description	Value
index *update-peer-group-index*	Specifies the index of a BGP update peer-group.	The value is an integer.

Views

All views

Default Level

1: Monitoring level

Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

When a VXLAN network is deployed using BGP EVPN, to view information about the update peer-group with a specified index in the EVPN address family, run the **display bgp evpn update-peer-group** command.

Example

Display information about all BGP update peer-groups in the EVPN address family.

```
<Huawei> display bgp evpn update-peer-group

 The EVPN instance's update peer group number : 1
 Keep buffer update peer group number : 0
 BGP Version : 4

 Group ID : 0
 Group Type : internal
 Addr Family : L2-EVPN
 AdvMinTimeVal : 0
 Total Peers : 2
 Leader Peer : 5.5.5.5
 Peers List : 5.5.5.5          4.4.4.4
```

Display information about the BGP update peer-group with the index 0 in the EVPN address family.

```
<Huawei> display bgp evpn update-peer-group index 0

 Group ID : 0
 BGP Version : 4
 Group Type : internal
 Addr Family : L2-EVPN
 AdvMinTimeVal : 0
 Total Peers : 1
 Leader Peer : 1.1.1.1

 Total format packet number : 85
 Total send packet number : 85
 Total replicate packet number : 0
 The replication percentages(%) : 0

 Peers List : 1.1.1.1
```

Table 12-106 Description of the **display bgp evpn update-peer-group** command output

Item	Description
The EVPN instance's update peer group number	Number of update peer-groups in the EVPN instance
Keep buffer update peer group number	Number of update peer-groups stored in the buffer
BGP Version	BGP version
Group ID	ID of the BGP update peer-group

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Group Type	Type of a BGP update peer-group: • external: EBGP update peer-group • internal: IBGP update peer-group • external-confed: EBGP update peer-group in the confederation • internal-confed: IBGP update peer-group in the confederation • unknown: unknown update peer-group
Addr Family	Address family
AdvMinTimeVal	Minimum interval at which Update messages with the same route prefix are sent, in seconds
Total Peers	Total number of BGP peers in the update peer-group
Leader Peer	Leader peer in the update peer-group
Total format packet number	Number of Update messages of a single peer sends in the update peer-group
Total send packet number	Number of Update messages sent to all BGP peers in the update peer-group
Total replicate packet number	Absolute value of the difference between Total send packet number and Total format packet number, that is, absolute value of the difference between the number of Update messages that are sent to all peers in the update peer-group and the number of Update messages sent to a single peer in the update peer-group
The replication percentages(%)	Percentage of the number of replicated Update messages to the total number of sent Update messages, that is, (Total send packet number – Total format packet number)/Total send packet number
Peers List	BGP peer list, displaying the IP addresses of all peers in the update peer-group

 Copyright © Huawei Technologies Co., Ltd.

12.10.4 export route-policy evpn

Function

The **export route-policy evpn** command associates the VPN instance IPv4 address family with an export route-policy to filter the EVPN routes that the VPN instance IPv4 address family advertises to the EVPN address family.

The **undo export route-policy evpn** command dissociates the VPN instance IPv4 address family from an export route-policy.

By default, the VPN instance IPv4 address family is not associated with any export route-policy.

Format

export route-policy *policy-name* **evpn**

undo export route-policy *policy-name* **evpn**

Parameters

Parameter	Description	Value
policy-name	Specifies the name of the export route-policy with which the VPN instance IPv4 address family is associated.	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 or VPN instance IPv4 address family view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

By default, the VPN instance IPv4 address family adds all EVPN-VPN targets in the export EVPN-VPN target list to routes when advertising the routes to the EVPN address family. To control route advertisement more precisely, run the **export route-policy** *policy-name* **evpn** command to associate the VPN instance IPv4 address family with an export route-policy and set attributes for eligible routes.

Prerequisites

An RD has been configured for the VPN instance IPv4 address family using the **route-distinguisher** *route-distinguisher* command.

Configuration Impact

 Copyright © Huawei Technologies Co., Ltd.

The VPN instance IPv4 address family can be associated with only one export route-policy. If the **export route-policy evpn** command is run more than once, the latest configuration overrides the previous one.

Configuration of the **export route-policy evpn** command does not affect the export route-policy applied to a VPN instance using the **export route-policy** *policy-name* command.

Precautions

If the route-policy with which the VPN instance IPv4 address family is associated does not exist, run the **route-policy** command to configure the route-policy.

Example

Associate a VPN instance named **vrf1** with an export route-policy named **policy-2** to filter EVPN routes that the VPN instance IPv4 address family advertises to other VPN instances.

```
<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 policy-2 evpn
```

12.10.5 import route-policy evpn

Function

The **import route-policy evpn** command associates the VPN instance IPv4 address family with an import route-policy that is used to filter the EVPN routes imported from the EVPN address family.

The **undo import route-policy evpn** command dissociates the VPN instance IPv4 address family from an import route-policy.

By default, the VPN instance IPv4 address family is not associated with any import route-policy.

Format

import route-policy *policy-name* **evpn**

undo import route-policy *policy-name* **evpn**

Parameters

Parameter	Description	Value
policy-name	Specifies the name of the import route-policy with which the VPN instance IPv4 address family is associated.	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.

 Copyright © Huawei Technologies Co., Ltd.

Views

VPN instance view or VPN instance IPv4 address family view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

By default, the VPN instance IPv4 address family matches the export EVPN-VPN targets of received routes against its import EVPN-VPN targets to determine whether to import these routes. To control route import more precisely, run the **import route-policy** *policy-name* **evpn** command to associate the VPN instance IPv4 address family with an import route-policy and set attributes for eligible routes.

Prerequisites

An RD has been configured for the VPN instance IPv4 address family using the **route-distinguisher** *route-distinguisher* command.

Configuration Impact

The VPN instance IPv4 address family can be associated with only one import route-policy. If the **import route-policy evpn** command is run more than once, the latest configuration overrides the previous one.

Configuration of the **import route-policy evpn** command does not affect the import route-policy applied to a VPN instance using the **import route-policy** *policy-name* command.

Precautions

If the route-policy with which the VPN instance IPv4 address family is associated does not exist, run the **route-policy** command to configure the route-policy.

Example

Associate a VPN instance named **vrf1** with an import route-policy named **policy-1** to filter EVPN routes imported from other VPN instances to the VPN instance IPv4 address family.

```
<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 policy-1 evpn
```

12.10.6 peer advertise

Function

The **peer advertise** command enables a device to advertise ARP or IRB routes to a BGP EVPN peer.

 Copyright © Huawei Technologies Co., Ltd.

The **undo peer advertise** command restores the default configuration.

By default, a device does not advertise ARP or IRB routes to a BGP EVPN peer.

Format

peer { *ipv4-address* | *group-name* } **advertise** { **arp** | **irb** }

undo peer { *ipv4-address* | *group-name* } **advertise** { **arp** | **irb** }

Parameters

Parameter	Description	Value
ipv4-address	Specifies the IPv4 address of a BGP peer.	The value is in dotted decimal notation.
group-name	Specifies the name of a peer group.	The value is a string of 1 to 47 case-sensitive characters, spaces not supported.
arp	Advertises ARP routes.	-
irb	Advertises IRB routes.	-

Views

BGP-EVPN address family view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To enable a device to advertise ARP or IRB routes to a BGP EVPN peer, run the **peer advertise** command. Advertising ARP or IRB routes allows a VXLAN tunnel to be established between VTEPs and suppresses ARP flooding on the network. Advertising IRB routes additionally allows the advertisement of host routes between the VTEPs.

Precautions

The **arp** and **irb** parameters are mutually exclusive in the BGP-EVPN address family view.

Example

Enable a device to advertise ARP routes to a BGP EVPN peer.

```
<Huawei> system-view
[Huawei] bgp 100
[Huawei-bgp] l2vpn-family evpn
[Huawei-bgp-af-evpn] peer 1.1.1.1 advertise arp
```

 Copyright © Huawei Technologies Co., Ltd.

12.10.7 peer advertise route-reoriginated

Function

The **peer advertise route-reoriginated** command enables a device to advertise IP prefix routes re-encapsulated by the EVPN address family to a BGP EVPN peer.

The **undo peer advertise route-reoriginated** command restores the default configuration.

By default, the local device does not advertise IP prefix routes re-encapsulated by the EVPN address family to a BGP EVPN peer.

Format

peer { *ipv4-address* | *group-name* } **advertise route-reoriginated evpn ip**

undo peer { *ipv4-address* | *group-name* } **advertise route-reoriginated evpn ip**

Parameters

Parameter	Description	Value
ipv4-address	Specifies the IPv4 address of a BGP EVPN peer.	The value is in dotted decimal notation.
group-name	Specifies the name of a BGP EVPN 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.
evpn	Re-encapsulates the received EVPN routes.	-
ip	Re-encapsulates the IP prefix routes in the received EVPN routes.	-

Views

BGP-EVPN address family view

Default Level

2: Configuration level

Task Name and Operations

Task Name	Operations
bgp	write

Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

Usage Scenario

In three-segment VXLAN scenarios, to re-encapsulate EVPN routes received from a DC into IP prefix routes and then send them to the BGP EVPN peer in another DC, run the **peer advertise route-reoriginated** command. This configuration allows communication between VMs in different DCs.

During EVPN route re-encapsulation, a border leaf node receives an EVPN route from a DC and changes the route next hop to the VTEP address of the leaf node. Additionally, the leaf node replaces the source MAC address in the gateway MAC attribute of the host route with its own MAC address and the L3VNI with that of an L3VPN instance.

Prerequisites

The device has been enabled to add a regeneration flag to the routes received from BGP EVPN peers using the **peer** { *ipv4-address* | *group-name* } **import reoriginate** command.

Example

Enable a device to advertise regenerated IP prefix routes to a BGP EVPN peer.

```
<Huawei> system-view
[Huawei] bgp 100
[Huawei-bgp] peer 2.2.2.2 as-number 100
[Huawei-bgp] l2vpn-family evpn
[Huawei-bgp-af-evpn] peer 2.2.2.2 enable
[Huawei-bgp-af-evpn] peer 2.2.2.2 import reoriginate
[Huawei-bgp-af-evpn] peer 2.2.2.2 advertise route-reoriginated evpn ip
```

12.10.8 peer import reoriginate

Function

The **peer import reoriginate** command enables a device to add a regeneration flag to the routes received from BGP EVPN peers.

The **undo peer import reoriginate** command restores the default configuration.

By default, a device does not add a regeneration flag to the routes received from BGP EVPN peers.

Format

peer { *ipv4-address* | *group-name* } **import reoriginate**

undo peer { *ipv4-address* | *group-name* } **import reoriginate**

Parameters

Parameter	Description	Value
ipv4-address	Specifies the IPv4 address of a BGP EVPN peer.	The value is in dotted decimal notation.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
group-name	Specifies the name of a BGP EVPN 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.

Views

BGP-EVPN address family view

Default Level

2: Configuration level

Task Name and Operations

Task Name	Operations
bgp	write

Usage Guidelines

Usage Scenario

In a three-segment VXLAN scenario, an edge node that connects to a carrier network does not re-encapsulate the routes received from BGP EVPN peers, causing the EVPN routes to be terminated on the edge node. As a result, the EVPN routes from one DC cannot be advertised to the BGP EVPN peers of another DC. To address this problem, run the **peer import reoriginate** command to enable the edge node to add a regeneration flag to the routes received from BGP EVPN peers. The edge node then re-encapsulates the EVPN routes received from one DC before sending them to another DC for inter-DC VM communication.

Prerequisites

A device has been enabled to exchange routes with a specified peer or peer group using the **peer** { *group-name* | *ipv4-address* } **enable** command.

Example

Enable a device to add a regeneration flag to the routes received from BGP EVPN peers.

```
<Huawei> system-view
[Huawei] bgp 100
[Huawei-bgp] peer 1.1.1.1 as-number 100
[Huawei-bgp] l2vpn-family evpn
[Huawei-bgp-af-evpn] peer 1.1.1.1 enable
[Huawei-bgp-af-evpn] peer 1.1.1.1 import reoriginate
```

 Copyright © Huawei Technologies Co., Ltd.

12.10.9 l2vpn-family evpn

Function

The **l2vpn-family evpn** command enables the BGP-EVPN address family and displays the BGP-EVPN address family view.

The **undo l2vpn-family evpn** command deletes the BGP-EVPN address family view.

By default, the BGP-EVPN address family is disabled, and the BGP-EVPN address family is not displayed.

NOTE

Only AR121, AR129, AR129CV, AR129CVW, AR129CGVW-L, AR160 series (except AR161EW, AR161EW-M1, AR169EW, AR169EGW-L, AR161W, AR169W, and AR169CGVW-L), AR200 series, AR1220E, AR1220EV, AR1220EVW, AR1220F, and AR2220E support this command.

Format

l2vpn-family evpn

undo l2vpn-family evpn

Parameters

None

Views

BGP view

Default Level

2: Configuration level

Usage Guidelines

Before you perform configurations in the BGP-EVPN address family view, run the **l2vpn-family evpn** command to enable the BGP-EVPN address family and display the BGP-EVPN address family view.

Example

Enable the BGP-EVPN address family and display the BGP-EVPN address family view.

```
<Huawei> system-view
[Huawei] bgp 100
[Huawei-bgp] l2vpn-family evpn
[Huawei-bgp-af-evpn]
```

Related Topics

9.8.12 bgp

 Copyright © Huawei Technologies Co., Ltd.

12.10.10 peer mac-limit

Function

The **peer mac-limit** command configures the maximum number of MAC advertisement routes allowed to be received from a peer.

The **undo peer mac-limit** command restores the default configuration.

By default, the number of MAC advertisement routes allowed to be received from a peer is not limited.

Format

peer { *group-name* | *ipv4-address* } **mac-limit** *mac-limit* [**idle-forever** | **idle-timeout** *times*]

undo peer { *group-name* | *ipv4-address* } **mac-limit**

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.	The value is in dotted decimal notation.
mac-limit	Specifies the maximum number of MAC advertisement routes allowed to be received from each peer.	-
idle-forever	Indicates that a connection that is interrupted after the maximum number of routes allowed have been received cannot be automatically re-established.	-
idle-timeout *times*	Specifies a timer for re-establishing a connection if the connection is interrupted after the maximum number of routes allowed have been received. Before the timer expires, the system does not re-establish a connection.	The value is an integer ranging from 1 to 1200, in minutes.

Views

BGP-EVPN address family view

 Copyright © Huawei Technologies Co., Ltd.

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If an EVPN instance imports many invalid MAC advertisement routes from peers and these routes occupy a large proportion of the total number of MAC advertisement routes, run the **peer mac-limit** command to configure the maximum number of MAC advertisement routes allowed to be received from each peer.

Configuration Impact

After this command is run, excess route prefixes of the BGP-EVPN address family may be discarded.

If the **undo peer mac-limit** command is run after the number of received MAC advertisement routes exceeds the specified maximum number, the system receives route prefixes from PEs again to construct the EVPN BGP routing table.

Example

Set the maximum number of MAC advertisement routes allowed to be received from the peer 2.2.2.2 to 1000.

```
<Huawei> system-view
[Huawei] bgp 100
[Huawei-bgp] l2vpn-family evpn
[Huawei-bgp-af-evpn] peer 2.2.2.2 mac-limit 1000
```

12.10.11 peer route-policy (BGP-EVPN address family view)

Function

route-policy

The **undo peer route-policy** deletes a specified route-policy.

By default, no route-policy is specified to filter routes received from an EVPN BGP peer or peer group or routes to be advertised to an EVPN BGP peer or peer group.

Format

peer { *group-name* | *ipv4-address* } **route-policy** *route-policy-name* { **import** | **export** }

undo peer { *group-name* | *ipv4-address* } **route-policy** *route-policy-name* { **import** | **export** }

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
group-name	Specifies the name of an EVPN 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 an EVPN BGP peer.	The value is in dotted decimal notation.
route-policy-name	Specifies the name of a 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.
import	Applies a route-policy to routes received from an EVPN BGP peer or peer group.	-
export	Applies a route-policy to routes advertised to an EVPN BGP peer or peer group.	-

Views

BGP-EVPN address family view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After a route-policy is created, you can run the **peer route-policy** command to apply the route-policy to an EVPN BGP peer or peer group so that the routes advertised to or received from the peer or peer group can be controlled. To be specific, only the necessary routes are advertised to or received from the peer or peer group. This configuration streamlines route management, reduces the routing table scale, and minimizes network resource consumption.

Prerequisites

EVPN BGP peers or peer groups have been enabled to exchange route information using the **peer** { *group-name* | *ipv4-address* } **enable** command.

Configuration Impact

If a route-policy is specified for an EVPN BGP peer group, all the members in the group inherit this configuration.

Copyright © Huawei Technologies Co., Ltd.

Precautions

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, all routes are advertised to the specified peer, or all routes received from the specified peer are accepted.

Example

Apply a route-policy named **test-rp** to the routes received from the EVPN BGP peer 1.1.1.9.

```
<Huawei> system-view
[Huawei] bgp 100
[Huawei-bgp] peer 1.1.1.9 as-number 200
[Huawei-bgp] l2vpn-family evpn
[Huawei-bgp-af-evpn] peer 1.1.1.9 enable
[Huawei-bgp-af-evpn] peer 1.1.1.9 route-policy test-rp import
```

12.10.12 policy vpn-target (BGP-EVPN address family view)

Function

The **policy vpn-target** command enables EVPN-VPN target-based filtering for received EVPN routes.

The **undo policy vpn-target** command disables EVPN-VPN target-based filtering for received EVPN routes.

By default, EVPN-VPN target-based filtering is enabled for received EVPN routes.

Format

policy vpn-target

undo policy vpn-target

Parameters

None

Views

BGP-EVPN address family view

Default Level

2: Configuration level

Usage Guidelines

To enable EVPN-VPN target-based filtering for EVPN routes, run the **policy vpn-target** command. This configuration allows received EVPN routes to be filtered based on an EVPN-VPN target. For example, if an export EVPN-VPN target in the

 Copyright © Huawei Technologies Co., Ltd.

received EVPN routes matches the local import EVPN-VPN target, the EVPN routes is accepted.

Example

Enable EVPN-VPN target-based filtering for received EVPN routes.

```
<Huawei> system-view
[Huawei] bgp 100
[Huawei-bgp] l2vpn-family evpn
[Huawei-bgp-af-evpn] policy vpn-target
```

12.10.13 refresh bgp evpn

Function

The **refresh bgp evpn** command configures EVPN BGP soft reset to allow EVPN BGP connections to be softly reset.

Format

refresh bgp evpn { **all** | *ipv4-address* | **group** *group-name* | **external** | **internal** } { **export** | **import** }

Parameters

Parameter	Description	Value
all	Softly resets all EVPN BGP connections.	-
ipv4-address	Specifies the IPv4 address of an EVPN BGP peer.	The value is in dotted decimal notation.
group *group-name*	Specifies an EVPN 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	Specifies the EVPN peer of an EBGP connection.	-
internal	Specifies the EVPN peer of an IBGP connection.	-
export	Softly resets EVPN BGP connections in the outbound direction.	-
import	Softly resets EVPN BGP connections in the inbound direction.	-

 Copyright © Huawei Technologies Co., Ltd.

Views

User view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To softly reset EVPN BGP connections, run the **refresh bgp evpn** command. EVPN BGP soft reset allows the system to refresh an EVPN BGP routing table without tearing down the EVPN BGP connections and to apply a new filtering policy.

With a delay configured for BGP to apply a route-policy,

- If an import policy is configured to filter the routes learned from a peer or peer group using the **peer route-policy import** command, BGP applies the import policy immediately when the **refresh bgp evpn all** command is run.
- If an export policy is configured to filter the routes to be sent to a peer or peer group using the **peer route-policy export** command, BGP does not apply the export policy even if the **refresh bgp evpn all** command is run.

Prerequisites

The route-refresh function has been enabled for EVPN BGP peers.

Example

Softly reset all EVPN BGP connections in the inbound direction so that new configurations can take effect.

```
<Huawei> refresh bgp evpn all import
```

Related Topics

9.8.121 peer keep-all-routes

12.10.11 peer route-policy (BGP-EVPN address family view)

12.10.14 vpn-target evpn

Function

The **vpn-target evpn** command configures EVPN-VPN targets for the VPN instance IPv4 address family.

The **undo vpn-target evpn** command deletes the EVPN-VPN targets configured for the VPN instance IPv4 address family.

By default, no EVPN-VPN targets are configured for the VPN instance IPv4 address family.

 Copyright © Huawei Technologies Co., Ltd.

Format

vpn-target { *vpn-target* &<1-8> [**both** | **export-extcommunity** | **import-extcommunity**] } **evpn**

undo vpn-target { **all** | *vpn-target* &<1-8> [**both** | **export-extcommunity** | **import-extcommunity**] } **evpn**

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
vpn-target	Specifies the EVPN-VPN targets to be added to the EVPN-VPN target list of the VPN instance IPv4 address family.	The value can be in one of the following four formats: • 16-bit AS number:32-bit user-defined number. For example, 1:3. The AS number is an integer ranging from 0 to 65535, and the user-defined number is an integer ranging from 0 to 4294967295. The AS number and user-defined number cannot be both 0s. That is, the EVPN-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, and a user-defined number ranges from 0 to 65535. The AS number and user-defined number cannot be both 0s. That is, the EVPN-VPN target value 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, the EVPN-VPN target value cannot be 0.0:0.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
both	Adds specified EVPN-VPN targets to both the import and export EVPN-VPN target lists of the VPN instance IPv4 address family. If you do not specify **both**, **export-extcommunity**, or **import-extcommunity**, EVPN-VPN targets are added to both the import and export EVPN-VPN target lists by default.	-
export-extcommunity	Adds specified EVPN-VPN targets to the export EVPN-VPN target list of the VPN instance IPv4 address family.	-
import-extcommunity	Adds specified EVPN-VPN targets to the import EVPN-VPN target list of the VPN instance IPv4 address family.	-
all	Deletes all the EVPN-VPN targets of the VPN instance IPv4 address family.	-

Views

VPN instance view or VPN instance IPv4 address family view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On a VPN instance-configured device, to configure import or export EVPN-VPN targets for the VPN instance IPv4 address family, run the **vpn-target evpn** command.

The EVPN-VPN targets control EVPN route learning between VPN instances. An EVPN-VPN target may be either import or export. An export EVPN-VPN target is contained in an EVPN route to be advertised to a remote EVPN peer. Upon receipt of the EVPN route, the remote EVPN peer compares the received export EVPN-VPN target with the local import EVPN-VPN target to determine whether the

 Copyright © Huawei Technologies Co., Ltd.

EVPN route can be added to the routing table of the local VPN instance IPv4 address family.

Prerequisites

An RD has been configured for the VPN instance IPv4 address family using the **route-distinguisher** command.

Configuration Impact

An EVPN-VPN target configured using the **vpn-target evpn** command does not overwrite any previously configured EVPN-VPN target. If the number of configured EVPN-VPN targets has reached the maximum limit, subsequent EVPN-VPN targets cannot be added any more.

Precautions

Multiple EVPN-VPN targets can be configured for the VPN instance IPv4 address family. One **vpn-target evpn** command can configure a maximum of eight EVPN-VPN targets at a time. To configure more EVPN-VPN targets for a VPN instance, run the **vpn-target evpn** command several times. When EVPN routes are advertised between VPN instances, if one of the EVPN-VPN targets carried in the EVPN routes matches the import EVPN-VPN target of the local VPN instance IPv4 address family, the EVPN routes will be added to the EVPN routing table of the local VPN instance.

Example

Add an EVPN-VPN target with the value 3:3 to the export EVPN-VPN target list and an EVPN-VPN target with the value 4:4 to the import EVPN-VPN target list for the IPv4 address family of 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 evpn
[Huawei-vpn-instance-vrf1-af-ipv4] vpn-target 4:4 import-extcommunity evpn
```

12.11 VLL Configuration Commands

NOTE

The AR100&AR120&AR150&AR160&AR200 series do not support VLL.

12.11.1 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.

 Copyright © Huawei Technologies Co., Ltd.

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.

 Copyright © Huawei Technologies Co., Ltd.

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
```

12.11.2 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.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
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 sprovider 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.

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.

Copyright © Huawei Technologies Co., Ltd.

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
```

Related Topics

12.11.16 display vll ccc

12.11.3 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 • 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.	-

 Copyright © Huawei Technologies Co., Ltd.

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 CCC : 2
up (2), down (0)
Interface                 Encap Type          State    VC Type
GigabitEthernet0/0/2          ethernet            up       ccc
GigabitEthernet0/0/1          ethernet            up       ccc
```

Table 12-107 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 router.
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 • vpls-vc: VPLS connection

Related Topics

12.11.4 display mpls l2vc

 Copyright © Huawei Technologies Co., Ltd.

12.11.12 display mpls static-l2vc

12.11.4 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

 Copyright © Huawei Technologies Co., Ltd.

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 router.

```
<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
```

 Copyright © Huawei Technologies Co., Ltd.

```
NKey                : 15
PW redundancy mode  : frr
AdminPw interface   : --
AdminPw link state  : --
Diffserv Mode       : uniform
Service Class       : be
Color               : --
DomainId            : --
Domain Name         : --
```

Table 12-108 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**. Currently, mPW is not supported on the device.
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 to ignore the impact of AC status changes on the active/standby PWE3 service status is enabled: • enable • disable
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.

Copyright © Huawei Technologies Co., Ltd.

Item	Description
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.
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.

Copyright © Huawei Technologies Co., Ltd.

Item	Description
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.
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.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
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.

```
<Huawei> display mpls l2vc interface ethernet 1/0/0
 *client interface       : Ethernet1/0/0 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                : Ethernet
  destination            : 10.3.3.9
  local group ID         : 0            remote group ID      : 0
  local VC label         : 1024         remote VC label      : 1024
  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
  forwarding entry       : exist
  link state             : up
```

 Copyright © Huawei Technologies Co., Ltd.

```
local VC MTU           : 1500         remote VC MTU        : 1500
local VCCV             : alert ttl lsp-ping bfd
remote VCCV            : alert ttl lsp-ping bfd
local control word     : disable      remote control word  : disable
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 : 0x5
  Backup TNL type      : lsp    , TNL ID : 0x0
create time            : 0 days, 0 hours, 29 minutes, 47 seconds
up time                : 0 days, 0 hours, 4 minutes, 54 seconds
last change time       : 0 days, 0 hours, 4 minutes, 54 seconds
VC last up time        : 2011/09/26 15:29:03
VC total up time       : 0 days, 0 hours, 4 minutes, 54 seconds
CKey                   : 5
NKey                   : 4
PW redundancy mode     : frr
AdminPw interface      : --
AdminPw link state     : --
Diffserv Mode          : uniform
Service Class          : --
Color                  : --
DomainId               : --
Domain Name            : --
```

Table 12-109 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.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
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.
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.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
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.
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
```

 Copyright © Huawei Technologies Co., Ltd.

```
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              : 101
VC Type            : ethernet
VC Label           : 1024
Peer Address       : 10.3.3.9
Group ID           : 0
MTU                : 1500
Control Word       : 0
Notification       : 0
Status Code        : 0
Match Local VC     : MATCH
Max ATM CELLS      : --
TDM RTP Header     : --
TDM Encap Num      : --
TDM Bit Rate       : --
```

Table 12-110 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
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.

Copyright © Huawei Technologies Co., Ltd.

Item	Description
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       : Ethernet1/0/0 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                : Ethernet
  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
```

 Copyright © Huawei Technologies Co., Ltd.

```
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            : --
```

Display information about the dynamic VC on the TDM interface.

```
<Huawei> display mpls l2vc interface serial 2/0/0
 *client interface       : Serial2/0/0 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                : CESoPSN basic mode
  destination            : 10.3.3.9
  local group ID         : 0           remote group ID      : 0
  local VC label         : 1039        remote VC label      : 1045
  local TDM Encap Num    : 8           remote TDM Encap Num : 0
  jitter-buffer          : 8
  idle-code              : ff
  local rtp-header       : disable     remote rtp-header    : disable
  local bit-rate         : 0           remote bit-rate      : 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
```

 Copyright © Huawei Technologies Co., Ltd.

```
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           : --          remote VC MTU       : --
local VCCV             : alert ttl lsp-ping bfd
remote VCCV            : alert ttl lsp-ping bfd
local control word     : disable     remote control word  : disable
tunnel policy name     : --
PW template name       : pe2pe
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 : 0x5
  Backup TNL type      : lsp   , TNL ID : 0x0
create time            : 0 days, 0 hours, 1 minutes, 36 seconds
up time                : 0 days, 0 hours, 1 minutes, 36 seconds
last change time       : 0 days, 0 hours, 1 minutes, 36 seconds
VC last up time        : 2013/11/02 09:30:04
VC total up time       : 0 days, 0 hours, 1 minutes, 36 seconds
CKey                   : 9
NKey                   : 8
PW redundancy mode     : frr
AdminPw interface      : --
AdminPw link state     : --
Diffserv Mode          : pipe
Service Class          : ef
Color                  : green
DomainId               : --
Domain Name            : --
```

Table 12-111 Description of the **display mpls l2vc interface** command output

Item	Description
local TDM Encap Num	Number of encapsulated TDM frames in Circuit Emulation Services over Packet Switch Network (CESoPSN) or Structure-Agnostic Time Division Multiplexing over Packet (SAToP) packets in the TDMoPSN application of the local VC.
remote TDM Encap Num	Number of encapsulated TDM frames in CESoPSN or SAToP packets in the TDMoPSN application of the remote VC. **NOTE** This field is displayed as 0 when the AC interface is a serial interface.
jitter-buffer	Depth of the jitter buffer, that is, the maximum allowed jitter delay.
idle-code	Idle code that is filled manually when a jitter buffer underflow occurs.
local rtp-header	Whether the RTP header is added to the transparently transmitted TDM frames on the local end.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
remote rtp-header	Whether the RTP header is added to the transparently transmitted TDM frames on the remote end.
local bit-rate	Bit rate of the local VC.
remote bit-rate	Bit rate of the remote VC.

Related Topics

12.11.20 mpls l2vc
12.11.7 display mpls l2vpn forwarding-info

12.11.5 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
```

 Copyright © Huawei Technologies Co., Ltd.

```
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 12-112 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
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.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
link state	Status of the VC: • up • down

Related Topics

12.11.20 mpls l2vc

12.11.7 display mpls l2vpn forwarding-info

12.11.6 display mpls l2vc oam-mapping

Function

The **display mpls l2vc oam-mapping** command displays status of an L2VPN AC established by using the LDP signaling and information about the OAM mapping table at the PSN side.

Format

display mpls l2vc oam-mapping [**interface** *interface-type interface-number*]

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Specifies the interface type and number. If this parameter specified, OAM mapping information on the specified VC interface using the LDP signaling is displayed. • *interface-type* specifies the interface type. • *interface-number* specifies the interface number.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After you run the **display mpls l2vc oam-mapping** command, either the following situation will occur:

- If an interface name is specified, detailed OAM mapping information on this interface is displayed.

 Copyright © Huawei Technologies Co., Ltd.

- If no interface name is specified, basic about the OAM mapping information on all interfaces is displayed.

Example

Display OAM mapping information on the VC interface using the LDP signaling.

```
<Huawei> display mpls l2vc oam-mapping
 Interface                 Active VC-ID      VC-status AC-OAM  BFD-for-PW
GigabitEthernet0/0/1          No     100       Primary   Enable  Disable
GigabitEthernet0/0/1          No     101       Secondary Enable  Disable
```

Table 12-113 Description of the **display mpls l2vc oam-mapping** command output

Item	Description
Interface	Type and number of the AC interface.
Active	Whether the PW is in the active state: ● Yes: indicates that the PW is in active state. ● No: indicates that the PW is in inactive state. This field is valid only when primary and secondary PWs coexist.
VC-ID	ID of the local VC.
VC-status	Status of the local PW: ● Primary: indicates the primary PW. ● Secondary: indicates the secondary PW.
AC-OAM	Whether the local PE reports an AC fault to the remote PE through OAM: ● Enable: indicates that the local PE reports an AC fault to the remote PE through OAM. ● Disable: indicates that the local PE does not report an AC fault to the remote PE through OAM.
BFD-for-PW	Whether BFD for PW is enabled on the local PE: ● Enable ● Disable

Display OAM mapping information on GE1/0/0.

```
<Huawei> display mpls l2vc oam-mapping interface gigabitethernet 1/0/0
 AC OAM Info:
```

 Copyright © Huawei Technologies Co., Ltd.

```
 EOAM Type      : 802.3ah
 AC OAM State   : Up
 OAM-mapping    : Enable
PSN info:
 VC-ID          : 100
 VC status      : Primary
 Active State   : Inactive
 Link State     : Down
 BFD for PW     : Disable
 BFD for LSP    : 0    TunnelNum: 0    PSN State : up
 VC-ID          : 101
 VC status      : Secondary
 Active State   : Inactive
 Link State     : Down
 BFD for PW     : Disable
 BFD for LSP    : 0    TunnelNum: 0    PSN State : up
```

Table 12-114 Description of the **display mpls l2vc oam-mapping interface** command output

Item	Description
AC OAM Info	Information about AC OAM to be displayed in the following lines.
ACFD Index	Index of the AC forwarding information.
EOAM Type	Type of the protocol used for fault detection and notification.
AC OAM State	Fault detection status on the local AC: • Up: indicates that AC fault detection is disabled or that AC fault detection is enabled but no AC fault is detected. • Down: indicates that AC fault detection is enabled and an AC fault is detected. • Invalid: indicates that AC fault detection is disabled, and the AC OAM state field is invalid.
OAM-mapping	Whether OAM mapping is enabled on the local PE: • Enable • Disable
PSN info	Information about the PW.
VC-ID	ID of the VC.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
VC status	Status of the PW: • Primary: indicates the primary PW. • Secondary: indicates the secondary PW. • Bypass: indicates the inter-chassis PW. • PW-Bypass: indicates the inter-chassis PW used to protect PW-side links. • AC-Bypass: indicates the inter-chassis PW used to protect AC-side links.
Active state	Whether the PW is in the active state: • Active: indicates that the PW is in active state. • Inactive: indicates that the PW is in inactive state. This field is valid only when primary and secondary PWs coexist. When an AC interface is configured with only one PW, the PW is in active state. If an AC interface is configured with primary and secondary PWs, the primary PW is in active state and the secondary PW is in inactive state. When the primary PW fails, the secondary PW becomes active and the primary PW becomes inactive.
Link State	Link status of the AC interface. • Up: indicates that the interface is Up. • Down: indicates that the interface is Down.
BFD for PW	Whether BFD for PW is enabled on the local PE.
BFD for LSP	Whether BFD is used to detect a tunnel: • zero: indicates that BFD is not used to detect a tunnel. • non-zero: indicates that BFD is used to detect a tunnel.
TunnelNum	Number of tunnels detected by BFD.

Copyright © Huawei Technologies Co., Ltd.

Item	Description
PSN State	• When the tunnel is not detected by BFD, the default status of the tunnel is Up. • When the PW uses the tunnel not detected by BFD, the PSN state is Up.

Related Topics

12.11.24 mpls l2vpn oam-mapping

12.11.7 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

Copyright © Huawei Technologies Co., Ltd.

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 carry 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 12-115 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.
ENTRYTYPE	Type of forwarding entries: • SEND: forwarding entries of L2VPN except CCC • 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.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
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.
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.
```

Related Topics

12.11.4 display mpls l2vc

12.11.8 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.

 Copyright © Huawei Technologies Co., Ltd.

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 12-116 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.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Label blocks (s) released in VPLS BGP connection	Indicates the total number of labels in the label cache for the VPLS BGP connections.

12.11.9 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                   512                0
 L2VPN VC Number                   512                1

 VPWS Capacity Statistics
 Statistics Item              Supported Number     Used Number
 L2VPN Local CCC Number            256                0
 L2VPN SVC Number                  256                0
 L2VPN LDP VC Number               256                1
 L2VPN Switch VC Number            256                0

 VPLS Capacity Statistics
 Statistics Item              Supported Number     Used Number
 L2VPN VSI Number                  512                0
```


Copyright © Huawei Technologies Co., Ltd.

```
L2VPN VSI VC Number          512              0
L2VPN VSI PWG Number          8000             0
```

Table 12-117 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 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
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 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

12.11.10 display mpls l2vpn vpws

Function

The **display mpls l2vpn vpws** command displays information about the VPWS service.

 Copyright © Huawei Technologies Co., Ltd.

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

VPLS 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
                     3.3.3.9:200                 Up     Active   Pri
                         2.2.2.9:201                 Up     Inactive Sec
```

 Copyright © Huawei Technologies Co., Ltd.

Table 12-118 Description of the display mpls l2vpn vpws command output

Item	Description
Access Circuit	Access circuit.
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  verbose

Access circuit     : GigabitEthernet
Interface state    : Up
Protect mode       : FRR

Members:
Virtual Circuit              States Active   Role
3.3.3.9:200                  Up     Active   Primary
2.2.2.9:201                  Up     Inactive Secondary

Primary:
 VC type              : LDP VC
 VC state             : up
 Peer IP              : 3.3.3.9
 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              : 2.2.2.9
 VC ID                : 201
```

 Copyright © Huawei Technologies Co., Ltd.

```
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 12-119 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.

 Copyright © Huawei Technologies Co., Ltd.

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.

12.11.11 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.

Copyright © Huawei Technologies Co., Ltd.

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 12-120 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

12.11.12 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.

 Copyright © Huawei Technologies Co., Ltd.

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     : Ethernet1/0/0 is up
  AC Status            : up
  VC State             : up
  VC ID                : 0
  VC Type              : Ethernet
  Destination          : 3.3.3.9
  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
```

 Copyright © Huawei Technologies Co., Ltd.

```
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, 1 hours, 44 minutes, 19 seconds
UP time              : 0 days, 1 hours, 44 minutes, 19 seconds
Last change time     : 0 days, 1 hours, 44 minutes, 19 seconds
VC last up time      : 2011/09/22 15:48:06
VC total up time     : 0 days, 1 hours, 44 minutes, 19 seconds
CKey                 : 10
NKey                 : 9
BFD for PW           : unavailable
```

Table 12-121 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.
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.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
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	Displays information about the VC tunnel or token ("1 tunnels/tokens" indicates that the PW uses one tunnel or token).
Backup TNL Type	Type of the backup tunnel when PW over LDP FRR is used.
NO.0 TNL Type	Type of the tunnel used by the PW
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.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
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.

Display information about static VCs on Ethernet1/0/0.

```
<Huawei> display mpls static-l2vc interface ethernet 1/0/0
 *Client Interface     : Ethernet1/0/0 is up
  AC Status            : up
  VC State             : up
  VC ID                : 0
  VC Type              : Ethernet
  Destination          : 3.3.3.9
  Transmit VC Label    : 100
  Receive VC Label     : 200
  Label Status         : 0
  Token Status         : 0
  Control Word         : Disable
  VCCV Capabilty       : alert ttl lsp-ping bfd
  active state         : active
  Link State           : up
  Tunnel Policy        : --
  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 : 0x3
  Backup TNL Type      : lsp   , TNL ID : 0x0
  Create time          : 0 days, 1 hours, 55 minutes, 52 seconds
  UP time              : 0 days, 1 hours, 55 minutes, 52 seconds
  Last change time     : 0 days, 1 hours, 55 minutes, 52 seconds
  VC last up time      : 2011/09/22 15:48:06
  VC total up time     : 0 days, 1 hours, 55 minutes, 52 seconds
  CKey                 : 10
  NKey                 : 9
  Diffserv Mode        : uniform
  Service Class        : --
  Color                : --
  DomainId             : --
  Domain Name          : --
  BFD for PW           : unavailable
```

Table 12-122 Description of the **display mpls static-l2vc interface** command output

Item	Description
Client Interface	AC interface and its status.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
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 Capabilty	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.
DomainId	ID of a domain.
Domain Name	Name of a domain.

Copyright © Huawei Technologies Co., Ltd.

Item	Description
BFD for PW	Whether BFD is configured. • unavailable: indicates that BFD is not configured. • available: indicates that BFD is configured.

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     : Ethernet1/0/0 is up
  AC Status            : up
  VC State             : up
  VC ID                : 0
  VC Type              : Ethernet
  Destination          : 3.3.3.9
  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, 1 hours, 56 minutes, 1 seconds
  UP time              : 0 days, 1 hours, 56 minutes, 1 seconds
  Last change time     : 0 days, 1 hours, 56 minutes, 1 seconds
  VC last up time      : 2011/09/22 15:48:06
  VC total up time     : 0 days, 1 hours, 56 minutes, 1 seconds
  CKey                 : 10
  NKey                 : 9
  BFD for PW           : unavailable
```

Table 12-123 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.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
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.

Display information about the static VC configured on TDM interface.

```
<Huawei> display mpls static-l2vc
 Total svc connections:  1,  0 up,  1 down

 *Client Interface     : Serial2/0/0 is up
  AC Status            : up
  VC State             : down
  VC ID                : 112
  VC Type              : CESoPSN basic mode
  Destination          : 1.1.1.9
  Transmit VC Label    : 115
  Receive VC Label     : 200
  Label Status         : 0
  Token Status         : 0
  Control Word         : Enable
  VCCV Capability      : cw alert ttl lsp-ping bfd
  active state         : inactive
  Link State           : down
  Tunnel Policy Name   : --
  PW Template Name     : --
  TDM encapsulation number : 8
  jitter-buffer        : 8
  idle-code            : ff
  rtp-header           : disable
  Main or Secondary    : Main
  load balance type    : flow
  Access-port          : false
```

 Copyright © Huawei Technologies Co., Ltd.

```
VC tunnel/token info : 0 tunnels/tokens
Backup TNL Type      : lsp   , TNL ID : 0x0
Create time          : 0 days, 0 hours, 0 minutes, 9 seconds
UP time              : 0 days, 0 hours, 0 minutes, 0 seconds
Last change time     : 0 days, 0 hours, 0 minutes, 9 seconds
VC last up time      : 0000/00/00 00:00:00
VC total up time     : 0 days, 0 hours, 0 minutes, 0 seconds
CKey                 : 4
NKey                 : 3
BFD for PW           : unavailable
```

Table 12-124 Description of the **display mpls static-l2vc** command output

Item	Description
TDM encapsulation number	Number of encapsulated TDM frames in Circuit Emulation Services over Packet Switch Network (CESoPSN) or Structure-Agnostic Time Division Multiplexing over Packet (SAToP) packets in the TDMoPSN application.
jitter-buffer	Depth of the jitter buffer, that is, the maximum allowed jitter delay.
idle-code	Idle code that is filled manually when a jitter buffer underflow occurs.
rtp-header	Whether the RTP header is added to the transparently transmitted TDM frame.

Related Topics

12.11.28 mpls static-l2vc

12.11.13 display mpls static-l2vc brief

12.11.13 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

 Copyright © Huawei Technologies Co., Ltd.

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:  1,  1 up,  0 down

*Client Interface     : Ethernet1/0/0 is up
 AC Status           : up
 VC State            : up
 VC ID               : 0
 VC Type             : Ethernet
 Destination         : 3.3.3.9
```

Table 12-125 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.
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.

Display brief information about the static VC configured on a TDM interface.

```
<Huawei> display mpls static-l2vc brief
 Total svc connections:  1,  0 up,  1 down
```

 Copyright © Huawei Technologies Co., Ltd.

```
*Client Interface     : Serial2/0/0 is up
 AC Status            : up
 VC State             : down
 VC ID                : 112
 VC Type              : CESoPSN basic mode
 Destination          : 1.1.1.9
 TDM encapsulation number : 8
 jitter-buffer        : 8
 idle-code            : ff
 rtp-header           : disable
```

Table 12-126 Description of the **display mpls static-l2vc** command output

Item	Description
TDM encapsulation number	Number of encapsulated TDM frames in Circuit Emulation Services over Packet Switch Network (CESoPSN) or Structure-Agnostic Time Division Multiplexing over Packet (SAToP) packets in the TDMoPSN application.
jitter-buffer	Depth of the jitter buffer, that is, the maximum allowed jitter delay.
idle-code	Idle code that is filled manually when a jitter buffer underflow occurs.
rtp-header	Indicates Whether the RTP header is added to the transparently transmitted TDM frames.

Related Topics

12.11.28 mpls static-l2vc

12.11.7 display mpls l2vpn forwarding-info

12.11.14 display snmp-agent trap feature-name l2vpn all

Function

The **display snmp-agent trap feature-name l2vpn all** command displays all trap messages about the L2VPN module.

Format

display snmp-agent trap feature-name l2vpn all

Parameters

None

Views

All views

 Copyright © Huawei Technologies Co., Ltd.

Default Level

1: Monitoring level

Usage Guidelines

The Simple Network Management Protocol (SNMP) is a standard network management protocol widely used on TCP/IP networks. It uses a central computer (a network management station) that runs network management software to manage network elements. The management agent on the network element automatically reports traps to the network management station. After that, the network administrator immediately takes measures to resolve the problem.

The **display snmp-agent trap feature-name l2vpn all** command displays whether all trap functions of the L2VPN module are enabled.

Example

Display all trap messages about the L2VPN module.

```
<Huawei> display snmp-agent trap feature-name l2vpn all
------------------------------------------------------------------------------
Feature name: L2VPN
Trap number : 14
------------------------------------------------------------------------------
Trap name                Default switch status   Current switch status
hwCCCVcDown                 off                     on
hwCCCVcUp                  off                    on
hwPWVcDeleted               off                     on
hwPWVcDown                  off                     on
hwPWVcUp                   off                    on
hwPWVcSwitchWtoP              off                     on
hwPWVcSwitchPtoW              off                     on
hwSvcDeleted               off                    on
hwSvcDown                  off                    on
hwSvcUp                   off                   on
hwPWVcBackup                off                     on
hwSvcSwitchWtoP             off                     on
hwSvcSwitchPtoW             off                     on
hwPWVcStatusChange            off                     on
```

Table 12-127 Description of the **display snmp-agent trap feature-name l2vpn all** command output

Item	Description
Feature name	Name of the module to which a trap message belongs.
Trap number	Number of trap messages.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Trap name	Name of a trap message about the L2VPN module: • hwCCCVcDown: indicates a Huawei private trap in case the status of the CCC VC changes to Down. • hwCCCVcUp: indicates a Huawei private trap in case the status of the CCC VC changes to Up. • hwPWVcDeleted: indicates a Huawei-specific trap in the event that a PWE3 VC is deleted. • hwPWVcDown: indicates a Huawei private trap in case the status of the PWE3 VC changes to Down. • hwPWVcUp: indicates a Huawei private trap in case the status of the PWE3 VC changes to Up. • hwPWVcSwitchWtoP: indicates a Huawei private trap in case the primary PWE3 PW is switched to the secondary PW. • hwPWVcSwitchPtoW: indicates a Huawei private trap in case the secondary PWE3 PW is switched to the primary PW. • hwSvcDeleted: indicates a Huawei-specific trap in the event that an SVC is deleted. • hwSvcDown: indicates a Huawei private trap in case the status of the SVC changes to Down. • hwSvcUp: indicates a Huawei private trap in case the status of the SVC changes to Up. • hwPWVcBackup: indicates a Huawei private trap in case the status of the PWE3 VC changes to Backup. • hwSvcSwitchWtoP: indicates that an SVC PW changes from the secondary state to the primary state. • hwSvcSwitchPtoW: indicates that an SVC PW changes from the primary state to the secondary state. • hwPWVcStatusChange: indicates that the status of the PWE3 VC change.
Default switch status	Default status of the trap function: • on: indicates that the trap default function is enabled. • off: indicates that the trap default function is disabled.
Current switch status	Current status of the trap function: • on: indicates that the trap function is enabled. • off: indicates that the trap function is disabled.

Copyright © Huawei Technologies Co., Ltd.

Related Topics

12.11.30 snmp-agent trap enable feature-name l2vpn

12.11.15 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 that ranges from 1 to 8192.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

If a device is configured with many VE-Groups, you can use the 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 Router.

```
<Huawei>display virtual-ethernet ve-group
 Ve-groupID    TerminateVE              AccessVE
 1             Virtual-Ethernet1/0/0(L2)  Virtual-Ethernet1/0/1(L3)
 5             Virtual-Ethernet2/0/0(L2)  Virtual-Ethernet2/0/1(L3)
Total 2, 2 printed
```

Table 12-128 Description of the **display virtual-ethernet ve-group** command output

Item	Description
Ve-groupID	Number of a VE-Group
TerminateVE	L2VE interface terminating the L2VPN

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
AccessVE	L3VE interface accessing an L3VPN

Related Topics

5.20.12 interface virtual-ethernet

12.11.32 ve-group

12.11.16 display vll ccc

Function

The **display vll ccc** command displays information about a CCC connection.

Format

display vll ccc [*ccc-name* | **type local**]

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.	-

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: local, state: up
```

 Copyright © Huawei Technologies Co., Ltd.

```
intf1: GigabitEthernet0/0/1 (up ethernet),access-port: false

intf2: GigabitEthernet0/0/2 (up ethernet),access-port: false
no control word
VC last up time : 2012/09/10 14:28:24
VC total up time: 0 days, 0 hours, 1 minutes, 41 seconds
```

Display information about all the CCC connections.

```
<Huawei> display vll ccc
total  ccc vc : 1
local  ccc vc : 1,  1 up
remote ccc vc : 0,  0 up

name: CE1-CE2, type: local, state: up,
intf1: GigabitEthernet0/0/1 (up), access-port: false

intf2: GigabitEthernet0/0/2 (up), access-port: false
VC last up time : 2012/09/10 14:28:24
VC total up time: 0 days, 0 hours, 0 minutes, 10 seconds
```

Table 12-129 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.
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.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
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 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: CE1-CE2, type: local, state: up,
intf1: GigabitEthernet0/0/2 (up),  access-port: false

intf2: GigabitEthernet0/0/1 (up),  access-port: false
VC last up time : 2011/09/21 22:17:44
VC total up time: 0 days, 0 hours, 8 minutes, 43 seconds
```

Related Topics

12.11.2 ccc interface out-interface

12.11.3 display l2vpn ccc-interface vc-type

12.11.17 l3ve track oam-state

Function

The **l3ve track oam-state** command enables the association between the L3VE interface status and the OAM status.

The **undo l3ve track oam-state** command disables the association between the L3VE interface status and the OAM status.

By default, the association between the L3VE interface status and the OAM status is disabled.

Format

l3ve track oam-state

undo l3ve track oam-state

Parameters

None

 Copyright © Huawei Technologies Co., Ltd.

Views

VE sub-interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In L2VPN accessing L3VPN scenarios in which PW protection is configured, if OAM (BFD, MPLS OAM, or MPLS-TP OAM) detects that services are interrupted between routers, OAM does not trigger the L3VE interface to withdraw reverse routes. Therefore, reverse traffic is still forwarded along the faulty PW until route convergence is complete, which causes traffic loss. To resolve this problem, run the **l3ve track oam-state** command to enable the association between the L3VE interface status and the OAM status. The L3VE interface then can identify the OAM status and have its status consistent with the OAM status. This prevents traffic loss.

Precautions

The **l3ve track oam-state** command applies only to the 1:1 mode and not to the N:1 mode.

- In 1:1 mode, one L2VE sub-interface is bound to one L3VE interface.
- In N:1 mode, N L2VE sub-interfaces are bound to one L3VE interface.

Example

Enable the association between the L3VE interface status and the OAM status.

```
<Huawei> system-view
[Huawei] interface virtual-ethernet 3/0/1.1
[Huawei-Virtual-Ethernet3/0/1.1] l3ve track oam-state
```

Related Topics

12.12.29 pw-template

12.11.18 l3ve track pw-state

12.11.18 l3ve track pw-state

Function

The **l3ve track pw-state** command associates the L3VE interface status with the PW status.

The **undo l3ve track pw-state** command disassociates the L3VE interface status from the PW status.

By default, the L3VE interface status is not associated with the PW status.

 Copyright © Huawei Technologies Co., Ltd.

Format

l3ve track pw-state

undo l3ve track pw-state

Parameters

None

Views

VE sub-interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In the L2VPN access L3VPN solution, if the primary and secondary PWs have been established and corresponding L3VE interfaces have gone Up when the primary router recovers, the downstream traffic may switch back to the primary router. However, if the downstream traffic switches back to the primary router before the primary/secondary PW switchover is complete, the downstream traffic may be temporarily dropped. To solve this problem, run the **l3ve track pw-state** command to associate the L3VE interface status with the PW status.

The **l3ve track pw-state** command associates the L3VE interface status with the PW status. Then, the L3VE interface can keep its status consistent with the PW status by detecting the active/standby status of the PW so that the traffic on the RNC can be properly switched between the master and backup routers.

Precautions

This command can be configured only on the VE sub-interface.

Example

Associate the L3VE interface status with the PW status.

```
<Huawei> system-view
[Huawei] interface Virtual-Ethernet 3/0/1.1
[Huawei-Virtual-Ethernet3/0/1.1] l3ve track pw-state
```

Related Topics

12.12.29 pw-template

 Copyright © Huawei Technologies Co., Ltd.

12.11.19 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
```

 Copyright © Huawei Technologies Co., Ltd.

12.11.20 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* [[**tunnel-policy** *policy-name*] | [{ **control-word** | **no-control-word** }] | [{ **raw** | **tagged** }] | [**secondary**]] *

undo mpls l2vc { *ip-address* | **pw-template** *pw-template-name* } * *vc-id* [[**tunnel-policy** *policy-name*] | [{ **control-word** | **no-control-word** }] | [{ **raw** | **tagged** }] | [**secondary**]] *

undo mpls l2vc [**secondary**]

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.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
tunnel-policy *policy-name*	Specifies a tunnel policy name for the L2VC. If no name is specified for a tunnel policy, 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. If the name of the tunnel policy is specified but no tunnel policy is configured, the default tunnel policy is still used.	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 service-delimiting (SD) tag from a packet. This parameter is required when the AC is an Ethernet link.	-
tagged	Retains the SD tag in a packet. This parameter is required when the AC is an Ethernet link.	-
control-word	Enables the control word function.	-
no-control-word	Disables the control word function.	-
secondary	Indicates that the VC is 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.	-

Views

Interface view

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

Usage Scenario

In a Martini VLL networking, you can run this command to create a VC connection for a Martini VLL.

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 parameters **raw** and **tagged** can be used only for Ethernet links.
- The MTU value is specified when you create Martini or PWE3 VLLs and is used for interconnection between the router 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**, **no-control-word**, **idle-code** *idle-code-value*, **jitter-buffer**, **tdm-encapsulation** *number*, and **tdm-sequence-number**.

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.
- To configure TDM PWE3, run the **link-protocol tdm** command to set the link layer protocol to TDM before you run this command to configure a PW.

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
```

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

12.11.4 display mpls l2vc
12.11.7 display mpls l2vpn forwarding-info

12.11.21 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.

 Copyright © Huawei Technologies Co., Ltd.

- If MPLS L2VPN is enabled on the device, the MPLS L2VPN view is displayed.

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]
```

12.11.22 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.

 Copyright © Huawei Technologies Co., Ltd.

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
```

Related Topics

12.11.21 mpls l2vpn

12.11.23 mpls l2vpn frag

Function

The **mpls l2vpn frag** command enables fragmentation of L2VPN IPv4 packets.

The **undo mpls l2vpn frag** command disables fragmentation of L2VPN IPv4 packets.

By default, fragmentation of L2VPN IPv4 packets is disabled.

Format

mpls l2vpn frag

undo mpls l2vpn frag

Parameters

None

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When an AR router communicates with another device, packet transmission between them may fail if the AR does not fragment packets, in which case the packet length may exceed the MTU value of the other device. To ensure normal packet transmission, configure the **mpls l2vpn frag** command to fragment packets.

Prerequisites

 Copyright © Huawei Technologies Co., Ltd.

MPLS L2VPN has been enabled on the interface.

Precautions

After the **mpls l2vpn frag** command is executed, the AR fragments IPv4 packets based on the MTU value on the tunnel's public network interface.

Example

Enable the packet fragmentation function.

```
<Huawei> system-view
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] mpls l2vpn frag
```

12.11.24 mpls l2vpn oam-mapping

Function

The **mpls l2vpn oam-mapping** command enables the mapping between the AC status and the Packet Switching Network (PSN) status.

The **undo mpls l2vpn oam-mapping** command disables the mapping between the AC status and the PSN status.

By default, the mapping between the AC status and the PSN status is disabled.

Format

mpls l2vpn oam-mapping 3ah

undo mpls l2vpn oam-mapping

Parameters

Parameter	Description	Value
3ah	Enables fault detection and fault notification defined in IEEE 802.3ah.	-

Views

Ethernet interface view, GE interface view, XGE interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In VLL FRR or PWE3 FRR scenarios, PEs and CEs do not advertise their primary/secondary status and link status to each other. PW OAM and AC OAM need to be configured to monitor PW and AC status respectively. OAM mapping is enabled on the PEs to associate PW OAM with AC OAM.

 Copyright © Huawei Technologies Co., Ltd.

After the **mpls l2vpn oam-mapping** command is configured on a PE, the system generates the mapping table between the AC status and the PSN status. If a fault occurs on an AC, the local PE will notify the remote PE of the AC fault. If a fault occurs on a PW, the local PE will notify the local CE of the fault. Timely fault notification allows PEs and CEs to coordinate with each other to implement end-to-end FRR.

Prerequisites

OAM fault detection and notification have been configured for the corresponding AC.

Configuration Impact

After the mapping between the AC status and the PSN status is enabled, if a fault occurs on the local AC:

- If BFD for PW is enabled, the local AC notifies the remote PE of the AC fault using BFD and the signaling protocol.
- If BFD for PW is disabled, the local AC notifies the remote PE of the AC fault using the signaling protocol.

Follow-up Procedure

After configuring this command, run the **display mpls l2vc interface** command to check the AC link status. The AC link status is displayed in the **Local AC OAM State** field of the command output.

Example

Enable fault detection and notification defined in IEEE 802.3ah on an Ethernet interface.

```
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] mpls l2vc 1.1.1.1 101
[Huawei-GgiabitEthernet1/0/0] mpls l2vpn oam-mapping 3ah
```

Related Topics

12.11.6 display mpls l2vc oam-mapping

12.11.25 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** }

 Copyright © Huawei Technologies Co., Ltd.

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

 Copyright © Huawei Technologies Co., Ltd.

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 gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] mpls l2vc 1.1.1.9 100
[Huawei-GigabitEthernet1/0/0] mpls l2vc 2.2.2.9 200 secondary
[Huawei-GigabitEthernet1/0/0] mpls l2vpn reroute delay 15 resume 20
```

Related Topics

12.11.20 mpls l2vc

12.11.26 mpls l2vpn service-name

Function

The **mpls l2vpn service-name** command sets the name of an SVC or Martini VLL 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.

 Copyright © Huawei Technologies Co., Ltd.

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 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 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.

 Copyright © Huawei Technologies Co., Ltd.

- On each PE, an L2VPN service name is unique.
- The **mpls l2vpn service-name** command cannot be run on a loopback interface.

Example

Set an L2VPN service name to **pw1** on a service interface.

```
<Huawei> system-view
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] mpls l2vc 10.1.1.1 1
[Huawei-GigabitEthernet1/0/0] mpls l2vpn service-name pw1
```

Related Topics

12.11.2 ccc interface out-interface

12.11.27 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.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
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. 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-**

 Copyright © Huawei Technologies Co., Ltd.

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
```

12.11.28 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**] | **idle-code** *idle-code-value* | **jitter-buffer** *depth* | **tdm-encapsulation** *number* | **tdm-sequence-number** | **secondary**] *

undo mpls static-l2vc [**secondary**]

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**] | **idle-code** *idle-code-value* | **jitter-buffer** *depth* | **tdm-encapsulation** *number* | **tdm-sequence-number** | **secondary**] *

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.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
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 service-delimiting (SD) tag from a packet. This parameter is required when the AC is an Ethernet link.	-
tagged	Retains the SD tag in a packet. This parameter is required when the AC is an Ethernet link.	-
idle-code *idle-code-value*	Specifies the idle code that is filled in manually when a jitter buffer underflow occurs. This parameter is required when the AC is a TDM link.	The value ranges from 00 to FF, in hexadecimal notation. The default value is FF.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
jitter-buffer *depth*	Specifies the depth of the jitter buffer, that is, the allowed maximum jitter delay. This parameter is required when the AC is a TDM link.	The value is an integer that ranges from 4 to 64, in milliseconds. The default value is 8 ms.
tdm-encapsulation *number*	Specifies the number of TDM frames encapsulated in a CESoPSN packet. This parameter is required when the AC is a TDM link.	The value is an integer, which can be 8, 16, 24, 32, or 40. The default value is 8. When the interface card where the AC interface locates is 8SA, 8E1T1-M or 8E1T1-F, the interface can encapsulate a maximum of 16 TDM frames in a packet. If the value is larger than 16, the interface only encapsulates 16 TDM frames in a packet.
tdm-sequence-number	Sets the sequence number of the first frame encapsulated for TDM transparent transmission to 1. This parameter is required when the AC is a TDM link.	-
secondary	Configures the PW as a static secondary PW. By default, a created PW is a primary PW.	-

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-12vc** 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**, **no-control-word**, **idle-code** *idle-code-value*, **jitter-buffer**, **tdm-encapsulation** *number*, and **tdm-sequence-number**.

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.
- To configure TDM PWE3, run the **link-protocol tdm** command to set the link layer protocol to TDM before you run this command to configure a PW.

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
```

Delete a static VC.

```
<Huawei> system-view
[Huawei] interface vlanif 10
[Huawei-Vlanif10] undo mpls static-l2vc
```

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

12.11.12 display mpls static-l2vc
12.11.21 mpls l2vpn

12.11.29 ping vc

Function

The **ping vc** command detects the status of a PW.

Format

ping vc *pw-type pw-id* [**-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*] [**uniform**]

ping vc *pw-type pw-id* [**-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*] [**uniform**]

ping vc *pw-type pw-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**] [**remote** *remote-ip-address* | **draft6**] * [**uniform**]

ping vc *pw-type pw-id* [**-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*] [**uniform**]

Parameters

Parameter	Description	Value
pw-type	Specifies the encapsulation type of a local PW.	Currently, PWs of the following types are supported: **ethernet**, **vlan**.
pw-id	Specifies the ID of a local PW.	The value is an integer that ranges from 1 to 4294967295.
-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.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
-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 larger 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. The value must be smaller than the MTU value of the interface.
-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.	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.	-

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
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.	-
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 version of the **ping vc** command. If this parameter is specified, the ping operation is performed based on "draft-ietf-mpls-lsp-ping-06".	-
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.	-

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
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.

 Copyright © Huawei Technologies Co., Ltd.

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 an 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
```

Related Topics

12.11.31 tracert vc

12.11.30 snmp-agent trap enable feature-name l2vpn

Function

The **snmp-agent trap enable feature-name l2vpn** command enables the trap function for the L2VPN module.

 Copyright © Huawei Technologies Co., Ltd.

The **undo snmp-agent trap enable feature-name l2vpn** command disables the trap function for the L2VPN module.

By default, the trap function is disabled for the L2VPN module.

Format

snmp-agent trap enable feature-name l2vpn [**trap-name** { **hwcccvcdown** | **hwcccvcup** | **hwpwvcbackup** | **hwpwvcdeleted** | **hwpwvcdown** | **hwpwvcstatuschange** | **hwpwvcswitchptow** | **hwpwvcswitchwtop** | **hwpwvcup** | **hwsvcdeleted** | **hwsvcdown** | **hwsvcswitchptow** | **hwsvcswitchwtop** | **hwsvcup** | **hwVpwsPwRedundancyDegraded** | **hwVpwsPwRedundancyDegradedClear** }]

undo snmp-agent trap enable feature-name l2vpn [**trap-name** { **hwcccvcdown** | **hwcccvcup** | **hwpwvcbackup** | **hwpwvcdeleted** | **hwpwvcdown** | **hwpwvcstatuschange** | **hwpwvcswitchptow** | **hwpwvcswitchwtop** | **hwpwvcup** | **hwsvcdeleted** | **hwsvcdown** | **hwsvcswitchptow** | **hwsvcswitchwtop** | **hwsvcup** | **hwVpwsPwRedundancyDegraded** | **hwVpwsPwRedundancyDegradedClear** }]

Parameters

Parameter	Description	Value
trap-name	Indicates the traps of L2VPN events of specified types.	-
hwcccvcdown	Enables or disables the trap indicating that the status of a CCC VC changes to Down.	-
hwcccvcup	Enables or disables the trap indicating that the status of a CCC VC changes to Up.	-
hwpwvcbackup	Enables or disables the trap indicating that the status of a PWE3 VC changes to Backup.	-
hwpwvcdeleted	Enables or disables the trap indicating that a PWE3 VC is deleted.	-
hwpwvcdown	Enables or disables the trap indicating that the status of a PWE3 VC changes to Down.	-
hwpwvcstatuschange	Enables or disables the trap indicating that the status of a PWE3 VC changes.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
hwpwvcswitchptow	Enables or disables the trap indicating that a PWE3 PW changes from the secondary state to the primary state.	-
hwpwvcswitchwtop	Enables or disables the trap indicating that a PWE3 PW changes from the primary state to the secondary state.	-
hwpwvcup	Enables or disables the trap indicating that the status of a PWE3 VC changes to Up.	-
hwsvcdeleted	Enables or disables the trap indicating that an SVC is deleted.	-
hwsvcdown	Enables or disables the trap indicating that the status of an SVC changes to Down.	-
hwsvcswitchptow	Enables or disables the trap indicating that an SVC PW changes from the secondary state to the primary state.	-
hwsvcswitchwtop	Enables or disables the trap indicating that an SVC PW changes from the primary state to the secondary state.	-
hwsvcup	Enables or disables the trap indicating that the status of an SVC changes to Up.	-
hwVpwsPwRedundancyDegraded	Indicates a Huawei-specific trap reported when the primary or secondary PW for PW APS degrades.	-
hwVpwsPwRedundancyDegradedClear	Indicates a Huawei-specific trap reported when the primary or secondary PW for PW APS recovers.	-

 Copyright © Huawei Technologies Co., Ltd.

Views

System view

Default Level

3: Management level

Usage Guidelines

The L2VPN module is not configured with the function of excessive traps. To enable the traps of one or more events, specify **trap-name**.

Example

Enable the system to generate an alarm when a VC in CCC mode goes Down.

```
<Huawei> system-view
[Huawei] snmp-agent trap enable feature-name l2vpn trap-name hwcccvcdown
```

Related Topics

12.11.14 display snmp-agent trap feature-name l2vpn all

12.11.31 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* [**-exp** *exp-value* | **-f** *first-ttl* | **-m** *max-ttl* | **-r** *reply-mode* | **-t** *timeout-value*] * **control-word** [**draft6**] [**full-lsp-path**] [**uniform**]

tracert vc *pw-type pw-id* [**-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**] [**uniform**]

tracert vc *pw-type pw-id* [**-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**] [**uniform**]

tracert vc *pw-type pw-id* [**-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**] [**uniform**]

tracert vc *pw-type pw-id* [**-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**] [**uniform**]

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
pw-type	Specifies the PW type.	Currently, PWs of the following types are supported: **ethernet**, **vlan**.
pw-id	Specifies the local PW ID.	The value is an integer that ranges from 1 to 4294967295.
-exp *exp-value*	Specifies the EXP value in the outer label of an MPLS Echo Request packet. The default value is 0.	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.
-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.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
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.	-
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.	-
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.	-
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.	-

Copyright © Huawei Technologies Co., Ltd.

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". **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.

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.

 Copyright © Huawei Technologies Co., Ltd.

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 12-130 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.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
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.

Related Topics

12.11.29 ping vc

12.11.32 ve-group

Function

The **ve-group** command sets 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 sets a VE interface to common mode.

By default, VE interfaces work 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 number of a VE-Group.	The value is an integer that ranges from 1 to 8192.
l2-terminate	Sets the VE interface as an L2VE that terminates the VLL.	-
l3-access	Sets the VE interface as an L3VE interface that accesses the MPLS L3VPN.	-

Views

VE interface view

Copyright © Huawei Technologies Co., Ltd.

Default Level

2: Configuration level

Usage Guidelines

Before using the **ve-group** command, if a VE interface is bound to a Permanent Virtual Circuit (PVC) that carries IPoEoA, you must disconnect the binding.

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 on the VE interface.
- To change a VE interface to an L3VE interface, run the **ve-group** *ve-group-id* **l3-access** command on the VE interface.

In L2VPN access to L3VPN scenarios, a VE group has only one L2VE interface and one L3VE interface. L2VE interfaces can only work in Dot1q termination mode, L3VE interfaces can work in QinQ termination and Dot1q termination mode. L2VE and L3VE interfaces can have multiple sub-interfaces created for different VLAN services.

Example

Set VE 1/0/0 as an L2VE.

```
<Huawei> system-view
[Huawei] interface virtual-ethernet 1/0/0
[Huawei-Virtual-Ethernet1/0/0] ve-group 1 l2-terminate
```

Set the VE 1/0/1 as an L3VE.

```
<Huawei> system-view
[Huawei] interface virtual-ethernet 1/0/1
[Huawei-Virtual-Ethernet1/0/1] ve-group 1 l3-access
```

Related Topics

5.20.12 interface virtual-ethernet

12.12 PWE3 Configuration Commands

NOTE

The AR100&AR120&AR150&AR160&AR200 series do not support PWE3.

12.12.1 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**]

 Copyright © Huawei Technologies Co., Ltd.

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.

Copyright © Huawei Technologies Co., Ltd.

- 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
```

12.12.2 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

When load balancing is used, packets may be out of sequence when reaching the destination. The control word function can be used to put the packets into the correct order.

Example

Enable the control word in the PW template named **pwt**.

 Copyright © Huawei Technologies Co., Ltd.

```
<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
```

Related Topics

12.12.29 pw-template

12.12.3 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.	-

 Copyright © Huawei Technologies Co., Ltd.

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 router.

```
<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
```

 Copyright © Huawei Technologies Co., Ltd.

```
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 12-131 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**. Currently, mPW is not supported on the device.
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 to ignore the impact of AC status changes on the active/standby PWE3 service status is enabled: ● enable ● disable
VC state	Status of the VC: ● up: A VC has been established. ● down: A VC is not established.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
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.
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.

Copyright © Huawei Technologies Co., Ltd.

Item	Description
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.
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.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
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.

```
<Huawei> display mpls l2vc interface ethernet 1/0/0
 *client interface       : Ethernet1/0/0 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                : Ethernet
  destination            : 10.3.3.9
  local group ID         : 0            remote group ID      : 0
  local VC label         : 1024         remote VC label      : 1024
  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
  forwarding entry       : exist
  link state             : up
```


Copyright © Huawei Technologies Co., Ltd.

```
local VC MTU           : 1500         remote VC MTU        : 1500
local VCCV             : alert ttl lsp-ping bfd
remote VCCV            : alert ttl lsp-ping bfd
local control word     : disable      remote control word  : disable
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 : 0x5
  Backup TNL type      : lsp    , TNL ID : 0x0
create time            : 0 days, 0 hours, 29 minutes, 47 seconds
up time                : 0 days, 0 hours, 4 minutes, 54 seconds
last change time       : 0 days, 0 hours, 4 minutes, 54 seconds
VC last up time        : 2011/09/26 15:29:03
VC total up time       : 0 days, 0 hours, 4 minutes, 54 seconds
CKey                   : 5
NKey                   : 4
PW redundancy mode     : frr
AdminPw interface      : --
AdminPw link state     : --
Diffserv Mode          : uniform
Service Class          : --
Color                  : --
DomainId               : --
Domain Name            : --
```

Table 12-132 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.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
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.
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.

Copyright © Huawei Technologies Co., Ltd.

Item	Description
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.
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
```

 Copyright © Huawei Technologies Co., Ltd.

```
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              : 101
VC Type            : ethernet
VC Label           : 1024
Peer Address       : 10.3.3.9
Group ID           : 0
MTU                : 1500
Control Word       : 0
Notification       : 0
Status Code        : 0
Match Local VC     : MATCH
Max ATM CELLS      : --
TDM RTP Header     : --
TDM Encap Num      : --
TDM Bit Rate       : --
```

Table 12-133 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
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.

Copyright © Huawei Technologies Co., Ltd.

Item	Description
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       : Ethernet1/0/0 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                : Ethernet
  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
```

 Copyright © Huawei Technologies Co., Ltd.

```
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            : --
```

Display information about the dynamic VC on the TDM interface.

```
<Huawei> display mpls l2vc interface serial 2/0/0
 *client interface       : Serial2/0/0 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                : CESoPSN basic mode
  destination            : 10.3.3.9
  local group ID         : 0           remote group ID      : 0
  local VC label         : 1039        remote VC label      : 1045
  local TDM Encap Num    : 8           remote TDM Encap Num : 0
  jitter-buffer          : 8
  idle-code              : ff
  local rtp-header       : disable     remote rtp-header    : disable
  local bit-rate         : 0           remote bit-rate      : 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
```

 Copyright © Huawei Technologies Co., Ltd.

```
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           : --          remote VC MTU       : --
local VCCV             : alert ttl lsp-ping bfd
remote VCCV            : alert ttl lsp-ping bfd
local control word     : disable     remote control word  : disable
tunnel policy name     : --
PW template name       : pe2pe
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 : 0x5
  Backup TNL type      : lsp   , TNL ID : 0x0
create time            : 0 days, 0 hours, 1 minutes, 36 seconds
up time                : 0 days, 0 hours, 1 minutes, 36 seconds
last change time       : 0 days, 0 hours, 1 minutes, 36 seconds
VC last up time        : 2013/11/02 09:30:04
VC total up time       : 0 days, 0 hours, 1 minutes, 36 seconds
CKey                   : 9
NKey                   : 8
PW redundancy mode     : frr
AdminPw interface      : --
AdminPw link state     : --
Diffserv Mode          : pipe
Service Class          : ef
Color                  : green
DomainId               : --
Domain Name            : --
```

Table 12-134 Description of the **display mpls l2vc interface** command output

Item	Description
local TDM Encap Num	Number of encapsulated TDM frames in Circuit Emulation Services over Packet Switch Network (CESoPSN) or Structure-Agnostic Time Division Multiplexing over Packet (SAToP) packets in the TDMoPSN application of the local VC.
remote TDM Encap Num	Number of encapsulated TDM frames in CESoPSN or SAToP packets in the TDMoPSN application of the remote VC. **NOTE** This field is displayed as 0 when the AC interface is a serial interface.
jitter-buffer	Depth of the jitter buffer, that is, the maximum allowed jitter delay.
idle-code	Idle code that is filled manually when a jitter buffer underflow occurs.
local rtp-header	Whether the RTP header is added to the transparently transmitted TDM frames on the local end.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
remote rtp-header	Whether the RTP header is added to the transparently transmitted TDM frames on the remote end.
local bit-rate	Bit rate of the local VC.
remote bit-rate	Bit rate of the remote VC.

Related Topics

12.12.15 mpls l2vc
12.11.7 display mpls l2vpn forwarding-info

12.12.4 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
```

 Copyright © Huawei Technologies Co., Ltd.

```
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 12-135 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
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.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
link state	Status of the VC: • up • down

Related Topics

12.12.15 mpls l2vc

12.11.7 display mpls l2vpn forwarding-info

12.12.5 display mpls l2vc oam-mapping

Function

The **display mpls l2vc oam-mapping** command displays status of an L2VPN AC established by using the LDP signaling and information about the OAM mapping table at the PSN side.

Format

display mpls l2vc oam-mapping [**interface** *interface-type interface-number*]

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Specifies the interface type and number. If this parameter specified, OAM mapping information on the specified VC interface using the LDP signaling is displayed. • *interface-type* specifies the interface type. • *interface-number* specifies the interface number.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After you run the **display mpls l2vc oam-mapping** command, either the following situation will occur:

- If an interface name is specified, detailed OAM mapping information on this interface is displayed.

Copyright © Huawei Technologies Co., Ltd.

- If no interface name is specified, basic about the OAM mapping information on all interfaces is displayed.

Example

Display OAM mapping information on the VC interface using the LDP signaling.

```
<Huawei> display mpls l2vc oam-mapping
 Interface                 Active VC-ID      VC-status AC-OAM  BFD-for-PW
GigabitEthernet0/0/1          No     100       Primary   Enable  Disable
GigabitEthernet0/0/1          No     101       Secondary Enable  Disable
```

Table 12-136 Description of the **display mpls l2vc oam-mapping** command output

Item	Description
Interface	Type and number of the AC interface.
Active	Whether the PW is in the active state: ● Yes: indicates that the PW is in active state. ● No: indicates that the PW is in inactive state. This field is valid only when primary and secondary PWs coexist.
VC-ID	ID of the local VC.
VC-status	Status of the local PW: ● Primary: indicates the primary PW. ● Secondary: indicates the secondary PW.
AC-OAM	Whether the local PE reports an AC fault to the remote PE through OAM: ● Enable: indicates that the local PE reports an AC fault to the remote PE through OAM. ● Disable: indicates that the local PE does not report an AC fault to the remote PE through OAM.
BFD-for-PW	Whether BFD for PW is enabled on the local PE: ● Enable ● Disable

Display OAM mapping information on GE1/0/0.

```
<Huawei> display mpls l2vc oam-mapping interface gigabitethernet 1/0/0
 AC OAM Info:
```

 Copyright © Huawei Technologies Co., Ltd.

```
 EOAM Type      : 802.3ah
 AC OAM State   : Up
 OAM-mapping    : Enable
PSN info:
 VC-ID          : 100
 VC status      : Primary
 Active State   : Inactive
 Link State     : Down
 BFD for PW     : Disable
 BFD for LSP    : 0    TunnelNum: 0    PSN State : up
 VC-ID          : 101
 VC status      : Secondary
 Active State   : Inactive
 Link State     : Down
 BFD for PW     : Disable
 BFD for LSP    : 0    TunnelNum: 0    PSN State : up
```

Table 12-137 Description of the **display mpls l2vc oam-mapping interface** command output

Item	Description
AC OAM Info	Information about AC OAM to be displayed in the following lines.
ACFD Index	Index of the AC forwarding information.
EOAM Type	Type of the protocol used for fault detection and notification.
AC OAM State	Fault detection status on the local AC: • Up: indicates that AC fault detection is disabled or that AC fault detection is enabled but no AC fault is detected. • Down: indicates that AC fault detection is enabled and an AC fault is detected. • Invalid: indicates that AC fault detection is disabled, and the AC OAM state field is invalid.
OAM-mapping	Whether OAM mapping is enabled on the local PE: • Enable • Disable
PSN info	Information about the PW.
VC-ID	ID of the VC.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
VC status	Status of the PW: • Primary: indicates the primary PW. • Secondary: indicates the secondary PW. • Bypass: indicates the inter-chassis PW. • PW-Bypass: indicates the inter-chassis PW used to protect PW-side links. • AC-Bypass: indicates the inter-chassis PW used to protect AC-side links.
Active state	Whether the PW is in the active state: • Active: indicates that the PW is in active state. • Inactive: indicates that the PW is in inactive state. This field is valid only when primary and secondary PWs coexist. When an AC interface is configured with only one PW, the PW is in active state. If an AC interface is configured with primary and secondary PWs, the primary PW is in active state and the secondary PW is in inactive state. When the primary PW fails, the secondary PW becomes active and the primary PW becomes inactive.
Link State	Link status of the AC interface. • Up: indicates that the interface is Up. • Down: indicates that the interface is Down.
BFD for PW	Whether BFD for PW is enabled on the local PE.
BFD for LSP	Whether BFD is used to detect a tunnel: • zero: indicates that BFD is not used to detect a tunnel. • non-zero: indicates that BFD is used to detect a tunnel.
TunnelNum	Number of tunnels detected by BFD.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
PSN State	• When the tunnel is not detected by BFD, the default status of the tunnel is Up. • When the PW uses the tunnel not detected by BFD, the PSN state is Up.

Related Topics

12.12.18 mpls l2vpn oam-mapping

12.12.6 display mpls l2vpn interface performance

Function

The **display mpls l2vpn interface performance** command displays PW performance information on a TDM interface.

Format

display mpls l2vpn interface *interface-type interface-number* **performance**

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Specifies the type and number of the AC interface. • *interface-type* specifies the interface type. • *interface-number* specifies the interface number.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

After configuring a TDM-encapsulated PW at the AC side, you can run the **display mpls l2vpn interface performance** command to view PW performance information.

Prerequisites

Copyright © Huawei Technologies Co., Ltd.

A static or dynamic PW has been configured on the ATM or TDM interface.

Precautions

- The **interface** *interface-type interface-number* parameter specifies the AC interface on which PW performance information is displayed.
- This command can be used only to display performance information of a primary PW.
- PW performance information is updated every 15 minutes. Therefore, only PW performance information updated for the latest 15 minutes is displayed when you run this command.

Example

Display PW performance information on a TDM interface.

```
<Huawei> display mpls l2vpn interface serial 2/0/0  performance
Client interface                          : Serial2/0/0
Number of missing packets                 : 0
Number of times the jitter buffer was overrun  : 0
Number of times the jitter buffer was underrun : 0
Number of misorder packets                : 0
Number of malformed packets               : 0
Number of misconnected packets            : 0
Number of error seconds                   : 0
Number of severely error seconds          : 0
Number of unavailable seconds             : 0
```

Table 12-138 Description of the **display mpls l2vpn interface performance** command output

Item	Description
Client interface	AC interface and its status.
Number of missing packets	Number of lost packets.
Number of times the jitter buffer was overrun	Number of times that a jitter buffer overflow occurs.
Number of times the jitter buffer was underrun	Number of times that a jitter buffer underflow occurs.
Number of misorder packets	Number of lost packets caused by packet disorder.
Number of malformed packets	Number of malformed packets.
Number of misconnected packets	Number of misconnected packets during the detection period.
Number of error seconds	Number of errored seconds, indicating the period during which a TDM-encapsulated PW discards packets or receives error packets. Any malformed packet or disorder packet is considered as an error packet.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Number of severely error seconds	Number of severely errored seconds.
Number of unavailable seconds	Number of unavailable seconds. When the SES is larger than 10 seconds, a TDM encapsulated PW is considered as unavailable. The number of unavailable seconds is counted when a severe error begins.

Related Topics

12.12.19 mpls l2vpn pw performance disable

12.12.7 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.	-

Copyright © Huawei Technologies Co., Ltd.

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     : Ethernet1/0/0 is up
  AC Status            : up
  VC State             : up
  VC ID                : 0
  VC Type              : Ethernet
  Destination          : 3.3.3.9
  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 : 0x800802
  Backup TNL type      : lsp   , TNL ID : 0x0
  Create time          : 0 days, 1 hours, 44 minutes, 19 seconds
  UP time              : 0 days, 1 hours, 44 minutes, 19 seconds
  Last change time     : 0 days, 1 hours, 44 minutes, 19 seconds
  VC last up time      : 2011/09/22 15:48:06
  VC total up time     : 0 days, 1 hours, 44 minutes, 19 seconds
  CKey                 : 10
  NKey                 : 9
  BFD for PW           : unavailable
```

Table 12-139 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.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
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.
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

Copyright © Huawei Technologies Co., Ltd.

Item	Description
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	Displays information about the VC tunnel or token ("1 tunnels/tokens" indicates that the PW uses one tunnel or token).
Backup TNL Type	Type of the backup tunnel when PW over LDP FRR is used.
NO.0 TNL Type	Type of the tunnel used by the PW
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.

Copyright © Huawei Technologies Co., Ltd.

Display information about static VCs on Ethernet1/0/0.

```
<Huawei> display mpls static-l2vc interface ethernet 1/0/0
 *Client Interface     : Ethernet1/0/0 is up
  AC Status           : up
  VC State            : up
  VC ID               : 0
  VC Type             : Ethernet
  Destination         : 3.3.3.9
  Transmit VC Label   : 100
  Receive VC Label    : 200
  Label Status        : 0
  Token Status        : 0
  Control Word        : Disable
  VCCV Capabilty      : alert ttl lsp-ping bfd
  active state        : active
  Link State          : up
  Tunnel Policy       : --
  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 : 0x3
  Backup TNL Type     : lsp   , TNL ID : 0x0
  Create time         : 0 days, 1 hours, 55 minutes, 52 seconds
  UP time             : 0 days, 1 hours, 55 minutes, 52 seconds
  Last change time    : 0 days, 1 hours, 55 minutes, 52 seconds
  VC last up time     : 2011/09/22 15:48:06
  VC total up time    : 0 days, 1 hours, 55 minutes, 52 seconds
  CKey                : 10
  NKey                : 9
  Diffserv Mode       : uniform
  Service Class       : --
  Color               : --
  DomainId            : --
  Domain Name         : --
  BFD for PW          : unavailable
```

Table 12-140 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 Capabilty	Whether VCCV is enabled.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
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.
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.

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     : Ethernet1/0/0 is up
  AC Status            : up
  VC State             : up
  VC ID                : 0
  VC Type              : Ethernet
  Destination          : 3.3.3.9
  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
```

 Copyright © Huawei Technologies Co., Ltd.

```
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, 1 hours, 56 minutes, 1 seconds
UP time             : 0 days, 1 hours, 56 minutes, 1 seconds
Last change time    : 0 days, 1 hours, 56 minutes, 1 seconds
VC last up time     : 2011/09/22 15:48:06
VC total up time    : 0 days, 1 hours, 56 minutes, 1 seconds
CKey                : 10
NKey                : 9
BFD for PW          : unavailable
```

Table 12-141 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.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
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.

Display information about the static VC configured on TDM interface.

```
<Huawei> display mpls static-l2vc
 Total svc connections:  1,  0 up,  1 down

 *Client Interface     : Serial2/0/0 is up
  AC Status            : up
  VC State             : down
  VC ID                : 112
  VC Type              : CESoPSN basic mode
  Destination          : 1.1.1.9
  Transmit VC Label    : 115
  Receive VC Label     : 200
  Label Status         : 0
  Token Status         : 0
  Control Word         : Enable
  VCCV Capability      : cw alert ttl lsp-ping bfd
  active state         : inactive
  Link State           : down
  Tunnel Policy Name   : --
  PW Template Name     : --
  TDM encapsulation number : 8
  jitter-buffer            : 8
  idle-code                : ff
  rtp-header               : disable
  Main or Secondary    : Main
  load balance type    : flow
  Access-port          : false
  VC tunnel/token info : 0 tunnels/tokens
  Backup TNL Type      : lsp   , TNL ID : 0x0
  Create time          : 0 days, 0 hours, 0 minutes, 9 seconds
  UP time              : 0 days, 0 hours, 0 minutes, 0 seconds
  Last change time     : 0 days, 0 hours, 0 minutes, 9 seconds
  VC last up time      : 0000/00/00 00:00:00
  VC total up time     : 0 days, 0 hours, 0 minutes, 0 seconds
  CKey                 : 4
  NKey                 : 3
  BFD for PW           : unavailable
```

Table 12-142 Description of the **display mpls static-l2vc** command output

Item	Description
TDM encapsulation number	Number of encapsulated TDM frames in Circuit Emulation Services over Packet Switch Network (CESoPSN) or Structure-Agnostic Time Division Multiplexing over Packet (SAToP) packets in the TDMoPSN application.
jitter-buffer	Depth of the jitter buffer, that is, the maximum allowed jitter delay.

Copyright © Huawei Technologies Co., Ltd.

Item	Description
idle-code	Idle code that is filled manually when a jitter buffer underflow occurs.
rtp-header	Whether the RTP header is added to the transparently transmitted TDM frame.

Related Topics

12.12.24 mpls static-l2vc

12.12.8 display mpls static-l2vc brief

12.12.8 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:  1,  1 up,  0 down

*Client Interface     : Ethernet1/0/0 is up
 AC Status            : up
 VC State             : up
 VC ID                : 0
 VC Type              : Ethernet
```

 Copyright © Huawei Technologies Co., Ltd.

```
Destination         : 3.3.3.9
```

Table 12-143 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.
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.

Display brief information about the static VC configured on a TDM interface.

```
<Huawei> display mpls static-l2vc brief
 Total svc connections:  1,  0 up,  1 down

 *Client Interface     : Serial2/0/0 is up
  AC Status            : up
  VC State             : down
  VC ID                : 112
  VC Type              : CESoPSN basic mode
  Destination          : 1.1.1.9
  TDM encapsulation number : 8
  jitter-buffer            : 8
  idle-code                : ff
  rtp-header               : disable
```

 Copyright © Huawei Technologies Co., Ltd.

Table 12-144 Description of the **display mpls static-l2vc** command output

Item	Description
TDM encapsulation number	Number of encapsulated TDM frames in Circuit Emulation Services over Packet Switch Network (CESoPSN) or Structure-Agnostic Time Division Multiplexing over Packet (SAToP) packets in the TDMoPSN application.
jitter-buffer	Depth of the jitter buffer, that is, the maximum allowed jitter delay.
idle-code	Idle code that is filled manually when a jitter buffer underflow occurs.
rtp-header	Indicates Whether the RTP header is added to the transparently transmitted TDM frames.

Related Topics

12.12.24 mpls static-l2vc

12.11.7 display mpls l2vpn forwarding-info

12.12.9 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.
encapsulation *encapsulation-type*	Specifies the PW encapsulation type.	Currently, the device supports the following types encapsulation types: **ethernet**, **vlan**, **satop-e1**, and **cesopsn-basic**.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
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             : 2013/11/24 14:31:31
 VC total up time            : 0 days, 2 hours, 12 minutes, 51 seconds
```

 Copyright © Huawei Technologies Co., Ltd.

Table 12-145 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.

Copyright © Huawei Technologies Co., Ltd.

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              : 2013/11/24 14:31:31
 VC total up time             : 0 days, 2 hours, 12 minutes, 51 seconds
```

 Copyright © Huawei Technologies Co., Ltd.

Table 12-146 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.

 Copyright © Huawei Technologies Co., Ltd.

```
<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             : 2013/11/24 14:31:31
 VC total up time            : 0 days, 2 hours, 12 minutes, 51 seconds
```

Related Topics

12.12.25 mpls switch-l2vc

12.12.10 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

 Copyright © Huawei Technologies Co., Ltd.

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 : 3, 0 up, 3 down

*Switch-l2vc type           : LDP<---->LDP
 Peer IP Address            : 2.2.2.2, 3.3.3.9
 VC ID                    : 18, 180
 VC Type                    : SAT E1 over Packet
 VC State                   : up
 Session State              : up, up

*Switch-l2vc type           : LDP<---->SVC
 Peer IP Address            : 3.3.3.3, 4.4.4.9
 VC ID                    : 19, 119
 VC Type                    : Ethernet
 VC State                   : up
 Session State              : up, up

*Switch-l2vc type           : SVC<---->SVC
 Peer IP Address            : 1.1.1.1, 2.2.2.9
 VC ID                    : 113, 1123
 VC Type                    : CESoPSN basic mode
 VC State                   : up
 In/Out Label               : 16/10, 17/150
```

Table 12-147 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.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
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.

Related Topics

12.12.25 mpls switch-l2vc

12.12.11 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

None.

Example

Display information about all PW templates.

```
<Huawei> display pw-template
Total PW template number : 1
  PW Template Name : p2
  PeerIP           : --
  Tnl Policy Name  : --
```

 Copyright © Huawei Technologies Co., Ltd.

```
CtrlWord         : Disable
MTU              : 1500
Max Atm Cells    : 28
ATM Pack Overtime: 1000
Seq-Number       : Disable
Transmit ATM Cells      : --
TDM Encapsulation Number: 8
Jitter-Buffer           : 8
Jitter-Buffer-Cep       : 1000
Payload-Compression DBA : --
Idle-Code               : ff
Rtp-Header              : Disable
VCCV Capability  : alert ttl lsp-ping bfd
Total PW         : 0, Static PW : 0, LDP PW : 0
```

Table 12-148 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).

Copyright © Huawei Technologies Co., Ltd.

Item	Description
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.
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.

Related Topics

12.12.29 pw-template

12.12.12 idle-code

Function

The **idle-code** command sets the idle code that is filled when a jitter buffer underflow occurs.

The **undo idle-code** command deletes the idle code that is filled when a jitter buffer underflow occurs.

By default, the system sets the idle code to FF when a jitter buffer underflow occurs.

Format

idle-code *idle-code-value*

undo idle-code

Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
idle-code-value	Specifies the value of the idle code that is filled when a jitter buffer underflow occurs.	The value is a hexadecimal number that ranges from 00 to FF. The default value is FF.

Views

PW template view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

This command is used to set the value of the idle code that is filled when a jitter buffer underflow occurs. A jitter buffer underflow occurs when the device needs to read packets but there are not sufficient packets in the buffer. The idle code has no significance, and can be set randomly.

Prerequisite

A PW template has been created and the PW template view is displayed by running the **pw-template** command in the system view.

Follow-up Procedure

After running the **idle-code** command, run the **reset pw** command to apply the attributes in the PW template to the PW. To check whether the idle code has taken effect on the PW, run the **display mpls l2vc** command to view the **idle-code** field.

Precautions

If you specify the **idle-code** parameter in the **mpls l2vc** command and run the **idle-code** command in the PW template view simultaneously, the idle code specified in the **mpls l2vc** command takes effect.

Example

Set the idle code to 0 when a jitter buffer underflow occurs.

```
<Huawei> system-view
[Huawei] pw-template tdmpw
[Huawei-pw-template-tdmpw] idle-code 0
```

Related Topics

12.12.13 jitter-buffer depth

12.12.29 pw-template

 Copyright © Huawei Technologies Co., Ltd.

12.12.13 jitter-buffer depth

Function

The **jitter-buffer depth** command sets the depth of the jitter buffer in the TDMoPSN application.

The **undo jitter-buffer depth** command restores the default maximum depth of the TDM jitter buffer.

By default, the depth of the jitter buffer is 8 ms.

Format

jitter-buffer depth *depth*

undo jitter-buffer depth

Parameters

Parameter	Description	Value
depth *depth*	Specifies the depth of the jitter buffer, that is, the allowed maximum jitter delay.	The value is an integer that ranges from 4 to 64, in milliseconds. The default value is 8 ms.

Views

PW template view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A jitter buffer is designed to smooth the transmission jitter. The jitter buffer receives TDM services at different rates, buffers TDM frames, and then sends the frames to the next hop at a certain rate. In this manner, the transmission jitter is smoothed. The **jitter-buffer depth** command can be run on TDM AC interfaces only.

The shallower the jitter buffer is, the weaker the anti-jitter capabilities are. The deeper the jitter buffer is, the stronger the anti-jitter capabilities are, but a long transmission delay will be introduced when data flows are reconstructed. If the jitter buffer is set to a too large or too small value, service transmission quality will be affected.

Therefore, during the configuration, you need to set a proper depth for the jitter buffer by considering the network bandwidth, jitter, and sensitivity of various services to the delay.

 Copyright © Huawei Technologies Co., Ltd.

- An 8 ms-deep jitter buffer is recommended for voice services because they are sensitive to the delay. The depth can be increased for video and data services.
- If the network topology is complex and the jitter of link transmission is large, you can increase the depth of the jitter buffer. If the network topology is simple and the jitter of link transmission is small, you can decrease the depth of the jitter buffer.
- If the initial wait delay is long, you can decrease the depth of the jitter buffer.

For a PSN, you need to pre-set the depth of the jitter buffer. More importantly, you need to monitor the jitter prevention effects of the jitter buffer with different depths and adjust the depth of the jitter buffer accordingly. In this manner, you can determine the depth of the jitter buffer based on service requirements.

Prerequisites

A PW template has been created and the PW template view is displayed by running the **pw-template** command in the system view.

Follow-up Procedure

After running the **jitter-buffer depth** command, run the **reset pw** command to apply the attributes in the PW template to the PW. To check whether the jitter buffer depth has taken effect on the PW, run the **display mpls l2vc** command to view the **jitter-buffer** field.

Precautions

If you specify the **jitter-buffer** parameter in the **mpls l2vc** command and run the **jitter-buffer depth** command in the PW template view simultaneously, the jitter buffer depth specified in the **mpls l2vc** command takes effect.

Example

Set the depth of the jitter buffer to 4 ms.

```
<Huawei> system-view
[Huawei] pw-template tdmpw
[Huawei-pw-template-tdmpw] jitter-buffer depth 4
```

Related Topics

12.12.12 idle-code

12.12.29 pw-template

12.12.32 tdm-encapsulation-number

12.12.14 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.

 Copyright © Huawei Technologies Co., Ltd.

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
```

12.12.15 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.

 Copyright © Huawei Technologies Co., Ltd.

Format

mpls l2vc { *ip-address* | **pw-template** *pw-template-name* } * *vc-id* [[**tunnel-policy** *policy-name*] | [{ **control-word** | **no-control-word** }] | [{ **raw** | **tagged** }] | [**secondary**]] *

undo mpls l2vc { *ip-address* | **pw-template** *pw-template-name* } * *vc-id* [[**tunnel-policy** *policy-name*] | [{ **control-word** | **no-control-word** }] | [{ **raw** | **tagged** }] | [**secondary**]] *

undo mpls l2vc [**secondary**]

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.
tunnel-policy *policy-name*	Specifies a tunnel policy name for the L2VC. If no name is specified for a tunnel policy, 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. If the name of the tunnel policy is specified but no tunnel policy is configured, the default tunnel policy is still used.	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 service-delimiting (SD) tag from a packet. This parameter is required when the AC is an Ethernet link.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
tagged	Retains the SD tag in a packet. This parameter is required when the AC is an Ethernet link.	-
control-word	Enables the control word function.	-
no-control-word	Disables the control word function.	-
secondary	Indicates that the VC is 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.	-

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.

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.

Copyright © Huawei Technologies Co., Ltd.

- 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 parameters **raw** and **tagged** can be used only for Ethernet links.
- The MTU value is specified when you create Martini or PWE3 VLLs and is used for interconnection between the router 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**, **no-control-word**, **idle-code** *idle-code-value*, **jitter-buffer**, **tdm-encapsulation** *number*, and **tdm-sequence-number**.

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.
- To configure TDM PWE3, run the **link-protocol tdm** command to set the link layer protocol to TDM before you run this command to configure a PW.

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
```

Related Topics

12.12.3 display mpls l2vc

12.11.7 display mpls l2vpn forwarding-info

12.12.16 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

 Copyright © Huawei Technologies Co., Ltd.

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.

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]
```

12.12.17 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.

 Copyright © Huawei Technologies Co., Ltd.

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

When a Huawei device and a non-Huawei device need to set up a PW using LDP but the non-Huawei device cannot process L2VPN label request messages, use this command to enable the two devices to communicate. Do not use this command in other conditions.

Example

Disable the device from sending L2VPN label request messages to a peer with the LSR ID being 2.2.2.9.

```
<Huawei> system-view
[Huawei] mpls l2vpn
[Huawei-l2vpn] mpls l2vpn no-request-message peer 2.2.2.9
```

12.12.18 mpls l2vpn oam-mapping

Function

The **mpls l2vpn oam-mapping** command enables the mapping between the AC status and the Packet Switching Network (PSN) status.

The **undo mpls l2vpn oam-mapping** command disables the mapping between the AC status and the PSN status.

By default, the mapping between the AC status and the PSN status is disabled.

Format

mpls l2vpn oam-mapping 3ah

 Copyright © Huawei Technologies Co., Ltd.

undo mpls l2vpn oam-mapping

Parameters

Parameter	Description	Value
3ah	Enables fault detection and fault notification defined in IEEE 802.3ah.	-

Views

Ethernet interface view, GE interface view, XGE interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In VLL FRR or PWE3 FRR scenarios, PEs and CEs do not advertise their primary/secondary status and link status to each other. PW OAM and AC OAM need to be configured to monitor PW and AC status respectively. OAM mapping is enabled on the PEs to associate PW OAM with AC OAM.

After the **mpls l2vpn oam-mapping** command is configured on a PE, the system generates the mapping table between the AC status and the PSN status. If a fault occurs on an AC, the local PE will notify the remote PE of the AC fault. If a fault occurs on a PW, the local PE will notify the local CE of the fault. Timely fault notification allows PEs and CEs to coordinate with each other to implement end-to-end FRR.

Prerequisites

OAM fault detection and notification have been configured for the corresponding AC.

Configuration Impact

After the mapping between the AC status and the PSN status is enabled, if a fault occurs on the local AC:

- If BFD for PW is enabled, the local AC notifies the remote PE of the AC fault using BFD and the signaling protocol.
- If BFD for PW is disabled, the local AC notifies the remote PE of the AC fault using the signaling protocol.

Follow-up Procedure

After configuring this command, run the **display mpls l2vc interface** command to check the AC link status. The AC link status is displayed in the **Local AC OAM State** field of the command output.

 Copyright © Huawei Technologies Co., Ltd.

Example

Enable fault detection and notification defined in IEEE 802.3ah on an Ethernet interface.

```
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] mpls l2vc 1.1.1.1 101
[Huawei-GgiabitEthernet1/0/0] mpls l2vpn oam-mapping 3ah
```

Related Topics

12.12.5 display mpls l2vc oam-mapping

12.12.19 mpls l2vpn pw performance disable

Function

The **mpls l2vpn pw performance disable** command disables the function of PW performance information collection on a TDM interface.

The **undo mpls l2vpn pw performance disable** command restores the default setting.

By default, the function of PW performance information collection is enabled on a TDM interface.

Format

mpls l2vpn pw performance disable

undo mpls l2vpn pw performance disable

Parameters

None

Views

TDM interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After a PW is configured on a TDM interface, the function of PW performance information collection is automatically enabled on the TDM interface. The system collects statistics about the packets sent and received by the primary PW at an interval of 15 minutes. If other performance statistics collection methods are available or you want to further improve system performance, you can run the **mpls l2vpn pw performance disable** command to disable the function of PW performance information collection.

Prerequisites

 Copyright © Huawei Technologies Co., Ltd.

A PW has been configured on the interface because this command needs to be associated with a PW.

NOTE

This command applies to only static PWs and dynamic LDP PWs.

Follow-up Procedure

If the function of PW performance information collection is enabled, you can run the **display mpls l2vpn interface performance** command to view PW performance statistics collected during the latest 15 minutes to obtain the current working status of the primary PW.

Precautions

The **mpls l2vpn pw performance disable** and **undo mpls l2vpn pw performance disable** commands apply to only primary PWs.

Example

Disable PW performance information collection on Serial2/0/0.

```
<Huawei> system-view
[Huawei] interface serial 2/0/0
[Huawei-Serial2/0/0] mpls l2vpn pw performance disable
```

Related Topics

12.12.6 display mpls l2vpn interface performance

12.12.20 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

 Copyright © Huawei Technologies Co., Ltd.

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

 Copyright © Huawei Technologies Co., Ltd.

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 gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] mpls l2vc 1.1.1.9 100
[Huawei-GigabitEthernet1/0/0] mpls l2vc 2.2.2.9 200 secondary
[Huawei-GigabitEthernet1/0/0] mpls l2vpn reroute delay 15 resume 20
```

Related Topics

12.12.15 mpls l2vc

12.12.21 mpls l2vpn service-name

Function

The **mpls l2vpn service-name** command sets the name of an SVC or Martini VLL 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.

 Copyright © Huawei Technologies Co., Ltd.

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 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 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.

 Copyright © Huawei Technologies Co., Ltd.

- On each PE, an L2VPN service name is unique.
- The **mpls l2vpn service-name** command cannot be run on a loopback interface.

Example

Set an L2VPN service name to **pw1** on a service interface.

```
<Huawei> system-view
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] mpls l2vc 10.1.1.1 1
[Huawei-GigabitEthernet1/0/0] mpls l2vpn service-name pw1
```

Related Topics

12.11.2 ccc interface out-interface

12.12.22 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 PWE3 FRR, 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.

 Copyright © Huawei Technologies Co., Ltd.

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.

Example

Enable the device to receive packets from both the primary and secondary PWs on GE1/0/0.

```
<Huawei> system-view
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] mpls l2vc 1.1.1.1 1
[Huawei-GigabitEthernet1/0/0] mpls l2vc 2.2.2.2 2 secondary
[Huawei-GigabitEthernet1/0/0] mpls l2vpn stream-dual-receiving
```

Related Topics

12.11.20 mpls l2vc

12.12.23 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*]

 Copyright © Huawei Technologies Co., Ltd.

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. 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.

 Copyright © Huawei Technologies Co., Ltd.

- 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
```

12.12.24 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**] | **idle-code** *idle-code-value* | **jitter-buffer** *depth* | **tdm-encapsulation** *number* | **tdm-sequence-number** | **secondary**] *

undo mpls static-l2vc [**secondary**]

undo mpls static-l2vc { { **destination** *ip-address* | **pw-template** *pw-template-name vc-id* } * | **destination** *ip-address vc-id* } **transmit-vpn-label** *transmit-label-*

 Copyright © Huawei Technologies Co., Ltd.

value **receive-vpn-label** *receive-label-value* [**tunnel-policy** *tnl-policy-name* | [**control-word** | **no-control-word**] | [**raw** | **tagged**] | **idle-code** *idle-code-value* | **jitter-buffer** *depth* | **tdm-encapsulation** *number* | **tdm-sequence-number** | **secondary**] *

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 service-delimiting (SD) tag from a packet. This parameter is required when the AC is an Ethernet link.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
tagged	Retains the SD tag in a packet. This parameter is required when the AC is an Ethernet link.	-
idle-code *idle-code-value*	Specifies the idle code that is filled in manually when a jitter buffer underflow occurs. This parameter is required when the AC is a TDM link.	The value ranges from 00 to FF, in hexadecimal notation. The default value is FF.
jitter-buffer *depth*	Specifies the depth of the jitter buffer, that is, the allowed maximum jitter delay. This parameter is required when the AC is a TDM link.	The value is an integer that ranges from 4 to 64, in milliseconds. The default value is 8 ms.
tdm-encapsulation *number*	Specifies the number of TDM frames encapsulated in a CESoPSN packet. This parameter is required when the AC is a TDM link.	The value is an integer, which can be 8, 16, 24, 32, or 40. The default value is 8. When the interface card where the AC interface locates is 8SA, 8E1T1-M or 8E1T1-F, the interface can encapsulate a maximum of 16 TDM frames in a packet. If the value is larger than 16, the interface only encapsulates 16 TDM frames in a packet.
tdm-sequence-number	Sets the sequence number of the first frame encapsulated for TDM transparent transmission to 1. This parameter is required when the AC is a TDM link.	-
secondary	Configures the PW as a static secondary PW. By default, a created PW is a primary PW.	-

Copyright © Huawei Technologies Co., Ltd.

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**, **no-control-word**, **idle-code** *idle-code-value*, **jitter-buffer**, **tdm-encapsulation** *number*, and **tdm-sequence-number**.

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.
- To configure TDM PWE3, run the **link-protocol tdm** command to set the link layer protocol to TDM before you run this command to configure a PW.

 Copyright © Huawei Technologies Co., Ltd.

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
```

Delete a static VC.

```
<Huawei> system-view
[Huawei] interface vlanif 10
[Huawei-Vlanif10] undo mpls static-l2vc
```

Related Topics

12.12.7 display mpls static-l2vc
12.12.16 mpls l2vpn

12.12.25 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*] **between** *ip-address vc-id* **trans** *trans-label* **recv** *received-label* [**tunnel-policy** *policy-name*] **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*] **between** *ip-address vc-id* **trans** *trans-label* **recv** *received-label* [**tunnel-policy** *policy-name*] **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*] **between** *ip-address vc-id* [**tunnel-policy** *policy-name*] **encapsulation** *encapsulation-type* [**control-word-transparent**]

undo mpls switch-l2vc *ip-address vc-id* [**tunnel-policy** *policy-name*] **between** *ip-address vc-id* [**tunnel-policy** *policy-name*] **encapsulation** *encapsulation-type* [**control-word-transparent**]

Mixed PW

 Copyright © Huawei Technologies Co., Ltd.

mpls switch-l2vc *ip-address vc-id* [**tunnel-policy** *policy-name*] **between** *ip-address vc-id* **trans** *trans-label* **recv** *received-label* [**tunnel-policy** *policy-name*] **encapsulation** *encapsulation-type* [**mtu** *mtu-value*] [**control-word** [**cc** { **alert** | **cw** } * **cv lsp-ping**] | [**no-control-word**] [**cc alert cv lsp-ping**]] [**timeslotnum** *timeslotnum*] [**tdm-encapsulation** *number*] [**control-word-transparent**]

undo mpls switch-l2vc *ip-address vc-id* [**tunnel-policy** *policy-name*] **between** *ip-address vc-id* **trans** *trans-label* **recv** *received-label* [**tunnel-policy** *policy-name*] **encapsulation** *encapsulation-type* [**mtu** *mtu-value*] [**control-word** [**cc** { **alert** | **cw** } * **cv lsp-ping**] | [**no-control-word**] [**cc alert cv lsp-ping**]] [**timeslotnum** *timeslotnum*] [**tdm-encapsulation** *number*] [**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.
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 a tunnel policy name for the L2VC. If no name is specified for a tunnel policy, 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. If the name of the tunnel policy is specified but no tunnel policy is configured, the default tunnel policy is used.	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.
between	Specifies the switching PW that corresponds to the PW	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
encapsulation *encapsulation-type*	Specifies the encapsulation type of a static PW.	The encapsulation types supported by PW switching are **ethernet**, **vlan**, **satop-e1**, and **cesopsn-basic**.
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.	-

 Copyright © Huawei Technologies Co., Ltd.

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.	-
timeslotnum *timeslotnum*	Specifies the number of timeslots in TDM PWE3.	The value is an integer. • If the encapsulation type of a non-channelized interface is **satop-e1**, you do not need to set the number of timeslots and the total number of supported timeslots is used by default. • If the encapsulation type of a channelized interface is **cesopsn-basic**, you need to set this number and the value ranges from 1 to 32.
tdm-encapsulation *number*	Specifies the number of TDM frames encapsulated in a packet.	The value is an integer, which can be 8, 16, 24, 32, or 40. The default value is 8. When the interface card where the AC interface locates is 8SA, 8E1T1-M or 8E1T1-F, the interface can encapsulate a maximum of 16 TDM frames in a packet. If the value is larger than 16, the interface only encapsulates 16 TDM frames in a packet.
all	Deletes all PW switching.	-

Copyright © Huawei Technologies Co., Ltd.

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 static 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.

When you configure static PW switching, the parameters that can be configured vary with the PW encapsulation type and the details are as follows:

- If *encapsulation-type* is set to **ethernet** or **vlan**, the following parameters can be specified: **control-word** [**cc** { **alert** | **cw** } * **cv lsp-ping**], and [**no-control-word**] [**cc alert cv lsp-ping**].
- If *encapsulation-type* is set to **satop-e1**, the following parameters can be specified: [**no-control-word**] [**cc alert cv lsp-ping**].
- If *encapsulation-type* is set to **cesopsn-basic**, the following parameters can be specified: **control-word** [**cc** { **alert** | **cw** } * **cv lsp-ping**], and [**no-control-word**] [**cc alert cv lsp-ping**].

 Copyright © Huawei Technologies Co., Ltd.

When you configure mixed PW switching, the parameters that can be configured vary with the PW encapsulation type and the details are as follows:

- If *encapsulation-type* is set to **ethernet** or **vlan**, the following parameters can be specified: **mtu** *mtu-value*, **control-word** [**cc** { **alert** | **cw** } * **cv lsp-ping**], and [**no-control-word**] [**cc alert cv lsp-ping**].
- If *encapsulation-type* is set to **satop-e1**, the following parameters can be specified: **mtu** *mtu-value*, **control-word**, **no-control-word**, and **tdm-encapsulation** *number*.
- If *encapsulation-type* is set to **cesopsn-basic**, the following parameters can be specified: **mtu** *mtu-value*, **control-word**, **no-control-word**, **timeslotnum** *timeslotnum*, and **tdm-encapsulation** *number*.

  The **timeslotnum** *timeslotnum* must be configured.

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**, **tdm-encapsulation** *number*, **timeslotnum** *timeslotnum*, and **mtu** *mtu-value*.

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
```

Related Topics

12.12.9 display mpls switch-l2vc

12.11.21 mpls l2vpn

12.12.26 mtu (PW template view)

Function

The **mtu** command specifies the MTU in a PW template.

 Copyright © Huawei Technologies Co., Ltd.

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
```

Related Topics

12.12.29 pw-template

 Copyright © Huawei Technologies Co., Ltd.

12.12.27 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

ip-address in this command is the same as that in the **mpls l2vc** command. You can update the IP address of the peer in real time. After updating the IP address, run the **reset pw** command to make it take effect if the PW is used. If the PW is not used, you do not need to restart the PW after updating the IP address.

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
```

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

12.12.29 pw-template

12.12.28 ping vc

Function

The **ping vc** command detects the status of a PW.

Format

ping vc *pw-type pw-id* [**-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*] [**uniform**]

ping vc *pw-type pw-id* [**-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*] [**uniform**]

ping vc *pw-type pw-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**] [**remote** *remote-ip-address* | **draft6**] * [**uniform**]

ping vc *pw-type pw-id* [**-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*] [**uniform**]

Parameters

Parameter	Description	Value
pw-type	Specifies the encapsulation type of a local PW.	Currently, PWs of the following types are supported: **ethernet**, **vlan**.
pw-id	Specifies the ID of a local PW.	The value is an integer that ranges from 1 to 4294967295.
-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.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
-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 larger 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. The value must be smaller than the MTU value of the interface.
-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.	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.	-

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
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.	-
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 version of the **ping vc** command. If this parameter is specified, the ping operation is performed based on "draft-ietf-mpls-lsp-ping-06".	-
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.	-

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
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.

 Copyright © Huawei Technologies Co., Ltd.

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 an 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
```

Related Topics

12.12.34 tracert vc

12.12.29 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.

 Copyright © Huawei Technologies Co., Ltd.

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 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 may 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**.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> system-view
[Huawei] pw-template pwt1
[Huawei-pw-template-pwt1]
```

Related Topics

12.12.2 control-word
12.12.26 mtu (PW template view)
12.12.11 display pw-template
12.12.27 peer-address
12.12.33 tnl-policy (PW template view)
12.12.30 reset pw

12.12.30 reset pw

Function

The **reset pw** command re-creates a PW or a PW template.

Format

reset pw { *pw-id pw-type* | **pw-template** *pw-template-name* }

Parameters

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**, **satop-e1**, and **cesopsn-basic**.
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

 Copyright © Huawei Technologies Co., Ltd.

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
```

Related Topics

12.12.29 pw-template

12.12.31 snmp-agent trap enable feature-name l2vpn

Function

The **snmp-agent trap enable feature-name l2vpn** command enables the trap function for the L2VPN module.

The **undo snmp-agent trap enable feature-name l2vpn** command disables the trap function for the L2VPN module.

By default, the trap function is disabled for the L2VPN module.

Format

snmp-agent trap enable feature-name l2vpn [**trap-name** { **hwcccvcdown** | **hwcccvcup** | **hwpwvcbackup** | **hwpwvcdeleted** | **hwpwvcdown** | **hwpwvcstatuschange** | **hwpwvcswitchptow** | **hwpwvcswitchwtop** | **hwpwvcup** | **hwsvcdeleted** | **hwsvcdown** | **hwsvcswitchptow** | **hwsvcswitchwtop** | **hwsvcup** | **hwVpwsPwRedundancyDegraded** | **hwVpwsPwRedundancyDegradedClear** }]

undo snmp-agent trap enable feature-name l2vpn [**trap-name** { **hwcccvcdown** | **hwcccvcup** | **hwpwvcbackup** | **hwpwvcdeleted** | **hwpwvcdown** | **hwpwvcstatuschange** | **hwpwvcswitchptow** | **hwpwvcswitchwtop** | **hwpwvcup** | **hwsvcdeleted** | **hwsvcdown** | **hwsvcswitchptow** | **hwsvcswitchwtop** | **hwsvcup** | **hwVpwsPwRedundancyDegraded** | **hwVpwsPwRedundancyDegradedClear** }]

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
trap-name	Indicates the traps of L2VPN events of specified types.	-
hwcccvcdown	Enables or disables the trap indicating that the status of a CCC VC changes to Down.	-
hwcccvcup	Enables or disables the trap indicating that the status of a CCC VC changes to Up.	-
hwpwvcbackup	Enables or disables the trap indicating that the status of a PWE3 VC changes to Backup.	-
hwpwvcdeleted	Enables or disables the trap indicating that a PWE3 VC is deleted.	-
hwpwvcdown	Enables or disables the trap indicating that the status of a PWE3 VC changes to Down.	-
hwpwvcstatuschange	Enables or disables the trap indicating that the status of a PWE3 VC changes.	-
hwpwvcswitchptow	Enables or disables the trap indicating that a PWE3 PW changes from the secondary state to the primary state.	-
hwpwvcswitchwtop	Enables or disables the trap indicating that a PWE3 PW changes from the primary state to the secondary state.	-
hwpwvcup	Enables or disables the trap indicating that the status of a PWE3 VC changes to Up.	-
hwsvcdeleted	Enables or disables the trap indicating that an SVC is deleted.	-

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
hwsvcdown	Enables or disables the trap indicating that the status of an SVC changes to Down.	-
hwsvcswitchptow	Enables or disables the trap indicating that an SVC PW changes from the secondary state to the primary state.	-
hwsvcswitchwtop	Enables or disables the trap indicating that an SVC PW changes from the primary state to the secondary state.	-
hwsvcup	Enables or disables the trap indicating that the status of an SVC changes to Up.	-
hwVpwsPwRedundancyDegraded	Indicates a Huawei-specific trap reported when the primary or secondary PW for PW APS degrades.	-
hwVpwsPwRedundancyDegradedClear	Indicates a Huawei-specific trap reported when the primary or secondary PW for PW APS recovers.	-

Views

System view

Default Level

3: Management level

Usage Guidelines

The L2VPN module is not configured with the function of excessive traps. To enable the traps of one or more events, specify **trap-name**.

Example

Enable the system to generate an alarm when a VC in CCC mode goes Down.

```
<Huawei> system-view
[Huawei] snmp-agent trap enable feature-name l2vpn trap-name hwcccvcdown
```

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

12.11.14 display snmp-agent trap feature-name l2vpn all

12.12.32 tdm-encapsulation-number

Function

The **tdm-encapsulation-number** command configures the number of TDM frames encapsulated in a Circuit Emulation Services over Packet Switch Network (CESoPSN) or Structure-Agnostic Time Division Multiplexing over Packet (SAToP) packet in the TDMoPSN application.

The **undo tdm-encapsulation-number** command restores the default number of TDM frames encapsulated in a CESoPSN or SAToP packet.

By default, the number of encapsulated TDM frames in a CESoPSN or SAToP packet is 8.

Format

tdm-encapsulation-number *number*

undo tdm-encapsulation-number

Parameters

Parameter	Description	Value
number	Specifies the number of TDM frames encapsulated in a CESoPSN or SAToP packet.	The value is an integer, which can be 8, 16, 24, 32, or 40. The default value is 8. When the interface card where the AC interface locates is 8SA, 8E1T1-M or 8E1T1-F, the interface can encapsulate a maximum of 16 TDM frames in a packet. If the value is larger than 16, the interface only encapsulates 16 TDM frames in a packet.

Views

PW template view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When a dynamic PW is configured on a TDM interface, three parameters need to be negotiated between the two ends of the PW. The parameters are the RTP header, time slot number, and time slot number x number of encapsulated frames.

 Copyright © Huawei Technologies Co., Ltd.

You can configure the number of TDM frames encapsulated in each PW packet. The smaller the number of frames encapsulated in a packet, the shorter the transmission delay but the larger the encapsulation overhead. The larger the number of frames encapsulated in a packet, the higher the bandwidth utilization but the longer the encapsulation delay.

Prerequisite

A PW template has been created and the PW template view is displayed by running the **pw-template** command in the system view.

Configuration Impact

After the **tdm-encapsulation-number** command is run, the two ends of a PW will negotiate the number of frames encapsulated in each packet. If the values at two ends of a PW are different, the PW cannot go Up.

Follow-up Procedure

After running the **tdm-encapsulation-number** command, run the **reset pw** command to enable the attributes in the PW template to take effect on the PW. To check whether the configuration of the number of TDM frames encapsulated in each packet has taken effect on the PW, run the **display mpls l2vc** command to view the **local TDM Encap Num** field.

Precautions

The **mpls l2vc** command can also be used to configure the number of TDM frames encapsulated in each packet if **tdm-encapsulation** is specified in the command. If both the **mpls l2vc** command and the **tdm-encapsulation-number** command are used to configure the number of TDM frames encapsulated in each packet, the value specified by the **mpls l2vc** command takes precedence over the **tdm-encapsulation-number** effect.

Example

Set the number of the TDM frames encapsulated in a CESoPSN or SAToP packet to 16.

```
<Huawei> system-view
[Huawei] pw-template tdmpw
[Huawei-pw-template-tdmpw] tdm-encapsulation-num 16
```

Related Topics

12.12.13 jitter-buffer depth

12.12.29 pw-template

12.12.33 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.

 Copyright © Huawei Technologies Co., Ltd.

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 the 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
```

Related Topics

12.12.29 pw-template

12.12.34 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* [**-exp** *exp-value* | **-f** *first-ttl* | **-m** *max-ttl* | **-r** *reply-mode* | **-t** *timeout-value*] * **control-word** [**draft6**] [**full-lsp-path**] [**uniform**]

 Copyright © Huawei Technologies Co., Ltd.

tracert vc *pw-type pw-id* [**-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**] [**uniform**]

tracert vc *pw-type pw-id* [**-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**] [**uniform**]

tracert vc *pw-type pw-id* [**-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**] [**uniform**]

tracert vc *pw-type pw-id* [**-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**] [**uniform**]

Parameters

Parameter	Description	Value
pw-type	Specifies the PW type.	Currently, PWs of the following types are supported: **ethernet**, **vlan**.
pw-id	Specifies the local PW ID.	The value is an integer that ranges from 1 to 4294967295.
-exp *exp-value*	Specifies the EXP value in the outer label of an MPLS Echo Request packet. The default value is 0.	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.

 Copyright © Huawei Technologies Co., Ltd.

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.	-
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.	-

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
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.	-
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.	-
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". **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.

Prerequisite

- The UDP module of each node works properly; otherwise, the tracert operation will fail.

Copyright © Huawei Technologies Co., Ltd.

- 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.

 Copyright © Huawei Technologies Co., Ltd.

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 12-149 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.

Related Topics

12.12.28 ping vc

12.13 VPLS Configuration Commands

NOTE

The AR100&AR120&AR150&AR160&AR200 series routers do not support VPLS.

12.13.1 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.

 Copyright © Huawei Technologies Co., Ltd.

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
```

Related Topics

12.13.48 vsi

12.13.2 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**]

 Copyright © Huawei Technologies Co., Ltd.

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 • 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 CCC : 2
up (2), down (0)
Interface                   Encap Type          State    VC Type
GigabitEthernet0/0/2          ethernet            up       ccc
GigabitEthernet0/0/1          ethernet            up       ccc
```


Copyright © Huawei Technologies Co., Ltd.

Table 12-150 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 router.
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 • vpls-vc: VPLS connection

Related Topics

12.11.4 display mpls l2vc
12.11.12 display mpls static-l2vc

12.13.3 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

Copyright © Huawei Technologies Co., Ltd.

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                      512                0
 L2VPN VC Number                      512                1

 VPWS Capacity Statistics
 Statistics Item                Supported Number     Used Number
 L2VPN Local CCC Number               256                0
 L2VPN SVC Number                     256                0
 L2VPN LDP VC Number                  256                1
 L2VPN Switch VC Number               256                0

 VPLS Capacity Statistics
 Statistics Item                Supported Number     Used Number
 L2VPN VSI Number                     512                0
 L2VPN VSI VC Number                  512                0
 L2VPN VSI PWG Number                 8000               0
```

Table 12-151 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 SVC Number	Number of VLLs in SVC mode, including the maximum number allowed and number already used

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
L2VPN LDP VC Number	Number of LDP 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 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

12.13.4 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

 Copyright © Huawei Technologies Co., Ltd.

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 12-152 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

12.13.5 display traffic-statistics vsi

Function

The **display traffic-statistics vsi** command displays public network traffic statistics on all PWs of a specified VSI.

Format

display traffic-statistics vsi *vsi-name*

Parameters

Parameter	Description	Value
vsi-name	Specifies the name of a VSI.	The value is an existing VSI.

 Copyright © Huawei Technologies Co., Ltd.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

After VPLS configurations are complete, you can run this command to view public network traffic statistics on all PWs of a specified VSI, so that you can learn the running status of all PWs of the specified VSI.

Prerequisites

The following operations have been performed before this command is used:

Run the **traffic-statistics enable** command in the VSI-LDP view to enable statistics collection on public network traffic of all PWs.

Precautions

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 12-153 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.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Input	Number of packets received by the PW from the AC.
Output	Number of packets sent from the PW to the AC.

Related Topics

12.13.37 reset traffic-statistics vsi name

12.13.44 traffic-statistics enable (VSI-LDP view)

12.13.6 display traffic-statistics vsi peer

Function

The **display traffic-statistics vsi peer** command displays public network traffic statistics on a specified PW of a specified VSI.

Format

display traffic-statistics vsi *vsi-name 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 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

 Copyright © Huawei Technologies Co., Ltd.

After VPLS configurations are complete, you can run this command to view public network traffic statistics on a specified PW of a specified VSI, so that you can learn the running status of the PW of the specified VSI.

Prerequisites

The following operations have been performed before this command is used:

Run the **traffic-statistics peer enable** command in the VSI-LDP view to enable statistics collection on public network traffic of specified PWs.

Precautions

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 VPLS PW.

```
<Huawei> display traffic-statistics vsi newvsi peer 10.22.33.20
vsi-name: newvsi
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 12-154 Description of the **display traffic-statistics vsi peer** command output

Item	Description
vsi-name	VSI name.
Peer-address	IP address of the remote peer.
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.

Related Topics

12.13.38 reset traffic-statistics vsi name peer

12.13.45 traffic-statistics peer enable

 Copyright © Huawei Technologies Co., Ltd.

12.13.7 display vpls connection

Function

The **display vpls connection** command displays the VPLS connection.

Format

display vpls connection [**ldp** | **vsi** *vsi-name*] [**down** | **up**] [**verbose**]

Parameters

Parameter	Description	Value
ldp	Displays information about LDP 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.

Precautions

If no keyword or parameter is specified, information about all VPLS connections in Up state is displayed.

 Copyright © Huawei Technologies Co., Ltd.

Example

Display information about the connections of all VSIs.

```
<Huawei> display vpls connection

1 total connections,
connections: 1 up, 0 down, 1 ldp, 0 bgp, 0 bgpad

VSI Name: a2                        Signaling: ldp
VsiID     EncapType          PeerAddr        InLabel   OutLabel  VCState
2         vlan               3.3.3.9         18        18        up
```

Table 12-155 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. To set the value, run the **pwsignal** command.
VsiID	VSI ID. To set the value, run the **vsi-id** command.
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.

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       : 0x10x0000000001004c4be1
```

 Copyright © Huawei Technologies Co., Ltd.

Table 12-156 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. To set the value, run the **pwsignal** command.
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.

Related Topics

12.11.3 display l2vpn ccc-interface vc-type

12.13.48 vsi

12.13.8 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**]

Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
vsi *vsi-name*	Displays forwarding information of a specified VSI.	The value is an existing VSI.
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.

Precautions

- The **display vpls forwarding-info vsi** *vsi-name* command is used to display forwarding information of a specified VSI.

Copyright © Huawei Technologies Co., Ltd.

- 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.

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 12-157 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.
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
```

 Copyright © Huawei Technologies Co., Ltd.

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 12-158 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.
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.
NKey	Network key. Each NKey corresponds to one peer + tunnel policy.
CKey	User key. Each CKey corresponds to a PW.

 Copyright © Huawei Technologies Co., Ltd.

12.13.9 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 12-159 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.

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

12.13.33 ping vpls mac vsi

12.13.39 reset vpls-ping statistics

12.13.10 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 12-160 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.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
vpls-trace reply sent	Number of sent VPLS MAC Trace Reply packets.

Related Topics

12.13.42 trace vpls mac vsi
12.13.40 reset vpls-trace statistics

12.13.11 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

Copyright © Huawei Technologies Co., Ltd.

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 peers 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
```

Table 12-161 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. Currently, only static member discovery is supported.
PW Type	PW type.
Mac Learn	Mode of learning the MAC address.
Encap Type	Encapsulation type. • 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 Value	Maximum transmission unit. To set the value, run the **mtu** command.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Vsi State	Status of the VSI: • up: The VSI is in Up state. • down: The VSI is in Down state. • *down: The VSI is in Down state. The network administrator has run the **shutdown** command on this interface.

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
   Service Class          : --
   Color                  : --
   DomainId               : 255
   Domain Name            :
   Ignore AcState         : disable
   P2P VSI                : disable
   Create Time            : 0 days, 0 hours, 3 minutes, 57 seconds
   VSI State              : down

   VSI ID                 : 2
   LDP MAC-WITHDRAW       : mac-withdraw Enable
  *Peer Router ID         : 3.3.3.9
   Negotiation-vc-id      : 2
   primary or secondary   : primary
   ignore-standby-state   : no
   VC Label               : 1025
   Peer Type              : dynamic
   Session                : up
   Tunnel ID              : 0x7
   Broadcast Tunnel ID    : 0x7
   Broad BackupTunnel ID  : 0x0
   CKey                   : 4
   NKey                   : 3
   Stp Enable             : 0
   PwIndex                : 0
   Control Word           : disable
   BFD for PW             : unavailable

   Interface Name         : Ethernet0/0/2
   State                  : up
   Access Port            : false
   Last Up Time           : 2017/07/13 11:27:13
   Total Up Time          : 2 days, 2 hours, 6 minutes, 36 seconds

  **PW Information:

   *Peer Ip Address       : 3.3.3.9
   PW State               : up
   Local VC Label         : 1025
   Remote VC Label        : 1025
```

 Copyright © Huawei Technologies Co., Ltd.

```
Remote Control Word    : disable
PW Type                : label
Local  VCCV            : alert lsp-ping bfd
Remote VCCV            : alert lsp-ping bfd
Tunnel ID              : 0x7
Broadcast Tunnel ID    : 0x7
Broad BackupTunnel ID  : 0x0
Ckey                   : 0x4
Nkey                   : 0x3
Main PW Token          : 0x0
Slave PW Token         : 0x0
Tnl Type               : LSP
OutInterface           :
Backup OutInterface    :
Stp Enable             : 0
PW Last Up Time        : 2017/07/13 11:31:24
PW Total Up Time       : 2 days, 2 hours, 2 minutes, 25 seconds
```

Table 12-162 Description of the **display vpls 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. To set the value, run the **pwsignal** command.
Member Discovery Style	Member discovery mode.
PW MAC Learn Style	Mode of MAC address learning of the PW.
Encapsulation Type	VPLS encapsulation type of the VSI, namely, the encapsulation type of the packets transmitted over the VC: • vlan • ethernet
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 value on one end to be the same as that on the other end.
Diffserv Mode	VSI QoS mode.
Service Class	QoS service class of a VSI.

Copyright © Huawei Technologies Co., Ltd.

Item	Description
Color	QoS packet color of a VSI.
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
VSI ID	VSI ID 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.
LDP MAC-WITHDRAW	Whether the MAC withdraw function is enabled.
Peer Router ID	ID of the peer device.
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.
Peer Type	PW type of the peer.
Session	Status of the session between the local end and its peer. The status can be Up or Down.
Tunnel ID	Tunnel ID that is displayed only when the Martini VPLS is configured.

Copyright © Huawei Technologies Co., Ltd.

Item	Description
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.
Stp Enable	Whether STP for PW is enabled: ● 0: disabled ● 1: enabled
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: BFD is not configured. ● available: BFD is configured. ● timeout: BFD session creation timed out.
Interface Name	Name of the interface bound to the VSI.
State	Status of the AC bound to the VSI. ● up ● down
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.
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
Local VC Label	VC label distributed locally.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Remote VC Label	VC label distributed by the peer.
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	VCCV mode supported by the local end: • **alert lsp-ping bfd** (default value): VCCV is implemented by sending LSP ping and BFD packets in label alert mode when the control word function is disabled. • **cw alert lsp-ping bfd**: VCCV is implemented by sending LSP ping and BFD packets in control word, label alert mode when the control word function is enabled. • **--**: VCCV is disabled.
Remote VCCV	VCCV mode supported by the remote end: • **alert lsp-ping bfd** (default value): VCCV is implemented by sending LSP ping and BFD packets in label alert mode when the control word function is disabled. • **cw alert lsp-ping bfd**: VCCV is implemented by sending LSP ping and BFD packets in control word, label alert mode when the control word function is enabled. • **--**: VCCV is disabled. • **none**: The remote PW does not exist.
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 • 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.

 Copyright © Huawei Technologies Co., Ltd.

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
------------------------------------------------------------------------------
3.3.3.9         2               1025       1025        up
```

Display detailed information of PW status of a specific peer to a specified VSI.

```
<Huawei> display vsi name a2 peer-info 3.3.3.9

VSI Name: a2                                    Signaling: ldp
------------------------------------------------------------------------------
Peer            Transport       Local      Remote      VC
Addr            VC ID/TAII      VC Label   VC Label    State
------------------------------------------------------------------------------
3.3.3.9         2               1025       1025        up
```

Table 12-163 Description of the **display vsi peer-info** command output

Item	Description
Vsi Name	Name of the VSI.
Signaling	Type of the PW signaling.
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
```

 Copyright © Huawei Technologies Co., Ltd.

Table 12-164 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.
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.

Related Topics

12.13.14 display vsi remote
12.13.48 vsi

12.13.12 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

 Copyright © Huawei Technologies Co., Ltd.

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 12-165 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.
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.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Receive peer	Peer from which MAC Withdraw messages are received.
Last loop time	Time when the MAC Withdraw message loop occurs.

Related Topics

12.13.47 vpls mac-withdraw loop-detect enable

12.13.13 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 only.

Example

Display information about the outgoing interface of the VSI PW.

Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> display vsi pw out-interface
Total: 1
------------------------------------------------------------------------------
Vsi Name                    peer          vcid      interface
------------------------------------------------------------------------------
a2                          3.3.3.9       2         GigabitEthernet2/0/0
```

Table 12-166 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.

Related Topics

12.13.11 display vsi

12.13.14 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 ldp verbose

Parameters

Parameter	Description	Value
ldp	Displays information about remote VSIs using LDP signaling.	-
route-id *ip-address*	Displays information about remote VSIs of specified peers.	*ip-address* specifies the IPv4 address of the peer.
pw-id *pw-id*	Displays information about remote VSIs of a specified PW.	*pw-id* specifies the number of a VC. It is a decimal integer that ranges from 1 to 4294967295.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
verbose	Display details about the remote VSIs using LDP signaling.	-

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 ldp** command:

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 12-167 Description of the **display vsi remote ldp** command output

Item	Description
Vsi ID	ID of a remote VSI.
Peer RouterID	Remote peer address.
VC Label	Remote VC label.
Group ID	Remote group ID. The default value is 0.
Encap Type	Remote VC encapsulation type. • vlan • ethernet
MTU Value	MTU of a remote VC.
Vsi Index	Index of a remote VSI.

Copyright © Huawei Technologies Co., Ltd.

Item	Description
State 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. • -: The negotiated communication mode is Martini.

Display detailed information about remote VSIs using LDP signaling.

```
<Huawei> display vsi remote ldp verbose
Total remote LDP VC : 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 12-168 Description of the **display vsi remote ldp verbose** command output

Item	Description
Total remote LDP VC	Indicates the total number of remote LDP VC.
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.

 Copyright © Huawei Technologies Co., Ltd.

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.

Related Topics

12.13.11 display vsi

12.13.15 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.

Copyright © Huawei Technologies Co., Ltd.

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: 1
Code: AS(Admin Status), PS(Physical Status)
--------------------------------------------------------------------------------
Interface                       Vsi Name                    AS    PS
--------------------------------------------------------------------------------
GigabitEthernet0/0/1            1                           up    up
--------------------------------------------------------------------------------
```

Table 12-169 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: The VSI is in Up state. • down: The VSI is in Down state. • *down: The VSI is in Down state. The network administrator has run the **shutdown** command on this interface.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
PS	Physical status of the interface: • up: The physical status of the interface is Up. • down: The physical status of the interface is Down.

Related Topics

12.13.11 display vsi

12.13.16 encapsulation (VSI view)

Function

The **encapsulation** command configures the encapsulation type of the interface in the VSI view.

The **undo encapsulation** command restores the default encapsulation type of the interface in the VSI view.

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.

Copyright © Huawei Technologies Co., Ltd.

Prerequisites

The VSI ID has been configured using the **vsi-id** *vsi-id* command.

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
```

Related Topics

12.13.48 vsi

12.13.17 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.

 Copyright © Huawei Technologies Co., Ltd.

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
```

Related Topics

12.13.46 vpls ignore-ac-state

12.13.18 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

If the router 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.

Example

When configuring the VPLS in LDP mode, delete the VCCV byte from the Mapping packet.

```
<Huawei1> system-view
[Huawei] vsi vsi1 static
```

 Copyright © Huawei Technologies Co., Ltd.

```
[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
```

12.13.19 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

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 sends LDP MAC Withdraw messages to all peers when the status of the AC interface bound to the VSI 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:

 Copyright © Huawei Technologies Co., Ltd.

- 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
```

Related Topics

12.13.24 mac-withdraw enable

12.13.20 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

GE interface view, Ethernet interface view, GE sub-interface view, Ethernet sub-interface view

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

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.

Prerequisites

A VSI has been created by using the **vsi** command, and a VSI instance ID has been configured by using the **vsi-id** *vsi-id* command.

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 a sub-interface is bound to a VSI, you can delete the sub-interface only after unbinding it from the VSI.
- A sub-interface cannot be bound to the VSI instance that uses Ethernet encapsulation.
- 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.

Example

Bind a Gigabitethernet sub-interface to a 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] quit
[Huawei] interface gigabitethernet 0/0/1.1
[Huawei-GigabitEthernet0/0/1.1] dot1q termination vid 10
[Huawei-GigabitEthernet0/0/1.1] l2 binding vsi company1
```

Related Topics

12.13.11 display vsi

12.13.14 display vsi remote

12.13.21 mac-address blackhole vsi

Function

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

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

 Copyright © Huawei Technologies Co., Ltd.

By default, no blackhole MAC address entry is configured.

Format

mac-address blackhole *mac-address* **vsi** *vsi-name*

undo mac-address blackhole [*mac-address*] **vsi** *vsi-name*

Parameters

Parameter	Description	Value
mac-address	Specifies the MAC address in a blackhole MAC address entry.	The value is in H-H-H format. An H is a hexadecimal number of 1 to 4 digits. The MAC address cannot be FFFF-FFFF-FFFF or a multicast MAC address.
vsi *vsi-name*	Specifies the name of a VSI in a blackhole MAC address entry. The VSI must have been created.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

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

Precautions

- If you configure a blackhole MAC address entry when the MAC address table is full, the device processes the MAC address entry as follows:
  - If a dynamic MAC address entry with the same MAC address and VLAN ID or VSI name exists in the MAC address table, the blackhole MAC address entry replaces the dynamic MAC address entry.
  - If no dynamic MAC address entry with the same MAC address and VLAN ID or VSI name exists in the MAC address table, the blackhole MAC address entry cannot be added to the MAC address table.

 Copyright © Huawei Technologies Co., Ltd.

- You can run the **mac-address blackhole** command multiple times to configure multiple blackhole MAC address entries.

Example

Add a blackhole MAC address entry to the MAC address table in the VSI named **vsi1**. In the blackhole MAC address entry, the MAC address is 0004-0004-0004.

```
<Huawei> system-view
[Huawei] mac-address blackhole 0004-0004-0004 vsi vsi1
```

Related Topics

6.1.3 display mac-address

6.1.5 display mac-address blackhole

12.13.22 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* [**pe-vid** *pe-vid* [**ce-vid** { *ce-vid* | **any** }]]

undo mac-address static *mac-address interface-type interface-number* **vsi** *vsi-name* [**pe-vid** *pe-vid* [**ce-vid** { *ce-vid* | **any** }]]

undo mac-address static vsi *vsi-name* [*interface-type interface-number*]

Parameters

Parameter	Description	Value
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).

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
interface-type interface-number	Specifies the type and number of an interface. • *interface-type* specifies the interface type. • *interface-number* specifies the interface number.	The interface can be an Ethernet interface, an Ethernet sub-interface, a GE interface, or a GE 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.
pe-vid *pe-vid*	Specifies the outer VLAN tag of user packets.	The value is a decimal integer that ranges from 1 to 4094.
ce-vid *ce-vid*	Specifies the inner VLAN tag of user packets. When you specify **ce-vid** *ce-vid*, the corresponding interface must be a sub-interface. QinQ termination is configured on the sub-interface, and a VSI is bound to the sub-interface.	The value is a decimal integer that ranges from 1 to 4094.
any	Specifies that the inner VLAN tag can be of any value. If **any** is specified, the VLAN ID in the inner tag is ignored to reduce configurations and system resource consumption.	-

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.

 Copyright © Huawei Technologies Co., Ltd.

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 vsi** 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 or the LPU is hot swapped.

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 0011-2233-4455, 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 0011-2233-4455 gigabitethernet 0/0/1 vsi abc
```

GE 1/0/0.1 is configured with a dot1q termination sub-interface and accesses the VPLS. Configure a static MAC address entry on this sub-interface. When a frame that belongs to VLAN 10 and has the destination MAC address

 Copyright © Huawei Technologies Co., Ltd.

0011-2233-4455 is received, its tag is deleted and it 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 1/0/0.1
[Huawei-GigabitEthernet1/0/0.1] dot1q termination vid 10
[Huawei-GigabitEthernet1/0/0.1] l2 binding vsi abc
[Huawei-GigabitEthernet1/0/0.1] quit
[Huawei] mac-address static 0011-2233-4455 gigabitethernet 1/0/0.1 vsi abc pe-vid 10
```

Related Topics

6.1.3 display mac-address

12.13.23 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

 Copyright © Huawei Technologies Co., Ltd.

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 on the current VSI.

```
<Huawei> system-view
[Huawei] vsi company1
[Huawei-vsi-company1] mac-learning disable
```

Related Topics

12.13.24 mac-withdraw enable

12.13.24 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

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

 Copyright © Huawei Technologies Co., Ltd.

In this case, the local end is unaware of an AC 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 occurs and the VSI remains Up. This solves the preceding problem.

Precautions

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 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
```

Related Topics

12.13.19 interface-status-change mac-withdraw enable

12.13.25 mpls l2vpn default vlan

Function

The **mpls l2vpn default vlan** sets the default VLAN of an interface to VLAN 0.

The **undo mpls l2vpn default vlan** command deletes the default VLAN of an interface.

By default, no default VLAN is configured for an interface.

Format

mpls l2vpn default vlan

undo mpls l2vpn default vlan

Parameters

None

Views

GE interface view, Ethernet interface view, GE sub-interface view, Ethernet sub-interface view

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

When the following conditions are met, you can run the **mpls l2vpn default vlan** command to specify the default VLAN on an 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 the Ethernet interface or GE interface as the AC interface.

  In this scenario, the computer sends and receives only untagged packets. After the default VLAN is specified on the 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.

Example

Configure the default VLAN of primary interface.

```
<Huawei> system-view
[Huawei] interface gigabitethernet 0/0/1
[Huawei-GigabitEthernet0/0/1] mpls l2vpn default vlan
```

12.13.26 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.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
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.

- *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
```

Related Topics

12.11.9 display mpls l2vpn resource

12.13.27 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*

 Copyright © Huawei Technologies Co., Ltd.

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 VSI ID has been configured using the **vsi-id** *vsi-id* command.

Precautions

When configuring MTUs, note that the MTUs of the VSIs created for the same VPLS on different PEs must be the same.

Example

Set the MTU of the VSI named **company1** as 1600.

```
<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
```

12.13.28 oam-detecting enable

Function

The **oam-detecting enable** command enables the L2VPN OAM detection on the PSN tunnel.

The **undo oam-detecting enable** command disables the L2VPN OAM detection on the PSN tunnel.

By default, the L2VPN OAM detection on the PSN tunnel is disabled.

 Copyright © Huawei Technologies Co., Ltd.

Format

oam-detecting enable

undo oam-detecting enable

Parameters

None

Views

MPLS-L2VPN view

Default Level

2: Configuration level

Usage Guidelines

After the L2VPN OAM detection on the PSN tunnel is enabled, you can:

Detect and locate the MPLS network faults swiftly and efficiently.

Report and process the faults.

Enable the VSI to sense the Down state of the LSP and then the VSI deletes the MAC address.

Example

Enable the L2VPN OAM detection on the PSN tunnel.

```
<Huawei> system-view
[Huawei] mpls l2vpn
[Huawei-l2vpn] oam-detecting enable
```

12.13.29 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*]

undo peer *peer-address* [**negotiation-vc-id** *vc-id*]

 Copyright © Huawei Technologies Co., Ltd.

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 VSI ID of another local VSI, or be the same as another VSI ID specified by another local **negotiate-vc-id**. In other words, *vc-id* must be an unused one. *vc-id* is a decimal integer that ranges from 1 to 4294967295.

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 using the **vsi-id** *vsi-id* command.

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.

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.

 Copyright © Huawei Technologies Co., Ltd.

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
```

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
[Huawei-vsi-company1-ldp] undo peer 10.3.3.3 negotiation-vc-id 10
```

Related Topics

12.13.49 vsi-id

12.13.30 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.	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 VSI ID of another local VSI, or be the same as another VSI ID specified by another local **negotiate-vc-id**. In other words, *vc-id* must be an unused one. *vc-id* is a decimal integer that ranges from 1 to 4294967295.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
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
```

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

12.13.29 peer (VSI-LDP view)

12.13.31 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*] **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.	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 VSI ID of another local VSI, or be the same as another VSI ID specified by another local **negotiate-vc-id**. In other words, *vc-id* must be an unused one. *vc-id* is a decimal integer that ranges from 1 to 4294967295.
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.

 Copyright © Huawei Technologies Co., Ltd.

Views

VSI-LDP view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On the VPLS network, you can run the **peer static-upe** 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 101
[Huawei-vsi-company1-ldp] peer 3.3.3.3 static-npe trans 100 recv 100
```

Related Topics

12.13.29 peer (VSI-LDP view)

12.13.30 peer pw

12.13.32 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* **peer** *peer-address* [**negotiate-vc-id** *vc-id*]

 Copyright © Huawei Technologies Co., Ltd.

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 ms.
-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, in bytes. The default value is 100 bytes.
-t *timeout-value*	Specifies the timeout period of sending Echo Request packets.	The value is an integer that ranges from 0 to 65535, in milliseconds. The default value is 2000 ms.
-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 is an integer that 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.
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

 Copyright © Huawei Technologies Co., Ltd.

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.

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 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 12-170 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.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
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.

Related Topics

12.13.48 vsi
12.13.43 tracert vpls
12.13.33 ping vpls mac vsi

12.13.33 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_rapid* | **-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.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
-c *count*	Specifies the number of VPLS MAC Ping Request packets to be sent.	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 VPLS MAC Ping Request packet.	The value is an integer that 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 is an integer that 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 is an integer that ranges from 0 to 65535, in milliseconds. The default value is 2000 ms.
-exp *exp*	Specifies the priority.	The value is an integer that 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. ● 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 mode 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.
-h *ttl*	Specifies the TTL value of an Echo Request packet to be sent.	The value is an integer that ranges from 1 to 255. The default value is 30.

Copyright © Huawei Technologies Co., Ltd.

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_rapid*	Specifies the number of VPLS MAC Ping Request packets to be sent.	The value is an integer that ranges from 1 to 1000. The default value is 5.

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 00e0-5952-6f01 is reachable.

```
<Huawei> ping vpls mac 00e0-5952-6f01 vsi v123
Ping mac 00e0-5952-6f01 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 5.5.5.9 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
```

Related Topics

12.13.48 vsi

12.13.32 ping vpls

 Copyright © Huawei Technologies Co., Ltd.

12.13.34 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
```

 Copyright © Huawei Technologies Co., Ltd.

```
[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
```

Related Topics

12.13.30 peer pw

12.13.35 pwsignal

Function

The **pwsignal** command configures the signaling mode for a VSI.

By default, no signaling mode is configured for a VSI.

Format

pwsignal ldp

Parameters

Parameter	Description	Value
ldp	Uses the LDP signaling mode.	-

Views

VSI view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When configuring the Martini VPLS, you need to run the **pwsignal** command to configure a signaling mode for a VSI or displays the VSI-LDP view.

Precautions

If the member discovery mode of the VSI is static, the signaling mode must be LDP.

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.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> system-view
[Huawei] vsi company1 static
[Huawei-vsi-company1] pwsignal ldp
[Huawei-vsi-company1-ldp]
```

Related Topics

12.13.48 vsi

12.13.36 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
```

Related Topics

12.13.5 display traffic-statistics vsi

12.13.6 display traffic-statistics vsi peer

12.13.37 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.

 Copyright © Huawei Technologies Co., Ltd.

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.

Prerequisites

The following operations have been performed before this command is used:

Run the **traffic-statistics enable** command in the VSI-LDP view to enable statistics collection on public network traffic of all PWs.

Precautions

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
```

Related Topics

12.13.5 display traffic-statistics vsi

12.13.44 traffic-statistics enable (VSI-LDP view)

 Copyright © Huawei Technologies Co., Ltd.

12.13.38 reset traffic-statistics vsi name peer

Function

The **reset traffic-statistics vsi name peer** command clears public network traffic statistics on a specified PW of 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 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.	-
negotiation-vc-id *vc-id*	Specifies the VC 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 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.

Prerequisites

The following operations have been performed before this command is used:

Run the **traffic-statistics peer enable** command in the VSI-LDP view to enable statistics collection on public network traffic of specified PWs.

Precautions

After you run this command, statistics about the traffic on the corresponding VPLS PW are cleared.

 Copyright © Huawei Technologies Co., Ltd.

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
```

Related Topics

12.13.6 display traffic-statistics vsi peer

12.13.45 traffic-statistics peer enable

12.13.39 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
```

Related Topics

12.13.9 display vpls-ping statistics

12.13.33 ping vpls mac vsi

 Copyright © Huawei Technologies Co., Ltd.

12.13.40 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
```

Related Topics

12.13.10 display vpls-trace statistics

12.13.42 trace vpls mac vsi

12.13.41 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

 Copyright © Huawei Technologies Co., Ltd.

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.

Prerequisites

The VSI ID has been configured using the **vsi-id** *vsi-id* command.

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
```

Related Topics

12.13.48 vsi

12.13.35 pwsignal

12.13.49 vsi-id

12.13.42 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.

 Copyright © Huawei Technologies Co., Ltd.

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.

 Copyright © Huawei Technologies Co., Ltd.

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 mode 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 of 781d-ba56-355e.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> trace vpls mac 781d-ba56-355e vsi a2
 Traceroute to mac 781d-ba56-355e vsi a2, 30 hops max, press CTRL_C to break
 TTL  Num     Replier          Time     Type     Downstream              Hit
            LSR-ID          Out Interface
 ------------------------------------------------------------------------------
 0    1                              Ingress  10.1.1.2/[3]          N
            1.1.1.9         GigabitEthernet2/0/0
 1    1      192.168.1.1       8 ms     Egress                        Y
            3.3.3.9
Info: Succeed in tracing the destination address 781d-ba56-355e.
```

Table 12-171 Description of the **trace vpls mac** 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, 192.168.1.1/[3] indicates that the IP address of the next hop is 192.168.1.1 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.

Related Topics

12.13.33 ping vpls mac vsi

Copyright © Huawei Technologies Co., Ltd.

12.13.43 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* **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.
-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.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
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.
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.	-

Views

All views

Default Level

0: Visit level

Usage Guidelines

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.

Example

Perform the tracert operation on the VPLS link.

```
<Huawei> tracert vpls vsi a1 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 12-172 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.

Copyright © Huawei Technologies Co., Ltd.

Item	Description
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.

Related Topics

12.13.32 ping vpls

12.13.44 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

Copyright © Huawei Technologies Co., Ltd.

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** command in the VSI-LDP view.

Example

Enable the statistics on all PWs in the VSI 1.

```
<Huawei> system-view
[Huawei] vsi vsi1
[Huawei-vsi-vsi1] pwsignal ldp
[Huawei-vsi-vsi1-ldp] vsi-id 1
[Huawei-vsi-vsi1-ldp] traffic-statistics enable
```

Related Topics

12.13.45 traffic-statistics peer enable

12.13.37 reset traffic-statistics vsi name

12.13.5 display traffic-statistics vsi

12.13.45 traffic-statistics peer enable

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.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
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** 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** 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
```

Related Topics

12.13.44 traffic-statistics enable (VSI-LDP view)

12.13.38 reset traffic-statistics vsi name peer

12.13.6 display traffic-statistics vsi peer

 Copyright © Huawei Technologies Co., Ltd.

12.13.46 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.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> system-view
[Huawei] mpls l2vpn
[Huawei-l2vpn] vpls ignore-ac-state
```

12.13.47 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

On a dual-homing VPLS 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.

Example

Enable MAC withdraw loop detection.

```
<Huawei> system-view
[Huawei] mpls l2vpn
[Huawei-l2vpn] vpls mac-withdraw loop-detect enable
```

 Copyright © Huawei Technologies Co., Ltd.

12.13.48 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* [**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.
static	Indicates that the static member discovery mode is used in the VSI. You must specify this parameter when creating a VSI.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To configure VPLS, run the **vsi** *vsi-name* **static** command to create a VSI first. Each device in a VPLS domain needs to be configured with a VSI that belongs to the domain.

Prerequisites

MPLS L2VPN has been enabled by using the **mpls l2vpn** command.

Precautions

Copyright © Huawei Technologies Co., Ltd.

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.
- Multiple peers can be specified for a VSI on a PE.

If the specified VSI exists, you can use the **vsi** *vsi-name* [**static**] 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
```

Related Topics

12.13.11 display vsi
12.13.14 display vsi remote
12.13.49 vsi-id

12.13.49 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

 Copyright © Huawei Technologies Co., Ltd.

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 101.

```
<Huawei> system-view
[Huawei] vsi company1 static
[Huawei-vsi-company1] pwsignal ldp
[Huawei-vsi-company1-ldp] vsi-id 101
```

Related Topics

12.13.11 display vsi

12.13.14 display vsi remote

12.13.48 vsi

12.13.35 pwsignal

12.14 VXLAN Configuration Commands

NOTE

Only the AR100, AR120, AR150, AR160, AR200, AR1200 series, AR2220E, AR2240, and AR3260 support VXLAN. AR2220E, AR2240, and AR3260 need to run the **portswitch** command to change the working mode of all interfaces on the SRU200, SRU400, 4GECS, and 2X10GL from Layer 3 mode to Layer 2 mode. The interfaces that change the working mode to layer 2 only support VXLAN. Only the 8FE1GE, 24GE, and 24ES2GP ethernet LAN card support VXLAN.

12.14.1 arp static vni

Function

The **arp static vni** command configures a static ARP entry for a VXLAN tunnel.

The **undo arp static vni** command deletes the static ARP entry of a VXLAN tunnel.

By default, a static MAC address entry of a VXLAN tunnel is not configured.

 Copyright © Huawei Technologies Co., Ltd.

Format

arp static *ip-address mac-address* **vni** *vni-id* **source-ip** *source-ip-address* **peer-ip** *peer-ip-address*

undo arp static *ip-address mac-address* **vni** *vni-id* **source-ip** *source-ip-address* **peer-ip** *peer-ip-address*

Parameters

Parameter	Description	Value
ip-address	Specifies the destination IP address.	The value is in dotted decimal notation.
mac-address	Specifies the destination MAC address mapping the destination IP address.	The value is in H-H-H format. An H is a hexadecimal number of 1 to 4 digits.
vni *vni-id*	Specifies a VNI ID.	The value is an integer that ranges from 0 to 16777215.
source-ip *source-ip-address*	Specifies the IP address of the source VTEP.	The value is in dotted decimal notation.
peer-ip *peer-ip-address*	Specifies the IP address of the destination VTEP.	The value is in dotted decimal notation.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Static ARP entries are manually configured and maintained. They cannot be aged and overridden by dynamic ARP entries. Running the **arp static vni** command on a Layer 3 VXLAN gateway to configure static ARP entries increases communication security. Static ARP entries ensure communication between the local device and a specified device by using a specified MAC address so that attackers cannot modify mappings between IP addresses and MAC addresses in static ARP entries.

Prerequisites

A VXLAN tunnel and a Layer 3 gateway have been configured.

Precautions

The IP address specified by the *ip-address* command must be in the same network segment as the IP address of the outbound interface specified by the **interface** *interface-type interface-number* command.

 Copyright © Huawei Technologies Co., Ltd.

If a static ARP entry to be created exists, the system updates the entry.

Example

Configure a static ARP entry for the VXLAN tunnel with the IP address 10.2.2.10 and MAC address 0011-0022-0033.

```
<Huawei> system-view
[Huawei] bridge-domain 10
[Huawei-bd10] vxlan vni 1010
[Huawei-bd10] quit
[Huawei] interface vbdif 10
[Huawei-Vbdif10] ip address 10.2.2.2 255.255.255.0
[Huawei-Vbdif10] quit
[Huawei] interface nve 1
[Huawei-Nve1] source 1.1.1.1
[Huawei-Nve1] vni 1010 head-end peer-list 2.2.2.2
[Huawei-Nve1] quit
[Huawei] arp static 10.2.2.10 0011-0022-0033 vni 1010 source-ip 1.1.1.1 peer-ip 2.2.2.2
```

12.14.2 arp static vni interface

Function

The **arp static vni interface** command configures static ARP entries.

The **undo arp static vni interface** command deletes static ARP entries.

By default, no static ARP entry is configured.

Format

arp static *ip-address mac-address* **vni** *vni-id* [**vid** *vlan-id* [**cevid** *ce-vid*]] **interface** *interface-type interface-number*

undo arp static *ip-address mac-address* **vni** *vni-id* [**vid** *vlan-id* [**cevid** *ce-vid*]] **interface** *interface-type interface-number*

Parameters

Parameter	Description	Value
ip-address	Specifies the destination IP address.	The value is in dotted decimal notation.
mac-address	Specifies the destination MAC address mapping the destination IP address.	The value is in H-H-H format. An H is a hexadecimal number of 1 to 4 digits.
vni *vni-id*	Specifies a VNI ID.	The value is an integer that ranges from 0 to 16777215.
vid *vlan-id*	Specifies the ID of the VLAN to which a static ARP entry belongs.	The value is an integer that ranges from 1 to 4094.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
cevid *ce-vid*	Specifies the ID of the inner VLAN to which a static ARP entry belongs.	The value is an integer that ranges from 1 to 4094.
interface *interface-type interface-number*	Specifies the outbound interface of a static ARP packet. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number. Only Layer 2 Ethernet interface or Layer 2 sub-interface is supported.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Static ARP entries are manually configured and maintained. They cannot be aged and overridden by dynamic ARP entries. Running the **arp static vni interface** command on a VXLAN network to configure static ARP entries increases communication security. Static ARP entries ensure communication between the local device and a specified device by using a specified MAC address so that attackers cannot modify mappings between IP addresses and MAC addresses in static ARP entries.

Prerequisites

An access-side VXLAN deployment mode and a Layer 3 gateway have been configured.

Precautions

The IP address specified by the *ip-address* command must be in the same network segment as the IP address of the outbound interface specified by the **interface** *interface-type interface-number* command.

If a static ARP entry to be created exists, the system updates the entry.

- On a Layer 2 Ethernet interface, run the **arp static** *ip-address mac-address* **vni** *vni-id* **vid** *vlan-id* **interface** *interface-type interface-number* command to configure static ARP entries.
- On a Layer 2 sub-interface:

 Copyright © Huawei Technologies Co., Ltd.

- If the traffic encapsulation type is **dot1q**, run the **arp static** *ip-address mac-address* **vni** *vni-id* **vid** *vlan-id* **interface** *interface-type interface-number* command to configure static ARP entries. The value of **vid** *vlan-id* in this command must be the same as that in the **encapsulation dot1q vid** *pe-vid* command.
- If the traffic encapsulation type is **qinq**, run the **arp static** *ip-address mac-address* **vni** *vni-id* **vid** *vlan-id* **cevid** *ce-vid* **interface** *interface-type interface-number* command to configure static ARP entries. The values of **vid** *vlan-id* and **cevid** *ce-vid* in this command must be the same as the values in the **encapsulation qinq vid** *vlan-vid* **ce-vid** *ce-vid* command.
- If the traffic encapsulation type is **untag**, run the **arp static** *ip-address mac-address* **vni** *vni-id* **interface** *interface-type interface-number* command to configure static ARP entries.

Example

Configure a static ARP entry with IP address 10.3.3.10, MAC address 0031-0032-0033, VLAN ID 300, and outbound interface GE0/0/3.

```
<Huawei> system-view
[Huawei] vlan 300
[Huawei-vlan300] quit
[Huawei] bridge-domain 30
[Huawei-bd30] vxlan vni 3010
[Huawei-bd30] l2 binding vlan 300
[Huawei-bd30] quit
[Huawei] interface gigabitethernet 0/0/3
[Huawei-GigabitEthernet0/0/3] port link-type access
[Huawei-GigabitEthernet0/0/3] port default vlan 300
[Huawei-GigabitEthernet0/0/3] quit
[Huawei] interface vbdif 30
[Huawei-Vbdif30] ip address 10.3.3.2 255.255.255.0
[Huawei-Vbdif30] quit
[Huawei] arp static 10.3.3.10 0031-0032-0033 vni 3010 vid 300 interface gigabitethernet 0/0/3
```

Configure a static ARP entry with IP address 10.1.1.10, MAC address 0011-0012-0013, VLAN ID 100, and outbound interface GE0/0/1.1.

```
<Huawei> system-view
[Huawei] bridge-domain 20
[Huawei-bd20] vxlan vni 2010
[Huawei-bd20] quit
[Huawei] interface gigabitethernet 0/0/1.1 mode l2
[Huawei-GigabitEthernet0/0/1.1] encapsulation dot1q vid 100
[Huawei-GigabitEthernet0/0/1.1] bridge-domain 20
[Huawei-GigabitEthernet0/0/1.1] quit
[Huawei] interface vbdif 20
[Huawei-Vbdif20] ip address 10.1.1.2 255.255.255.0
[Huawei-Vbdif20] quit
[Huawei] arp static 10.1.1.10 0011-0012-0013 vni 2010 vid 100 interface gigabitethernet 0/0/1.1
```

12.14.3 bridge-domain (Layer 2 sub-interface view)

Function

The **bridge-domain** command associates a Layer 2 sub-interface with a BD.

The **undo bridge-domain** command restores the default settings.

By default, no Layer 2 sub-interface is associated with a BD.

 Copyright © Huawei Technologies Co., Ltd.

Format

bridge-domain *bd-id*

undo bridge-domain [*bd-id*]

Parameters

Parameter	Description	Value
bd-id	Specifies the ID of the BD that is associated with a Layer 2 sub-interface.	The BD ID must exist.

Views

Layer 2 sub-interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

VXLAN needs to be deployed on a downlink interface to provide access services and an uplink interface to establish a VXLAN tunnel.

On the access side, two methods are available for creating a large Layer 2 BD.

- Based on VLAN: You can associate one or multiple VLANs with a BD to add users in these VLANs to the BD. This VLAN-based mode implements larger-granularity control, but is easy to configure. It applies to VXLAN deployment on a live network.
- Based on encapsulation mode: The device sends packets of different encapsulation modes to different Layer 2 sub-interfaces based on the VLAN tags contained in the packets. You can bind a Layer 2 sub-interface to a BD to add specified users to the BD. This mode implements refined and flexible control but requires more complex configuration. It applies to VXLAN deployment on a new network.

To create a BD based on encapsulation mode, create a Layer 2 sub-interface first. Then run the **encapsulation (Layer 2 sub-interface view)** command to configure a supported encapsulation mode on the sub-interface. After you run the **bridge-domain (Layer 2 sub-interface view)** command to associate a Layer 2 sub-interface with a BD, packets containing the same VLAN tag from different LANs can communicate at Layer 2.

Prerequisites

A BD has been created using the **12.14.4 bridge-domain (system view)** command in the system view.

Precautions

One Layer 2 sub-interface can be associated with only one BD.

 Copyright © Huawei Technologies Co., Ltd.

For the BD that bind to the Layer 2 sub-interfaces which use **dot1q** encapsulation, the VBDIF interface of this BD cannot be created on the device.

Example

Associate Layer 2 sub-interface Eth2/0/0.1 with BD 10.

```
<Huawei> system-view
[Huawei] bridge-domain 10
[Huawei-bd10] quit
[Huawei] interface ethernet 2/0/0.1 mode l2
[Huawei-Ethernet2/0/0.1] bridge-domain 10
```

12.14.4 bridge-domain (system view)

Function

The **bridge-domain** command creates a bridge domain (BD) and displays the BD view, or directly displays the view of an existing BD view.

The **undo bridge-domain** command deletes a BD.

By default, no BD is created.

Format

bridge-domain *bd-id*

undo bridge-domain *bd-id*

Parameters

Parameter	Description	Value
bd-id	Specifies the ID of a BD.	The value is an integer. The value ranges are as follows: • AR100&AR120&AR150&AR160&AR200 series: 1-64 • AR1200 series: 1-128 • AR2220E: 1-256

Views

System view

Default Level

2: Configuration level

Usage Guidelines

BDs are Layer 2 bridge domains on a large Layer 2 network constructed using VXLAN. VXLAN packets can be forwarded at Layer 2 within a BD through a VXLAN tunnel.

 Copyright © Huawei Technologies Co., Ltd.

After you run the **bridge-domain** command to create a BD, you can complete other VXLAN configurations in the BD.

Example

Create BD 10 and enter the view of BD 10.

```
<Huawei> system-view
[Huawei] bridge-domain 10
[Huawei-bd10]
```

12.14.5 description (BD view)

Function

The **description** command configures the description of a bridge domain (BD).

The **undo description** command deletes the description of a BD.

By default, no description is configured for a BD.

Format

description *description*

undo description

Parameters

Parameter	Description	Value
description	Specifies the BD description.	The value is a string of 1 to 80 case-sensitive characters without spaces.

Views

BD view

Default Level

2: Configuration level

Usage Guidelines

If you have configured multiple BDs using the **bridge-domain (system view)** command, run the **description** command in the corresponding BD view to configure the description for each BD. BD description helps you quickly understand the function of each BD, facilitating service management.

Example

Configure description **vxlan** for BD 10.

```
<Huawei> system-view
[Huawei] bridge-domain 10
[Huawei-bd10] description vxlan
```

 Copyright © Huawei Technologies Co., Ltd.

12.14.6 display bridge-domain

Function

The **display bridge-domain** command displays the BD configuration.

Format

display bridge-domain [*bd-id* [**brief** | **verbose**]]

Parameters

Parameter	Description	Value
bd-id	Displays the configuration of a specified BD. If this parameter is not specified, the device displays the configuration of all BDs.	The BD ID must exist.
brief	Displays brief BD configuration.	-
verbose	Displays detailed BD configuration.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After BDs are created on a device, you can run the **display bridge-domain** command to view the configuration of a specified BD or all BDs.

Example

Display the configuration of all BDs.

```
<Huawei> display bridge-domain
--------------------------------------------------------------------------------

BDID    State     Description
--------------------------------------------------------------------------------
10      down      vxlan
20      up        vxlan
--------------------------------------------------------------------------------
The total number of bridge-domains is : 2
```

Display the detailed configuration of BD 10.

```
<Huawei> display bridge-domain 10 verbose
Bridge-domain ID   :10
Description        :vxlan
State              :Down
```

 Copyright © Huawei Technologies Co., Ltd.

```
--------------------------------------------------------------------------------

Interface                         State
--------------------------------------------------------------------------------
Ethernet2/0/0.1                     down
--------------------------------------------------------------------------------
VLAN                              State
--------------------------------------------------------------------------------
2                                 down
3                                 down
10                                 down
--------------------------------------------------------------------------------
```

Table 12-173 Description of the **display bridge-domain** command output

Item	Description
BDID/Bridge-domain ID	ID of a BD. To set the BD ID, run the **12.14.4 bridge-domain (system view)** command in the system view.
State	BD status: • up: The BD is bound to a Layer 2 sub-interface, VLAN, or VNI, and at least one of the bound Layer 2 sub-interface, VLAN, and VNI is Up. • down: The BD is not bound to a Layer 2 sub-interface, VLAN, or VNI; alternatively, the BD is bound to a Layer 2 sub-interface, VLAN, or VNI and the bound Layer 2 sub-interface, VLAN, and VNI are Down.
Description	BD description. To configure the description of a BD, run the **description (BD view)** command.
The total number of bridge-domains is	Total number of BDs on the device.
Interface State	Member interface in a BD and its status. • up: The link layer protocol of the interface is in the Up state. • down: The link layer protocol of the interface is Down.
VLAN State	Status of the VLAN associated with the BD. • up • down The status of a VLAN is determined by the status of member interfaces in the VLAN. A VLAN is Up only when at least one member interface in the VLAN is Up.

Copyright © Huawei Technologies Co., Ltd.

12.14.7 display interface nve

Function

The **display interface nve** command displays NVE interface information.

Format

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

Parameters

Parameter	Description	Value
nve-number	Specifies the number of an NVE interface. If *nve-number* is not specified, information about all NVE interfaces is displayed.	The value is 1.
main	Displays the running status and statistics of the main interface.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

To monitor the NVE interface status or locate an NVE interface fault on the VXLAN network, run the **display interface nve** command to check the running status and statistics of the NVE interface.

Example

Display the running status of the NVE interface.

```
<Huawei> display interface nve 1
Nve1 current state : UP
Line protocol current state : UP
Description:HUAWEI, AR Series, Nve1 Interface
Route Port,The Maximum Transmit Unit is 1500
Current system time: 2016-09-21 17:05:06
```

 Copyright © Huawei Technologies Co., Ltd.

Table 12-174 Description of the **display interface nve** command output

Item	Description
Nve1 current state	Indicates the physical status of the NVE interface. The physical status of the successfully created NVE interface is always Up.
Line protocol current state	Link layer protocol status of the NVE interface. The link layer protocol status of the successfully created NVE interface is always Up.
Description	Description of the NVE interface.
Current system time	System time. If a time zone is configured and the daylight saving time is used, the time is displayed in the format of YYYY/MM/DD HH:MM:SS UTC ±HH:MM DST.

12.14.8 display mac-address bridge-domain

Function

The **display mac-address bridge-domain** command displays MAC address entries of a BD.

Format

display mac-address [*mac-address*] **bridge-domain** *bd-id*

Parameters

Parameter	Description	Value
mac-address	Specifies the MAC address.	The value is in H-H-H format. An H is a hexadecimal number of 4 digits, such as 00e0 and fc01. The MAC address cannot be the broadcast MAC address (FFFF-FFFF-FFFF), multicast MAC address (the eighth bit is 1), or MAC address of all 0s.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
bd-id	Displays MAC address entries of a specified BD.	The value is an integer. The value ranges are as follows: • AR100&AR120&AR150&AR160&AR200 series: 1-64 • AR1200 series: 1-128 • AR2220E: 1-256

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The MAC address table needs to be updated constantly because the network topology always changes. To learn about MAC address entries of a BD in a timely manner, run the **display mac-address bridge-domain** command.

NOTE

The device supports only query of MAC address entries based on a BD.

Example

Display all MAC address entries of BD 10.

```
<Huawei> display mac-address bridge-domain 10
MAC_Address    VLAN/Bridge/VSI/BD        Learned-From            Type
0003-0002-0003 -/-/-/10                  Ethernet0/0/1.1         static
Total items: 1
```

Display the MAC address entry with the MAC address of 0004-0003-0004 in BD 20.

```
<Huawei> display mac-address 0004-0003-0004 bridge-domain 20
MAC_Address    VLAN/Bridge/VSI/BD        Learned-From            Type
0004-0003-0004 -/-/-/20                  2.2.2.2                 static
Total items: 1
```

Table 12-175 Description of the **display mac-address bridge-domain** command output

Item	Description
MAC_Address	Destination MAC address.

Copyright © Huawei Technologies Co., Ltd.

Item	Description
VLAN/ Bridge/VSI/BD	• VLAN: VLAN associated with the interface • Bridge: bridge that the interface belongs to • VSI: VSI associated with the interface • BD: BD associated with the interface **NOTE** BD information is displayed only on the VXLAN-enabled device.
Learned-From	• LAN side: Layer 2 sub-interface that joins a BD • VXLAN side: IP address of the remote VTEP
Type	Type of a MAC address: • **static**: indicates the static MAC address entry. A static MAC address entry is manually configured and will not be aged out. • **dynamic**: indicates the MAC address entry learned by the device based on the source MAC address. Dynamic MAC address entries have the aging time and can be aged.
Total items	Total number of MAC address entries that match the filtering condition.

Related Topics

12.14.19 mac-address static bridge-domain

12.14.9 display vxlan encapsulation

Function

The **display vxlan encapsulation** command displays VXLAN encapsulation information about Layer 2 sub-interfaces of a main interface.

Format

display vxlan encapsulation interface *interface-type interface-number* [**bridge-domain** *bd-id* | **default** | **dot1q** [**vid** *pe-vid*] | **qinq** [**vid** *vlan-vid* [**ce-vid** *ce-vid*]] | **untag**]

Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Displays VXLAN encapsulation information about a specified Layer 2 sub-interface. • *interface-type* specifies the interface type. • *interface-number* specifies the interface number.	-
bridge-domain *bd-id*	Displays VXLAN encapsulation information about Layer 2 sub-interfaces by BD ID.	The BD ID must exist.
default	Displays VXLAN encapsulation information about Layer 2 sub-interfaces for the flow encapsulation mode **default**.	-
dot1q	Displays VXLAN encapsulation information about Layer 2 sub-interfaces for the flow encapsulation mode **Dot1q**.	-
vid *pe-vid*	Displays VXLAN encapsulation information about Layer 2 sub-interfaces by VLAN ID in packets with the flow encapsulation mode **Dot1q**.	The VLAN ID must exist.
qinq	Displays VXLAN encapsulation information about Layer 2 sub-interfaces for the flow encapsulation mode **QinQ**.	-
vid *vlan-vid* [**ce-vid** *ce-vid*]	Displays VXLAN encapsulation information about Layer 2 sub-interfaces by VLAN ID in packets with the flow encapsulation mode **QinQ**. • *vlan-vid* specifies the outer VLAN ID. • *ce-vid* specifies the inner VLAN ID.	The VLAN ID must exist.
untag	Displays VXLAN encapsulation information about Layer 2 sub-interfaces for the flow encapsulation mode **untag**.	-

Views

All views

Default Level

1: Monitoring level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

You can run the **display vxlan encapsulation** command to view VXLAN encapsulation information about Layer 2 sub-interfaces of a main interface as well as the bindings between the sub-interface and BD.

Example

Display VXLAN encapsulation information about Layer 2 sub-interfaces of a main interface.

```
<Huawei> display vxlan encapsulation interface ethernet 1/0/1
-------------------------------------------------------------------------------
Interface              EncapType       PeVid      CeVid      BD-ID
-------------------------------------------------------------------------------
Ethernet1/0/1.1        QinQ            4093       4093       16000
-------------------------------------------------------------------------------
Total number to display is 1.
```

Table 12-176 Description of the **display vxlan encapsulation** command output

Item	Description
Interface	Name of the Layer 2 sub-interface.
EncapType	Flow encapsulation type of the Layer 2 sub-interface. • QinQ • Dot1q • Default • Untag To configure the flow encapsulation type, run the **12.14.13 encapsulation (Layer 2 sub-interface view)** command.
PeVid	VLAN ID of packets with the flow encapsulation type **Dot1q** or outer VLAN ID of packets with the flow encapsulation type **QinQ**. To configure the VLAN ID, run the **12.14.13 encapsulation (Layer 2 sub-interface view)** command.
CeVid	Inner VLAN ID of packets with the flow encapsulation type **QinQ**. To configure the VLAN ID, run the **12.14.13 encapsulation (Layer 2 sub-interface view)** command.
BD-ID	BD. To configure the BD, run the **12.14.3 bridge-domain (Layer 2 sub-interface view)** command.
Total number to display is	Total number of encapsulation data records about Layer 2 sub-interfaces of a main interface.

Copyright © Huawei Technologies Co., Ltd.

12.14.10 display vxlan peer

Function

The **display vxlan peer** command displays the IP address of the destination virtual tunnel end point (VTEP) of a Virtual Network Identifier (VNI).

Format

display vxlan peer [**vni** *vni-id*]

Parameters

Parameter	Description	Value
vni *vni-id*	Displays the IP address of the destination VTEP of a specified VNI.	The VNI ID must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

After completing VXLAN configuration, you can run the **display vxlan peer** command to view information about the source and destination IP address bound to the VNI.

Precautions

Before running the **display vxlan peer** command, ensure that the device has been configured with VNIs. Otherwise, the command output is meaningless.

Example

Display the IP address of the destination VTEP of a specified VNI.

```
<Huawei> display vxlan peer
 Vni ID      Source            Destination       Type
--------------------------------------------------------------
 10          10.1.1.2          10.1.1.3          static
 10          10.1.1.2          10.1.1.4          static
--------------------------------------------------------------
Number of peers :
Total: 2   Static: 2   L3 dynamic: 0
```

 Copyright © Huawei Technologies Co., Ltd.

Table 12-177 Description of the **display vxlan peer** command output

Item	Description
Vni ID	ID of a VNI. To configure or modify a VNI ID, run the **12.14.23 vxlan vni (BD view)** command.
Source	IP address of the source VTEP. To configure or modify the IP address of the source VTEP, run the **12.14.21 source (NVE interface view)** command.
Destination	IP address of the destination VTEP. To configure or modify the IP address of the destination VTEP, run the **vni head-end peer-list** command.
Type	IP address configuration mode of the destination VTEP: • static: The IP address is manually configured. • l3 dynamic: Layer 3 VXLAN tunnel IP addresses are dynamically generated through the BGP protocol. To configure the IP address configuration mode, run the **vni head-end peer-list** command.
Number of peers	Number of IP addresses of destination VTEPs on the device: • Total: indicates the number of IP addresses of destination VTEPs. • Static: indicates the number of IP addresses of static destination VTEPs. • L3 dynamic: indicates the number of IP addresses of Layer 3 dynamic destination VTEPs.

12.14.11 display vxlan tunnel

Function

The **display vxlan tunnel** command displays information about VXLAN tunnels.

Format

display vxlan tunnel [*tunnel-id*] [**verbose**]

Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
tunnel-id	Displays information about the VXLAN tunnel with a specified ID. If this parameter is not specified, the device displays information about all VXLAN tunnels.	The value is an integer that ranges from 1 to 4294967295.
verbose	Displays detailed VXLAN tunnel information.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After VXLAN tunnels are established, you can run the **display vxlan tunnel** command to view VXLAN tunnel information.

Example

Display VXLAN tunnel information.

```
<Huawei> display vxlan tunnel
 Tunnel ID       Source            Destination       State     Type
 --------------------------------------------------------------------------------
 4026531841      10.1.1.2          10.1.1.4          up        static
 4026531842      10.1.1.1          10.1.1.3          up        l3 dynamic
 --------------------------------------------------------------------------------
 Number of vxlan tunnel :
 Total: 2   Static: 1   L3 dynamic: 1
```

Display detailed VXLAN tunnel information.

```
<Huawei> display vxlan tunnel verbose
 Tunnel ID       : 4026531841
 Source          : 10.1.1.2
 Destination     : 10.1.1.4
 State           : up
 Type            : static

 Tunnel ID       : 4026531842
 Source          : 10.1.1.1
 Destination     : 10.1.1.3
 State           : up
 Type            : l3 dynamic
 --------------------------------------------------------------------------------
 Number of vxlan tunnel :
 Total: 2   Static: 1   L3 dynamic: 1
```

 Copyright © Huawei Technologies Co., Ltd.

Table 12-178 Description of the **display vxlan tunnel** command output

Item	Description
Tunnel ID	ID of a VXLAN tunnel. After a VXLAN tunnel is established, the ID is automatically generated by the device.
Source	Source IP address of the VXLAN tunnel. To configure the source IP address, run the **source (NVE interface view)** command.
Destination	Destination IP address of the VXLAN tunnel.
State	Status of the VXLAN dynamic tunnel: • up: The VXLAN tunnel is reachable. • down: The VXLAN tunnel is unreachable. Status of the VXLAN static tunnel: • up: The destination route exists. • down: The destination route not exists.
Type	Status of the VXLAN tunnel, which is determined by the **peer-list** parameter in the **vni head-end peer-list** command. • static: The peer list is configured manually. • l3 dynamic: The peer list is learned by a dynamic routing protocol.
Number of vxlan tunnel	Total number of VXLAN tunnels on the device. • Total: indicates the number of VXLAN tunnels. • Static: indicates the number of static VXLAN tunnels. • L3 dynamic: indicates the number of Layer 3 dynamic VXLAN tunnels.

12.14.12 display vxlan vni

Function

The **display vxlan vni** command displays the VXLAN configuration of a specified VNI or all VNIs.

Format

display vxlan vni [*vni-id* [**verbose**]]

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
vni-id	Displays VXLAN information about a specified VNI. If this parameter is not specified, the device displays VXLAN configuration of all VNIs.	The VNI ID must exist.
verbose	Displays detailed VXLAN information about a specified VNI.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Applications

After VXLAN is configured, you can run the **display vxlan vni** command to view information about BDs associated with VNIs, VPN instances bound to the VNIs, and VNI status.

Precautions

Before running the **display vxlan vni** command, ensure that the device has been configured with VNIs. Otherwise, the command output is meaningless.

Example

Display VXLAN information about all VNIs.

```
<Huawei> display vxlan vni
 VNI             BD-ID           State
 ----------------------------------------
 10              10              up
 50              50              up
 ----------------------------------------
 Number of vxlan vni bound to BD is : 2

 VNI             VRF-ID
 ----------------------------------------
 20              5
 ----------------------------------------
 Number of vxlan vni bound to VPN is : 1
```

Display detailed VXLAN information about VNI 10.

```
<Huawei> display vxlan vni 10 verbose
 BD ID             :10
 State             :up
 Source            :10.1.1.2
```

 Copyright © Huawei Technologies Co., Ltd.

```
UDP Port          :4789
Peer List         :10.1.1.1 10.1.1.3
```

Display detailed VXLAN information about VNI 20.

```
<Huawei> display vxlan vni 20 verbose
 VRF-ID           :5
```

Table 12-179 Description of the **display vxlan vni** command output

Item	Description
VNI	ID of a VNI. To configure or modify a VNI ID, run the **vxlan vni** command.
BD-ID (BD ID)	ID of the BD associated with a VNI. To configure or modify a BD ID, run the **bridge-domain (system view)** command.
State	VNI status: • up • down To ensure that the VNI status is up, the corresponding VXLAN tunnel must exist and be up for the VNI. If the VNI status is down, check whether **Source** and **Peer List** in this command output are the same as **Source** and **Destination** in the output of the **display vxlan tunnel** command. • If they are different, no VXLAN tunnel exists for the specified VNI. Run the **source (NVE interface view)** or **vni head-end peer-list** command to change the source or destination IP address of the VXLAN tunnel to ensure that the corresponding VXLAN tunnel exists for the VNI. • If they are the same, collect related configuration and contact technical support personnel.
VRF-ID	VPN instance ID.
Number of vxlan vni bound to VPN is	Number of existing VNIs bound to VPN instances.
Source	IP address of the source VTEP. To configure the IP address of the source VTEP, run the **source (NVE interface view)** command.
Source IPv6 Address	IPv6 address of the source VTEP. To configure the IP address of the source VTEP, run the **source (NVE interface view)** command.
UDP Port	Destination UDP port. The port number is fixed as 4789.

Copyright © Huawei Technologies Co., Ltd.

Item	Description
Peer List	IP address of the destination VTEP. To configure the IP address of the destination VTEP, run the **vni head-end peer-list** command.
IPv6 Peer List	IPv6 address of the destination VTEP. To configure the IP address of the destination VTEP, run the **vni head-end peer-list** command.

12.14.13 encapsulation (Layer 2 sub-interface view)

Function

The **encapsulation** command configures the encapsulation mode of packets allowed to pass a Layer 2 sub-interface.

The **undo encapsulation** command deletes the encapsulation mode of packets allowed to pass a Layer 2 sub-interface.

By default, the encapsulation mode of packets allowed to pass a Layer 2 sub-interface is not configured.

Format

encapsulation { **dot1q vid** *pe-vid* | **default** | **untag** | **qinq vid** *vlan-vid* **ce-vid** *ce-vid* }

undo encapsulation { **dot1q vid** *pe-vid* | **default** | **untag** | **qinq vid** *vlan-vid* **ce-vid** *ce-vid* }

Parameters

Parameter	Description	Value
dot1q	Sets encapsulation mode of packets allowed to pass a Layer 2 sub-interface to Dot1q. This mode enables a Layer 2 sub-interface to receive packets with a VLAN tag.	-
vid *pe-vid*	Specifies the outer VLAN ID in packets allowed to pass a Layer 2 sub-interface in Dot1q encapsulation mode.	The value is an integer that ranges from 2 to 4094.
default	Sets the encapsulation mode of packets allowed to pass a Layer 2 sub-interface to default. This mode enables a Layer 2 sub-interface to receive all packets, regardless of whether they contain VLAN tags.	-

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
untag	Sets the encapsulation mode of packets allowed to pass a Layer 2 sub-interface to untag. This mode enables a Layer 2 sub-interface to receive packets without VLAN tags.	-
qinq	Sets encapsulation mode of packets allowed to pass a Layer 2 sub-interface to QinQ. This mode enables a Layer 2 sub-interface to receive packets with double VLAN tags.	-
vid *vlan-vid*	Specifies the outer VLAN ID in double-tagged packets allowed to pass a Layer 2 sub-interface in QinQ encapsulation mode.	The value is an integer that ranges from 2 to 4094.
ce-vid *ce-vid*	Specifies the inner VLAN ID in double-tagged packets allowed to pass a Layer 2 sub-interface in QinQ encapsulation mode.	The value is an integer that ranges from 1 to 4094.

Views

Layer 2 sub-interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On a VXLAN network, a Layer 2 sub-interface functions as a VXLAN service access point to forward data packets in a BD.

Packets passing through a physical interface may contain one or two VLAN tags or no VLAN tag. After you run the **encapsulation** command in a Layer 2 sub-interface view to configure the encapsulation mode, the sub-interface can forward only specified types of packets.

Precautions

When configuring an encapsulation mode on a Layer 2 sub-interface, pay attention to the following points:

- The VLAN ID in **dot1q** mode or outer VLAN ID in **qinq** mode cannot be the same as the allowed VLAN of the corresponding main interface or the global VLAN.
- On the same main interface, the VLAN ID in **dot1q** mode and the outer VLAN ID in **qinq** mode must be different.
- After NAC authentication is configured on the main interface, the traffic encapsulation type on a Layer 2 sub-interface cannot be set to **default**.

 Copyright © Huawei Technologies Co., Ltd.

- When the encapsulation mode of a Layer 2 sub-interface is **default**, the corresponding main interface cannot be added to any VLAN, including VLAN 1.
- Before the encapsulation mode of a Layer 2 sub-interface is set to **default**, the main interface has only one sub-interface.
- After the encapsulation mode of a Layer 2 sub-interface is set to **default**, no other sub-interface can be created on the main interface.
- When the encapsulation mode of a Layer 2 sub-interface is set to **untag**, other sub-interfaces of the main interface cannot be set to **untag**.
- You can configure only one encapsulation mode for each Layer 2 sub-interface. If an encapsulation mode has been configured for a Layer 2 sub-interface, run the **undo encapsulation** command to delete the original mode before you configure another mode.
- When the device functions as a Layer 3 VXLAN gateway, the traffic encapsulation type on a Layer 2 sub-interface cannot be set to **default**.

Example

Set the encapsulation mode of packets allowed to pass Layer 2 sub-interface Eth2/0/0.1 to Dot1q and the outer VLAN ID in the packets to 10.

```
<Huawei> system-view
[Huawei] interface ethernet 2/0/0.1 mode l2
[Huawei-Ethernet2/0/0.1] encapsulation dot1q vid 10
```

Related Topics

12.14.9 display vxlan encapsulation

12.14.14 interface mode l2

Function

The **interface mode l2** command creates a Layer 2 sub-interface and displays the Layer 2 sub-interface view.

The **undo interface** command deletes the created Layer 2 sub-interface.

By default, no Layer 2 sub-interface is created.

NOTE

Only 8FE1GE, 24GE, and 24ES2GP ethernet LAN card support this function.

Format

interface *interface-type interface-number.subinterface-number* **mode l2**

undo interface *interface-type interface-number.subinterface-number*

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
interface-type interface-number.subinterface-number	Specifies the type and number of a Layer 2 sub-interface.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On a VXLAN network, you need to configure VXLAN service access points on a VXLAN network edge node. On the device, VXLAN service access points can be configured through a Layer 2 sub-interface or binding between VLANs and bridge domains (BDs).

When VXLAN service access points are configured through a Layer 2 sub-interface, the **interface mode l2** command needs to be used to configure the Layer 2 sub-interface first. After the Layer 2 sub-interface is created, you can run the **bridge-domain** *bd-id* command to add the Layer 2 sub-interface to a BD so that service packets are forwarded in the BD.

Precautions

The Layer 2 sub-interface can only join a BD but cannot directly connect to a Layer 3 network. Each Layer 2 sub-interface belongs to only one BD.

After the **interface mode l2** command is used to create a Layer 2 sub-interface, you can run the **interface** *interface-type interface-number.subinterface-number* **mode l2** or **interface** *interface-type interface-number.subinterface-number* command to enter the Layer 2 sub-interface view.

Example

Create Eth0/0/1.1.

```
<Huawei> system-view
[Huawei] interface ethernet 0/0/1.1 mode l2
```

12.14.15 interface nve

Function

The **interface nve** command creates a Network Virtualization Edge (NVE) interface and displays the NVE interface view.

The **undo interface nve** command deletes a specified NVE interface.

By default, no NVE interface is created.

 Copyright © Huawei Technologies Co., Ltd.

Format

interface nve *nve-number*

undo interface nve *nve-number*

Parameters

Parameter	Description	Value
nve-number	Specifies the number of an NVE interface.	The value is 1.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To make full use of advantages of server virtualization, you can deploy Virtual eXtensible Local Area Network (VXLAN) to connect to multiple tenants. VXLAN tunnel information needs to be configured on an NVE interface, so the **interface nve** command needs to be executed to create the NVE interface.

Precautions

After a VXLAN tunnel is configured, running the **undo interface nve** command will delete the specified NVE interface and all the configuration of the NVE interface.

Example

Create an NVE interface.

```
<Huawei> system-view
[Huawei] interface nve 1
```

12.14.16 interface vbdif

Function

The **interface vbdif** command creates a VBDIF interface and displays the VBDIF interface view.

The **undo interface vbdif** command deletes a VBDIF interface.

By default, no VBDIF interface is created.

 Copyright © Huawei Technologies Co., Ltd.

Format

interface vbdif *bd-id*

undo interface vbdif *bd-id*

Parameters

Parameter	Description	Value
bd-id	Specifies a BD ID.	The value is an integer. The value ranges are as follows: • AR100&AR120&AR150&AR160&AR200 series: 1-64 • AR1200 series: 1-128 • AR2220E: 1-256

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

IP routes are required for communication between VXLANs on different network segments and between VXLANs and non-VXLANs.

To allow communication between these networks, run the **vxlan vni** command to map VXLAN Network Identifiers (VNIs) to BDs in 1:1 mode, run the **interface vbdif** command to create a VBDIF interface for the BD, and configure an IP address for the BD. As a VBDIF interface is a Layer 3 logical interface similar to a VLANIF interface, it can have an IP address configured.

Prerequisites

A BD has been created by running the **bridge-domain** command.

Follow-up Procedure

Run the **ip address** command to configure an IP address for the VBDIF interface.

Example

Create VBDIF10.

```
<Huawei> system-view
[Huawei] bridge-domain 10
[Huawei-bd10] quit
[Huawei] interface vbdif 10
```

 Copyright © Huawei Technologies Co., Ltd.

12.14.17 l2 binding vlan

Function

The **l2 binding vlan** command associates a specified VLAN with a BD.

The **undo l2 binding vlan** command restores the default settings.

By default, a VLAN is associated with no BD.

Format

l2 binding vlan *vlan-id*

undo l2 binding vlan *vlan-id*

Parameters

Parameter	Description	Value
vlan-id	Specifies a VLAN ID.	The value is an integer that ranges from 1 to 4094.

Views

BD view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

VXLAN needs to be deployed on a downlink interface to provide access services and an uplink interface to establish a VXLAN tunnel.

On the access side, two methods are available for creating a large Layer 2 BD.

- Based on VLAN: You can associate one or multiple VLANs with a BD to add users in these VLANs to the BD. This VLAN-based mode implements larger-granularity control, but is easy to configure. It applies to VXLAN deployment on a live network.
- Based on encapsulation mode: The device sends packets of different encapsulation modes to different Layer 2 sub-interfaces based on the VLAN tags contained in the packets. You can bind a Layer 2 sub-interface to a BD to add specified users to the BD. This mode implements refined and flexible control but requires more complex configuration. It applies to VXLAN deployment on a new network.

After you run this command to associate specified VLANs with a BD, different VLANs associated with the same BD form a large Layer 2 network. Users belong to these VLANs can communicate at Layer 2 through VXLAN tunnels.

Copyright © Huawei Technologies Co., Ltd.

Prerequisites

The VLAN to be bound to the BD has been created using the **6.3.43 vlan** command.

Precautions

- One VLAN can be associated with only one BD, but one BD can be associated with multiple VLANs.
- After a global VLAN is associated with a BD, you need to add corresponding interfaces to the VLAN. An Eth-Trunk cannot be added to the VLAN.

Example

Associate VLAN 10 with BD 10.

```
<Huawei> system-view
[Huawei] vlan 10
[Huawei-vlan10] quit
[Huawei] bridge-domain 10
[Huawei-bd10] l2 binding vlan 10
```

12.14.18 mac-address (VBDIF interface view)

Function

The **mac-address** command configures a MAC address for a VBDIF interface.

The **undo mac-address** command restores the default MAC address of a VBDIF interface.

By default, the MAC address of a VBDIF interface is the system MAC address.

Format

mac-address *mac-address*

undo mac-address

Parameters

Parameter	Description	Value
mac-address	Specifies the MAC address of a VBDIF interface.	The value is in the format of H-H-H. Each H is a 4-digit hexadecimal number, such as 00e0 or fc01. If you enter fewer than four digits, the system pads 0s before the input digits. For example, if you enter e0, 00e0 is displayed. The MAC address cannot be FFFF-FFFF-FFFF, all 0s, or a multicast MAC address.

Views

VBDIF interface view

 Copyright © Huawei Technologies Co., Ltd.

Default Level

2: Configuration level

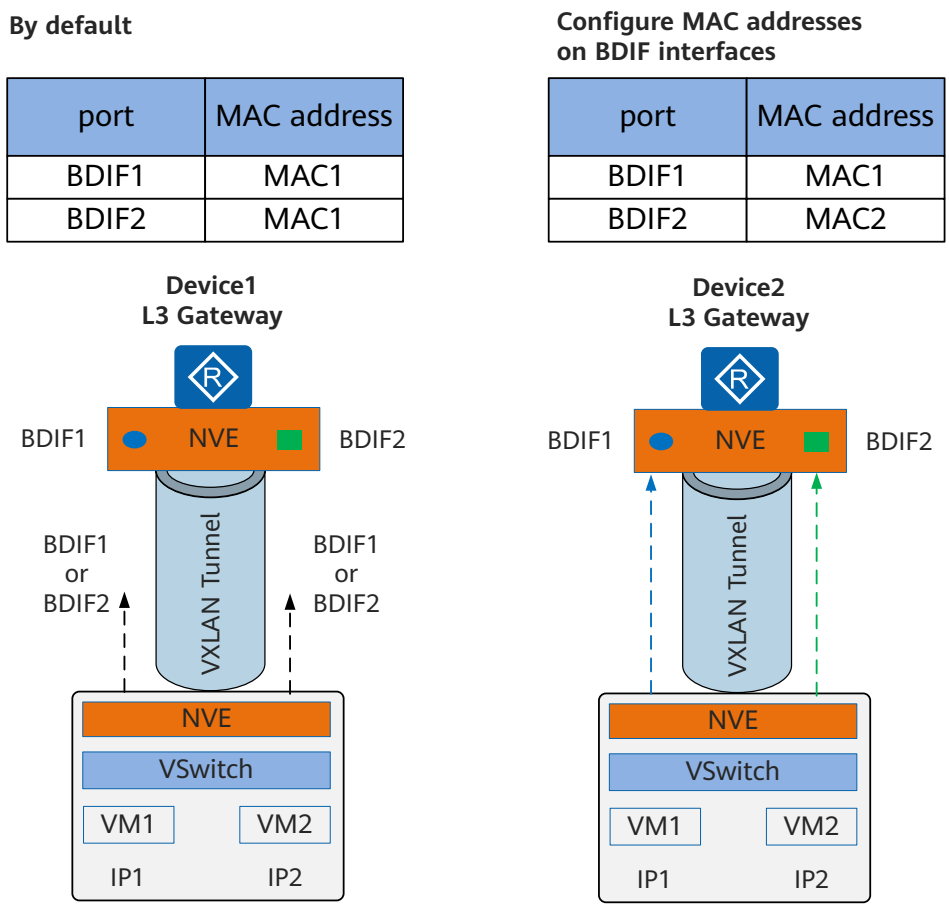
Usage Guidelines

Usage Scenario

In Figure 12-1, the VBDIF interface on both Layer 3 VXLAN gateways uses the system MAC address as its MAC address.

In a distributed gateway or centralized all-active gateway scenario, multiple Layer 3 gateways are simulated into one gateway. You need to configure the **mac-address** command to configure the same MAC address for the VBDIF interface on these Layer 3 gateways to ensure normal traffic forwarding and VM migration. Using the same MAC address, the Layer 3 gateways act like one gateway for terminals.

Figure 12-1 Default MAC addresses of VBDIF interfaces



Configuration Impact

 Copyright © Huawei Technologies Co., Ltd.

After the MAC address of a VBDIF interface is changed, the device proactively sends gratuitous ARP packets to update ARP entries on the remote device.

Example

Set the MAC address of VBDIF 10 to 0001-2345-abcd.

```
<Huawei> system-view
[Huawei] bridge-domain 10
[Huawei-bd10] quit
[Huawei] interface vbdif 10
[Huawei-Vbdif10] mac-address 0001-2345-abcd
```

12.14.19 mac-address static bridge-domain

Function

The **mac-address static bridge-domain** command configures a static MAC address entry based on a bridge domain (BD). The static MAC address entry guides data forwarding.

The **undo mac-address static** command deletes a static MAC address entry based on a BD.

By default, no static MAC address entry based on a BD is configured.

Format

mac-address static *mac-address interface-type interface-number.subnum* **bridge-domain** *bd-id* { **default** | **untag** | **vid** *vid* }

undo mac-address [*mac-address*] **bridge-domain** *bd-id*

undo mac-address { **static** | **dynamic** } **bridge-domain** *bd-id*

Parameters

Parameter	Description	Value
mac-address	Specifies the destination MAC address.	The value is in H-H-H format. An H is a hexadecimal number of 4 digits, such as 00e0 and fc01. The MAC address cannot be the broadcast MAC address (FFFF-FFFF-FFFF), multicast MAC address (the eighth bit is 1), or MAC address of all 0s.
interface-type interface-number.subnum	Specifies the type and number of a Layer 2 sub-interface that joins a BD.	The interface type must be Ethernet.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
bd-id	Specifies the ID of a BD.	The value is an integer. The value ranges are as follows: • AR100&AR120&AR150&AR160&AR200 series: 1-64 • AR1200 series: 1-128 • AR2220E: 1-256
default	Indicates that the flow encapsulation mode of a Layer 2 sub-interface is default. All packets are transparently transmitted, without any VLAN tag processing.	-
untag	Indicates that the flow encapsulation mode of a Layer 2 sub-interface is untag. Packets are forwarded after VLAN tags are removed from the packets.	-
vid *vid*	Specifies the outer VLAN ID in packets received by a Layer 2 sub-interface.	The value is an integer that ranges from 1 to 4094.
dynamic	Deletes dynamic MAC address entries, that is, MAC address entries learned by an interface based on its source MAC address.	-

Copyright © Huawei Technologies Co., Ltd.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the VXLAN-enabled device forwards BUM packets to the user side, the following issues may occur:

- MAC address table attacks

  When an attack source sends packets with variable MAC addresses, the network device receives the packets and learns source MAC addresses. Because the size of the MAC address table is limited, the device cannot learn MAC addresses of packets after the number of MAC address entries reaches the maximum. During Layer 2 forwarding, these packets will be broadcast in a BD. This seriously affects the network bandwidth and affects the downstream hosts connected to the device.

- MAC address entry attacks

  When the device creates a MAC address table by learning source MAC addresses, the device cannot distinguish packets from authorized and unauthorized users. This threatens network security. If an unauthorized user uses the MAC address of an authorized user as the source MAC address of attack packets and connects to another interface of the device, the device learns an incorrect MAC address entry. The device incorrectly forwards the packets to the unauthorized user. Actually, the packets should be forwarded to the authorized user.

To improve interface security, the network administrator can run the **mac-address static bridge-domain** command to manually add a static MAC address entry to the MAC address table. The static MAC address entry binds the MAC address of an authorized user to a specified interface, which prevents unauthorized users from intercepting data of authorized users.

Prerequisites

Ensure that the following operations have been performed:

- The network administrator is familiar with MAC addresses of devices that need to use static MAC address entries for communication on a network; otherwise, communication of authorized users will be interrupted.
- A Layer 2 sub-interface has been created and joined a BD, and the flow encapsulation mode of the Layer 2 sub-interface has been configured.

Configuration Notes

Manually created MAC address entries take precedence over automatically created MAC address entries. Manually created static MAC address entries and blackhole MAC address entries are not overridden by dynamic MAC address entries, but dynamic MAC address entries can be overridden by static MAC address entries and blackhole MAC address entries.

 Copyright © Huawei Technologies Co., Ltd.

The created static MAC address entries never age out. When the device receives a frame with a specific MAC address, it forwards the frame through the outbound interface. After the configuration is saved, MAC address entries are not lost during system reset or hot swapping of cards.

Example

Configure the device to use Eth0/0/1.1 to forward the received packets that have the destination MAC address of 0003-0002-0003 and belong to BD 10. Eth0/0/1.1 uses dot1q encapsulation.

```
<Huawei> system-view
[Huawei] bridge-domain 10
[Huawei-bd10] quit
[Huawei] interface ethernet0/0/1.1 mode l2
[Huawei-Ethernet0/0/1.1] bridge-domain 10
[Huawei-Ethernet0/0/1.1] encapsulation dot1q vid 10
[Huawei-Ethernet0/0/1.1] quit
[Huawei] mac-address static 0003-0002-0003 ethernet0/0/1.1 bridge-domain 10 vid 10
```

12.14.20 mac-address static vni

Function

The **mac-address static vni** command configures a static MAC address entry of a VXLAN tunnel.

The **undo mac-address static** command deletes a static MAC address entry of a VXLAN tunnel.

By default, a static MAC address entry of a VXLAN tunnel is not configured.

Format

mac-address static *mac-address* **bridge-domain** *bd-id* **source** *source-ip-address* **peer** *peer-ip-address* **vni** *vni-id*

undo mac-address [*mac-address*] **bridge-domain** *bd-id*

undo mac-address { **static** | **dynamic** } **bridge-domain** *bd-id*

Parameters

Parameter	Description	Value
mac-address	Specifies the destination MAC address.	The value is in H-H-H format. An H is a hexadecimal number of 4 digits, such as 00e0 and fc01. The MAC address cannot be the broadcast MAC address (FFFF-FFFF-FFFF), multicast MAC address (the eighth bit is 1), or MAC address of all 0s.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
bridge-domain *bd-id*	Specifies the ID of a BD associated with a VNI.	The value is an integer. The value ranges are as follows: • AR100&AR120&AR150&AR160&AR200 series: 1-64 • AR1200 series: 1-128 • AR2220E: 1-256
source *source-ip-address*	Specifies the IP address of the local VTEP.	The value is in dotted decimal notation.
peer *peer-ip-address*	Specifies the IP address of the remote VTEP.	The value is in dotted decimal notation.
vni-id	Specifies the VNI ID.	The value is an integer that ranges from 0 to 16777215.
dynamic	Deletes dynamic MAC address entries, that is, MAC address entries learned by an interface based on its source MAC address.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After receiving a broadcast, unknown unicast, and multicast (BUM) packet, the VXLAN tunnel ingress replicates the packet based on the VTEP list and forwards it to all the VTEPs with the same VNI. To reduce broadcast traffic and improve network security, run the **mac-address static vni** command to configure a static MAC address entry to specify the forwarding path. This prevents unauthorized users from using the source MAC address of attack packets and intercepting data of authorized users.

Prerequisites

 Copyright © Huawei Technologies Co., Ltd.

A VXLAN tunnel has been configured successfully.

Precautions

The network administrator must be familiar with MAC addresses of devices that need to use static MAC address entries for communication on a network; otherwise, communication of authorized users will be interrupted.

Example

Configure a static MAC address entry with the destination MAC address of 0004-0003-0004 for a VXLAN tunnel.

```
<Huawei> system-view
[Huawei] bridge-domain 20
[Huawei-bd20] vxlan vni 5000
[Huawei-bd20] quit
[Huawei] interface nve 1
[Huawei-Nve1] source 1.1.1.1
[Huawei-Nve1] vni 5000 head-end peer-list 2.2.2.2
[Huawei-Nve1] quit
[Huawei] mac-address static 0004-0003-0004 bridge-domain 20 source 1.1.1.1 peer 2.2.2.2 vni 5000
```

12.14.21 source (NVE interface view)

Function

The **source** command configures an IP address for a source VXLAN Tunnel Endpoint (VTEP).

The **undo source** command deletes the IP address of the source VTEP.

By default, no IP address is configured for a source VTEP.

Format

source *ip-address*

undo source [*ip-address*]

Parameters

Parameter	Description	Value
ip-address	Specifies the IPv4 address of a source VTEP.	The value is in dotted decimal notation.

Views

NVE interface view

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

Usage Scenario

VXLAN needs to be deployed on a downlink interface to provide access services and an uplink interface to establish a VXLAN tunnel.

To establish a VXLAN tunnel, configure IP addresses for the source and destination VTEPs.

To configure an IP address for a source VTEP, run this command. When access service packets reach a Network Virtualization Edge (NVE), the VTEP encapsulates the packets based on the IP addresses of source and destination VTEPs and forwards them.

Precautions

- You can specify the IP address of a physical interface or a loopback interface as the IP address of the source VTEP. The address of a loopback interface is recommended.
- Generally, the NVE interfaces of different devices must be configured with different VTEP addresses; otherwise, traffic forwarding errors may occur.
- The IP address of a VBDIF interface cannot be configured as the IP address of the source VTEP of a VXLAN tunnel.

Follow-up Procedure

Run the **vni head-end peer-list** command to configure an IP address for a destination VTEP.

Example

Set the IP address of the source VTEP to 10.1.1.2.

```
<Huawei> system-view
[Huawei] interface nve 1
[Huawei-Nve1] source 10.1.1.2
```

12.14.22 vni head-end peer-list

Function

The **vni head-end peer-list** command configures an ingress replication list that contains the IP addresses of those remote VTEPs for a VXLAN network identifier (VNI).

The **undo vni head-end peer-list** command deletes the ingress replication list of a VNI.

By default, no ingress replication list is configured for any VNI.

Format

vni *vni-id* **head-end peer-list** *ip-address* &<1-10>

undo vni *vni-id* [**head-end peer-list** *ip-address* &<1-10>]

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
vni-id	Specifies a VNI ID.	The value is an integer that ranges from 0 to 16777215.
ip-address	Specifies the IPv4 address of a remote VTEP.	The value is in dotted decimal notation.

Views

NVE interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the ingress of a VXLAN tunnel receives broadcast, unknown unicast, and multicast (BUM) packets, it replicates these packets and sends a copy to each VTEP in the ingress replication list. The ingress replication list is a collection of remote VTEP IP addresses to which the ingress of a VXLAN tunnel should send replicated BUM packets.

If a source VTEP on a VXLAN connects to multiple remote VTEPs on the same VXLAN segment, run the **vni head-end peer-list** command to configure an ingress replication list that contains the IP addresses of those remote VTEPs. After the source NVE receives BUM packets, the local VTEP sends a copy of the BUM packets to every VTEP in the list.

Precautions

- You need to run the **vni head-end peer-list** command to configure the corresponding VTEP address even if the source VTEP matches only one destination VTEP.
- Run the **ping** command to check whether a reachable route exists between two ends of the tunnel. If there is a reachable route, the tunnel can be established and packets can be normally forwarded. If the two devices have a route to each other but the route is unreachable, the tunnel can still go Up but packets cannot be forwarded.

Example

Configure an ingress replication list for VNI 10, with the remote VTEPs' IP addresses being 10.1.1.1 and 10.1.1.3.

```
<Huawei> system-view
[Huawei] bridge-domain 10
[Huawei-bd10] vxlan vni 10
```

 Copyright © Huawei Technologies Co., Ltd.

```
[Huawei-bd10] quit
[Huawei] interface nve 1
[Huawei-Nve1] vni 10 head-end peer-list 10.1.1.1 10.1.1.3
```

Related Topics

12.14.10 display vxlan peer

12.14.23 vxlan vni (BD view)

Function

The **vxlan vni** command associated a specified VNI with a BD.

The **undo vxlan vni** command restores the default settings.

By default, no VNI is associated with a BD.

Format

vxlan vni *vni-id*

undo vxlan vni *vni-id*

Parameters

Parameter	Description	Value
vni-id	Specifies a VNI ID.	The value is an integer that ranges from 0 to 16777215.

Views

BD view

Default Level

2: Configuration level

Usage Guidelines

Similar to VLAN ID, VNI is used to distinguish VXLAN segments.

On the VXLAN network, one VXLAN segment is a large Layer 2 BD; therefore, VNI and BD have a one-to-one mapping relationship.

You can run this command to configure the mapping relationship between VNIs and BDs. In this way, the VTEP can forward received packets through a correct VXLAN tunnel based on the mapping between BDs and VNIs.

Example

Set the mapping between VNI 10 and BD 10.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> system-view
[Huawei] bridge-domain 10
[Huawei-bd10] vxlan vni 10
```

12.14.24 vxlan vni (VPN instance view)

Function

The **vxlan vni** command binds a VXLAN Network Identifier (VNI) to a Virtual Private Network (VPN) instance.

The **undo vxlan vni** command deletes the binding between the VNI and VPN instance.

By default, a VNI is not bound to any VPN instance.

Format

vxlan vni *vni-id*

undo vxlan vni *vni-id*

Parameters

Parameter	Description	Value
vni-id	Specifies a VNI ID.	The value is an integer that ranges from 1 to 16777215.

Views

VPN instance view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Generally, VPN is used to isolate Layer 3 routes.

On a network with distributed VXLAN gateways deployed, a Layer 2 VNI needs to be allocated for each subnet and a Layer 3 VNI needs to be allocated for each tenant (VPN instance) on a Layer 3 gateway to implement communication over the Layer 3 gateway. After a Layer 3 VNI is bound to a VPN instance, the remote Layer 3 gateway can identify VPN information based on the tenant's VNI ID in packets received from the VXLAN tunnel. In this way, tenants belonging to the same VPN can communicate, while tenants in different VPNs are isolated.

Precautions

Currently, one VNI can be bound to only one VPN instance.

 Copyright © Huawei Technologies Co., Ltd.

The VNI bound to a VPN instance by running the **vxlan vni** command cannot be the same as the VNI configured in the BD.

Example

Bind VNI 50 to VPN instance **huawei**.

```
<Huawei> system-view
[Huawei] ip vpn-instance huawei
[Huawei-vpn-instance-huawei] vxlan vni 50
```

 Copyright © Huawei Technologies Co., Ltd.