11 VPN Configuration Commands

11.1 GRE Configuration Commands

11.1.1 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, a tunnel interface does not have a description.

Format

description *text*

undo description

Parameters

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

Views

Tunnel interface view

Default Level

2: Configuration level

Usage Guidelines

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

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

Example

# Configure the description of Tunnel 1.

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

# Delete the description of Tunnel 1.

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

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

NOTE

- The command supports **vpn-instance** *vpn-instance-name* when the tunnel protocol on a tunnel interface is **gre**.

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.	The value is the name of an existing VPN instance.

Parameter	Description	Value
dest-ip-address	Specifies the destination IP address of a tunnel interface. ● For a GRE tunnel, the destination address is the IP address of the remote tunnel interface that actually receives packets.	The value is in dotted decimal notation.

Views

Tunnel interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When configuring a GRE, create a tunnel interface. After a tunnel interface is created, run the **destination** command to specify the destination IP address for the tunnel interface.

Prerequisites

A tunnel interface has been created using the **interface tunnel** command, and the encapsulation mode is set using the **tunnel-protocol** command.

Example

# Set the destination address of the GRE tunnel Tunnel 2 to 10.1.1.1.

```
<HUAWEI> system-view
[~HUAWEI] interface tunnel 2
[*HUAWEI-Tunnel2] tunnel-protocol gre
[*HUAWEI-Tunnel2] destination 10.1.1.1
```

11.1.3 display interface tunnel

Function

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

Format

display interface tunnel [*interface-number*]

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.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

To check status of tunnels or diagnose the fault in these tunnels, run the **display interface tunnel** command.

When the CPU of the device reaches more than 70%, there will be jitter caused by uneven packet counts of Tunnel at different query time points.

Example

# Display the details of the tunnel interface.

```
<HUAWEI> display interface tunnel 2
Tunnel2 current state : UP (ifindex: 19)
Line protocol current state : UP
Last line protocol up time : 2012-03-26 15:23:28
Description:HUAWEI, Tunnel2 Interface
Route Port,The Maximum Transmit Unit is 1500
Internet Address is 10.1.1.1/24
Encapsulation is TUNNEL, loopback not set
Tunnel source 10.1.1.2 (10GE1/0/1), destination 10.1.2.1
Tunnel protocol/transport GRE/IP, key disabled
keepalive disabled
Checksumming of packets disabled
Current system time: 2012-03-26 15:59:20
    300 seconds input rate 0 bits/sec, 0 packets/sec
    300 seconds output rate 0 bits/sec, 0 packets/sec
    1 seconds input rate 0 bits/sec, 0 packets/sec
    1 seconds output rate 0 bits/sec, 0 packets/sec
    14643 packets input,  1493744 bytes
    0 input error
    14749 packets output,  1500171 bytes
    0 output error
    Input:
      Unicast: 14560 packets, Multicast: 0 packets
    Output:
      Unicast: 14670 packets, Multicast: 0 packets
    Input bandwidth utilization  :    --
    Output bandwidth utilization :    --
```

Table 11-1 Description of the **display interface tunnel** command output

Item	Description
Tunnel2 current state	Status at the physical layer of a tunnel interface: ● UP: The interface is in the normal state. ● Administratively DOWN: The network administrator has run the **shutdown** command on the interface. ● DOWN: The tunnel is not established. After a tunnel interface is created, its status at the physical layer is generally Down.
Line protocol current state	Link protocol status: ● Up: The link layer protocol of the tunnel interface works normally. ● Down: The link layer protocol of the tunnel interface is abnormal.
Last line protocol up time	Last time when the link layer protocol was Up.
Description	Description of the tunnel interface.
Route Port, The Maximum Transmit Unit is 1500	MTU of the tunnel interface. By default, it is 1500 bytes. A packet larger than the MTU is fragmented before being sent. If non-fragmentation is configured, the packet is discarded.
Internet Address is 10.1.1.1/24	The IP address of the tunnel.
Encapsulation is TUNNEL	Encapsulation type of packets on the tunnel interface.
loopback not set	The tunnel interface does not have the loopback mode set.
Tunnel source 10.1.1.2 (10GE1/0/1)	The source address of the tunnel is 10.1.1.2.
destination 10.1.2.1	The destination address of the tunnel is 10.1.2.1.
Tunnel protocol/transport GRE/IP, key disabled	The tunnel encapsulation protocol is GRE/IP. GRE key is disabled on the GRE tunnel interface.
keepalive disabled	Indicates that Keepalive is disabled on the GRE tunnel interface.
Checksumming of packets disabled	Indicates that checksum check is disabled on the GRE tunnel interface.
Current system time	Current system time.

Item	Description
300 seconds input rate 0 bits/sec, 0 packets/sec	Indicates the rates at which the interface receives bits and packets in the last 300 seconds.
300 seconds output rate 0 bits/sec, 0 packets/sec	Indicates the rates at which the interface sends bits and packets in the last 300 seconds.
1 seconds input rate 0 bits/ sec, 0 packets/sec	Indicates the rates at which the interface receives bits and packets during the interval at which traffic statistics are collected.
1 seconds output rate 0 bits/sec, 0 packets/sec	Indicates the rates at which the interface sends bits and packets during the interval at which traffic statistics are collected.
14643 packets input, 1493744 bytes	Indicates the number of received packets and number of received bytes.
0 input error	Indicates the number of received error packets. On a GRE tunnel interface, this option value cannot be calculated and fixed at 0.
14749 packets output, 1500171 bytes	Indicates the number of send packets and number of send bytes.
0 output error	Indicates the number of sent error packets. On a GRE tunnel interface, this option value cannot be calculated and fixed at 0.
Input	Indicates the number of unicast or multicast packets the GRE tunnel interface receives. ● Unicast: indicates the number of unicast packets. ● Multicast: indicates the number of multicast packets.
Output	Indicates the number of unicast or multicast packets the GRE tunnel interface sends. ● Unicast: indicates the number of unicast packets. ● Multicast: indicates the number of multicast packets.
Input bandwidth utilization	Indicates the percentage of the rate for receiving packets in the total bandwidth.
Output bandwidth utilization	Indicates the percentage of the rate for sending packets in the total bandwidth.

11.1.4 interface tunnel

Function

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

The **undo interface tunnel** command deletes a tunnel interface.

By default, no tunnel interface is configured.

Format

interface tunnel *interface-number*

undo interface tunnel *interface-number*

Parameters

Parameter	Description	Value
interface-number	Specifies the number of the tunnel interface.	The value is an integer in the range from 0 to 20479.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

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

- GRE tunnel

Precautions

Tunnel interfaces can be created in all VSs in group mode.

After a tunnel interface is created, configure an IP address and encapsulation protocol for the tunnel interface.

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

Example

# Create a tunnel interface.

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

11.1.5 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 46 to 9216, 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.

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

The switch does not perform the MTU check for IP packets forwarded by the chip by default. If the length of IPv4 packets forwarded by the chip exceeds the interface MTU after the **ip fragment enable** command is configured on a switch, the switch fragments the packets and then forwards them.

Example

# Set the MTU of Tunnel 1 to 1492.

```
<HUAWEI> system-view
[~HUAWEI] interface tunnel 1
[*HUAWEI-Tunnel1] mtu 1492
[*HUAWEI-Tunnel1] shutdown
[*HUAWEI-Tunnel1] undo shutdown
```

11.1.6 source

Function

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

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

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

Format

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

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

Parameters

Parameter	Description	Value
source-ip-address	Specifies the source address of a tunnel interface.	The value is in dotted decimal notation.
interface-type interface-number	Specifies the type and the number of the source interface of the tunnel.	-

Views

Tunnel 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 using the **tunnel-protocol** command.

Precautions

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

You can configure an Ethernet interface working in Layer 3 mode as the source tunnel interface.

GRE tunnel is bidirectional tunnel. 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.

Example

# Set the tunnel type of Tunnel1 to GRE tunnel and configure the source IP address of Tunnel1 as 10.1.1.1.

```
<HUAWEI> system-view
[~HUAWEI] interface tunnel 1
[*HUAWEI-Tunnel1] tunnel-protocol gre
[*HUAWEI-Tunnel1] source 10.1.1.1
```

11.1.7 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** | **none** }

undo tunnel-protocol

Parameters

Parameter	Description	Value
gre	Indicates that the GRE tunnel protocol is configured on a tunnel interface.	-
none	Indicates that no tunnel protocol is configured on a tunnel interface.	-

Views

Tunnel interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

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

Precautions

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

Example

# Set the tunnel encapsulation mode of Tunnel2 to gre.

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

11.2 VPN Configuration Commands

11.2.1 advertise valid-routes

Function

The **advertise valid-routes** command configures a device to send only valid routes in a BGP VPN routing table to a BGP VPNv4/VPNv6 routing table.

The **undo advertise valid-routes** command restores the default configuration.

By default, a device sends all routes in a BGP VPN routing table to a BGP VPNv4/VPNv6 routing table.

Format

advertise valid-routes

undo advertise valid-routes

Parameters

None

Views

BGP-VPN instance IPv4 address family view or BGP-VPN instance IPv6 address family view

Default Level

2: Configuration level

Usage Guidelines

Run this command to configure a device to send only valid routes in a BGP VPN routing table to a BGP VPNv4/VPNv6 routing table.

Example

# Configure a device to send only valid routes in a BGP VPN routing table to a BGP VPNv4 routing table.

```
<HUAWEI> system-view
[~HUAWEI] bgp 100
[*HUAWEI-bgp] ipv4-family vpn-instance vpn1
[*HUAWEI-bgp-vpn1] advertise valid-routes
```

11.2.2 alarm-threshold route vpn-instance

Function

The **alarm-threshold route vpn-instance** command sets a threshold and log recovery percentage for the number of routes in a VPN instance.

The **undo alarm-threshold route vpn-instance** command cancels the settings.

By default, the threshold and log recovery percentage for the number of routes in an L3VPN instance are not configured.

Format

alarm-threshold route *route-number* [**recovery-percentage** *percentage*] { **ipv4** | **ipv6** } **vpn-instance** *vpn-instance-name*

undo alarm-threshold route *route-number* [**recovery-percentage** *percentage*] { **ipv4** | **ipv6** } **vpn-instance** *vpn-instance-name*

Parameters

Parameter	Description	Value
route-number	Specifies the threshold for the number of routes.	The value is an integer ranging from 1 to 4294967295.
recovery-percentage *percentage*	Specifies the log recovery percentage.	The value is an integer ranging from 1 to 95. After the threshold for the number of routes is set, the log recovery percentage is 80 by default.
ipv4	Specifies the VPN instance IPv4 address family.	-
ipv6	Specifies the VPN instance IPv6 address family.	-
vpn-instance *vpn-instance-name*	Specifies the name of a VPN instance.	The value is a string of 1 to 31 case-sensitive characters except spaces. When double quotation marks are used to include the string, spaces are allowed in the string. The value _public_ is reserved and cannot be used as the VPN instance name.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

In a distributed VXLAN gateway scenario or BPG/MPLS VPN networking, EVPN or VPNv4/VPNv6 serves as the control plane to deliver host routes, and VPN instances store IP routes. As the number of access hosts increases, routes stored control plane increase greatly, consuming a lot of memory resources. To better monitor the impact of an increase in route quantity on memory and prevent device restart caused by memory insufficiency, run the **alarm-threshold route vpn-instance** command to set a threshold for the number of routes by VPN instance. When the number of routes exceeds the threshold, a user log will be generated. When the number of routes equals the log recovery percentage, a recovery log will be generated.

Example

# Set a threshold and log recovery percentage for the number of routes in a VPN instance.

```
<HUAWEI> system-view
[~HUAWEI] alarm-threshold route 10000 recovery-percentage 90 ipv4 vpn-instance vrf1
```

11.2.3 as-number

Function

The **as-number** command configures an AS number for a VPN instance.

The **undo as-number** command restores the default setting.

By default, a VPN instance uses the AS number of BGP.

Format

as-number { *as-number-plain* | *as-number-dot* }

undo as-number

Parameters

Parameter	Description	Value
as-number-plain	Integral AS number	The value is an integer ranging from 1 to 4294967295.
as-number-dot	AS number in dotted notation	The value is in the format of *x.y*, where *x* and *y* are integers that range from 1 to 65535 and from 0 to 65535, respectively.

Views

BGP-VPN instance IPv4 address family view, BGP-VPN instance IPv6 address family view, BGP multi-instance VPN instance IPv4 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 BGP 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.

The AS number configured in the BGP-VPN instance view cannot be the same as the AS number configured in the BGP view.

Example

# Set the AS number of the VPN instance named **vpna** to 65001.

```
<HUAWEI> system-view
[~HUAWEI] bgp 100
[*HUAWEI-bgp] ipv4-family vpn-instance vpna
[*HUAWEI-bgp-vpna] as-number 65001
```

11.2.4 description (VPN instance view)

Function

The **description** command specifies the description of the current VPN instance.

The **undo description** command deletes the description of the current VPN instance.

By default, no description is specified for a VPN instance.

Format

description *description-information*

undo description

Parameters

Parameter	Description	Value
description-information	Specifies the description of a VPN instance.	The value is a string of 1 to 242 case-sensitive characters with spaces.

Views

VPN instance view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To record the purpose of creating a VPN instance and the CEs with which the VPN instance is associated, you can run the **description** command to specify the description of the VPN instance.

To check the description of a VPN instance, run the **display ip vpn-instance** command.

Precautions

If you run the **description** command several times, the latest configuration overrides the previous configurations.

Example

# Specify the description of a VPN instance named vpn1.

```
<HUAWEI> system-view
[~HUAWEI] ip vpn-instance vpn1
[*HUAWEI-vpn-instance-vpn1] description OnlyForAB
```

11.2.5 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**

Parameters

Parameter	Description	Value
verbose	Displays detailed information about VPN instances.	-
vpn-instance-name	Specifies the name of a VPN instance.	The value is the name of an existing VPN instance.
interface	Displays information about the interfaces bound to the VPN instance.	-

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.

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      : 5
 Total IPv4 VPN-Instances configured : 3
 Total IPv6 VPN-Instances configured : 2

  VPN-Instance Name               RD                    Address-family
  vpn1                            100:1                 IPv4
  HWTest                               IPv6
  vpna                    30:1         IPv6
  vpnb                    33:1         IPv4
  device                              IPv4
```

Table 11-2 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 : 0

 VPN-Instance Name and ID : vpna, 1
  Description : sss
  Interfaces : LoopBack1
               Vlanif11
 Address family ipv4
  Create date : 2012-06-26 07:24:40
  Up time : 14 days, 13 hours, 53 minutes and 24 seconds
  Vrf Status : UP
  Route Distinguisher : 100:1
  Export VPN Targets : 100:1
  Import VPN Targets : 100:1
  Label Policy : label per instance
  Per-Instance Label : 16
  IP FRR Inter-Protocol Enable
  VPN FRR Enable
  Import Route Policy : policy1
  Export Route Policy : policy2
```

```
Maximum Routes Limit : 200
Threshold Routes Limit : 80%
```

Table 11-3 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.
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.
Vrf Status	VPN status: ● UP ● DOWN
Route Distinguisher	RD of the VPN instance IPv4 address. To configure an RD, run the **route-distinguisher**command.
Export VPN Targets	Route Target list in the outbound direction. To set the VPN target, run the **vpn-target**command.

Item	Description
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. ● label per route: indicates that each route of a VPN instance is assigned a label. This field is displayed in the command output only when the **apply-label per-route**command is run in the VPN instance view.
Per-Instance Label	Label value used when all VPN routes of the VPN instance address family share one label.
IP FRR Inter-Protocol Enable	IP FRR is enabled for the address family. This item is displayed only after the **ip frr**command is run in the VPN instance address family view.
VPN FRR Enable	VPN FRR is enabled for the address family. This field is displayed only after the **vpn frr**command is run in the VPN instance 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.
Maximum Routes 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.

Item	Description
Threshold Routes 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.

# Display information about the interface bound to the VPN instance named **vrf1**.

```
<HUAWEI> display ip vpn-instance vrf1 interface
 VPN-Instance Name and ID : vrf1, 1
  Interface Number : 4
  Interface list : Vlanif40,
                   LoopBack1,
                   LoopBack2,
                   LoopBack3
```

Table 11-4 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.

11.2.6 display ip vpn-instance import-vt

Function

The **display ip vpn-instance import-vt** command displays all VPN instances with the specified import vpn-target attribute.

Format

display ip vpn-instance import-vt *ivt-value*

Parameters

Parameter	Description	Value
ivt-value	Specifies the value of the import VPN-target attribute. The forms of VPN targets are as follows: ● 2-byte AS number: 4-byte user-defined number, for example, 1:3. The AS number ranges from 0 to 65535. The user-defined number ranges from 0 to 4294967295. The AS number and the user-defined number cannot both be 0. That is, a VPN target cannot be 0:0. ● IPv4-address: 2-byte user-defined number, for example, 192.168.122.15:1. The IP address ranges from 0.0.0.0 to 255.255.255.255. The user-defined number ranges from 0 to 65535. ● Integral 4-byte AS number:2-byte user-defined number, for example, 65537:3. An AS number ranges from 65536 to 4294967295. A user-defined number ranges from 0 to 65535. The AS number and user-defined number cannot be both 0s. That is, a VPN target cannot be 0:0. ● 4-byte AS number in dotted notation:2-byte user-defined number, for example, 0.0:3 or 0.1:0. A 4-byte AS number in dotted notation is in the format of *x.y*, where *x* and *y* are integers that range from 0 to 65535 and from 0 to 65535, respectively. A user-defined number ranges from 0 to 65535. The AS number and user-defined number cannot be both 0s. That is, a VPN target cannot be 0.0:0.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

If a PE is configured with multiple VPN instances, the **display ip vpn-instance import-vt** command can be run on the PE to check into which VPN instances a VPNv4 route with a specified VPN target can be imported.

The VPN target controls route learning between VPN instances. A VPN target may be either an import VPN target or an export VPN target. An export VPN target is contained in a VPNv4 route to be advertised to a remote MP-BGP peer. Receiving a VPNv4 route, an MP-BGP peer compares the received export VPN target with the local import VPN target to determine whether the VPNv4 route can be added to the routing table of the local VPN instance IPv4 address family.

Precautions

At present, this command cannot be used to view the VPN instance with multiple import VPN-target attributes specified.

Example

# Display the VPN instance with the import VPN-target attribute being 1:1.

```
<HUAWEI> display ip vpn-instance import-vt 1:1
The number of ipv4-family matched the import-vt : 3
 VPN-Instance Name and ID : vrf1, 1
 VPN-Instance Name and ID : vrf4, 5
 VPN-Instance Name and ID : vrf5, 4

The number of ipv6-family matched the import-vt : 2
 VPN-Instance Name and ID : vrf1, 1
 VPN-Instance Name and ID : vrf5, 4
```

Table 11-5 Description of the display ip vpn-instance import-vt command output

Item	Description
The number of ipv4-family matched the import-vt	Number of VPN instances with the specified import VPN-target attribute in the VPN instance IPv4 address family view.
The number of ipv6-family matched the import-vt	Number of VPN instances with the specified import VPN-target attribute in the VPN instance IPv6 address family view.
VPN-Instance Name and ID	Name and ID of the VPN instance.

11.2.7 display interface tunnel

Function

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

Format

display interface tunnel [*interface-number*]

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.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

To check status of tunnels or diagnose the fault in these tunnels, run the **display interface tunnel** command.

When the CPU of the device reaches more than 70%, there will be jitter caused by uneven packet counts of Tunnel at different query time points.

Example

# Display the details of the tunnel interface.

```
<HUAWEI> display interface tunnel 2
Tunnel2 current state : UP (ifindex: 19)
Line protocol current state : UP
Last line protocol up time : 2012-03-26 15:23:28
Description:HUAWEI, Tunnel2 Interface
Route Port,The Maximum Transmit Unit is 1500
Internet Address is 10.1.1.1/24
Encapsulation is TUNNEL, loopback not set
Tunnel source 10.1.1.2 (10GE1/0/1), destination 10.1.2.1
Tunnel protocol/transport GRE/IP, key disabled
keepalive disabled
Checksumming of packets disabled
Current system time: 2012-03-26 15:59:20
    300 seconds input rate 0 bits/sec, 0 packets/sec
    300 seconds output rate 0 bits/sec, 0 packets/sec
    1 seconds input rate 0 bits/sec, 0 packets/sec
    1 seconds output rate 0 bits/sec, 0 packets/sec
    14643 packets input,  1493744 bytes
    0 input error
    14749 packets output,  1500171 bytes
    0 output error
    Input:
      Unicast: 14560 packets, Multicast: 0 packets
    Output:
      Unicast: 14670 packets, Multicast: 0 packets
    Input bandwidth utilization  :    --
    Output bandwidth utilization :    --
```

Table 11-6 Description of the **display interface tunnel** command output

Item	Description
Tunnel2 current state	Status at the physical layer of a tunnel interface: ● UP: The interface is in the normal state. ● Administratively DOWN: The network administrator has run the **shutdown** command on the interface. ● DOWN: The tunnel is not established. After a tunnel interface is created, its status at the physical layer is generally Down.
Line protocol current state	Link protocol status: ● Up: The link layer protocol of the tunnel interface works normally. ● Down: The link layer protocol of the tunnel interface is abnormal.
Last line protocol up time	Last time when the link layer protocol was Up.
Description	Description of the tunnel interface.
Route Port, The Maximum Transmit Unit is 1500	MTU of the tunnel interface. By default, it is 1500 bytes. A packet larger than the MTU is fragmented before being sent. If non-fragmentation is configured, the packet is discarded.
Internet Address is 10.1.1.1/24	The IP address of the tunnel.
Encapsulation is TUNNEL	Encapsulation type of packets on the tunnel interface.
loopback not set	The tunnel interface does not have the loopback mode set.
Tunnel source 10.1.1.2 (10GE1/0/1)	The source address of the tunnel is 10.1.1.2.
destination 10.1.2.1	The destination address of the tunnel is 10.1.2.1.
Tunnel protocol/transport GRE/IP, key disabled	The tunnel encapsulation protocol is GRE/IP. GRE key is disabled on the GRE tunnel interface.
keepalive disabled	Indicates that Keepalive is disabled on the GRE tunnel interface.
Checksumming of packets disabled	Indicates that checksum check is disabled on the GRE tunnel interface.
Current system time	Current system time.

Item	Description
300 seconds input rate 0 bits/sec, 0 packets/sec	Indicates the rates at which the interface receives bits and packets in the last 300 seconds.
300 seconds output rate 0 bits/sec, 0 packets/sec	Indicates the rates at which the interface sends bits and packets in the last 300 seconds.
1 seconds input rate 0 bits/ sec, 0 packets/sec	Indicates the rates at which the interface receives bits and packets during the interval at which traffic statistics are collected.
1 seconds output rate 0 bits/sec, 0 packets/sec	Indicates the rates at which the interface sends bits and packets during the interval at which traffic statistics are collected.
14643 packets input, 1493744 bytes	Indicates the number of received packets and number of received bytes.
0 input error	Indicates the number of received error packets. On a GRE tunnel interface, this option value cannot be calculated and fixed at 0.
14749 packets output, 1500171 bytes	Indicates the number of send packets and number of send bytes.
0 output error	Indicates the number of sent error packets. On a GRE tunnel interface, this option value cannot be calculated and fixed at 0.
Input	Indicates the number of unicast or multicast packets the GRE tunnel interface receives. ● Unicast: indicates the number of unicast packets. ● Multicast: indicates the number of multicast packets.
Output	Indicates the number of unicast or multicast packets the GRE tunnel interface sends. ● Unicast: indicates the number of unicast packets. ● Multicast: indicates the number of multicast packets.
Input bandwidth utilization	Indicates the percentage of the rate for receiving packets in the total bandwidth.
Output bandwidth utilization	Indicates the percentage of the rate for sending packets in the total bandwidth.

11.2.8 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

Default Level

3: Management 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 : 16
------------------------------------------------------------------------------
Trap name                     Default switch status   Current switch status
hwIpv4RouteExceed                   off                     off
hwIpv4RouteExceedClear              off                     off
hwIpv4RouteThresholdExceed          off                     off
hwIpv4RouteThresholdExceedClear
                                    off                     off
hwIpv6RouteExceed                   off                     off
hwIpv6RouteExceedClear              off                     off
hwIpv6RouteThresholdExceed          off                     off
hwIpv6RouteThresholdExceedClear
                                    off                     off
```

```
hwL3vpnVrfRouteMidThreshCleared
                         off                  off
hwL3vpnVrfV6Down              off                  off
hwL3vpnVrfV6Up              off                  off
mplsL3VpnNumVrfRouteMaxThreshCleared
                         off                  off
mplsL3VpnVrfDown              off                  off
mplsL3VpnVrfNumVrfRouteMaxThreshExceeded
                         off                  off
mplsL3VpnVrfRouteMidThreshExceeded
                         off                  off
mplsL3VpnVrfUp              off                  off
```

Table 11-7 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.
Trap name	Types of trap messages.
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.

11.2.9 display tunnel

Function

The **display tunnel** command displays information about tunnels.

Format

display tunnel { *tunnel-id* | **all** | **statistics** }

Parameters

Parameter	Description	Value
tunnel-id	Specifies a tunnel ID.	The value is a string of 1 to 20 characters without spaces. When double quotation marks are used around the string, spaces are allowed in the string.
all	Displays information about all tunnels.	-
statistics	Collects the statistics about tunnels by type.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The **display tunnel** *tunnel-id* command displays detailed information about a specific tunnel.

The **display tunnel all** command displays information about the tunnels that are already set up, including the tunnel IDs, tunnel types, and destination IP addresses.

The **display tunnel statistics** command displays the statistics about different types of tunnels that are already set up.

Example

# Display information about a tunnel.

```
<HUAWEI> display tunnel 0x000000000300000001
Tunnel ID          : 0x000000000300000001
Type               : te
Name               : Tunnel1
Destination        : 2.2.2.2
Instance ID        : 0
Mtu                : 1500
Cost               : 0
Status             : UP
Out Interface:   Tunnel1
NextHop:         0.0.0.0
```

Table 11-8 Description of the **display tunnel** command output

Item	Description
Tunnel ID	Indicates the tunnel ID. Tunnel IDs identify tunnels with the same instance ID and same tunnel type.
Type	Indicates the tunnel types.
Name	Indicates the name of the tunnel.
Destination	Indicates the destination IP address of the tunnel.
Instance ID	Indicates the ID of the VPN instance (0 indicates that the tunnel is a public network tunnel).
Mtu	Indicates the tunnel MTU.
Cost	Indicates the tunnel cost.
Status	Indicates the tunnel status: ● UP: The tunnel is established. ● Down: The tunnel is not established.
Out Interface	Interface of tunnel.
NextHop	NextHop of tunnel.

# Display information about all tunnels.

```
<HUAWEI> display tunnel all
Tunnel ID                 Type           Destination       Status
----------------------------------------------------------------------------
0x0000000001004c4b4c      ldp            10.3.3.3          UP
0x0000000001004c4b4d      ldp            10.3.3.9          UP
```

# Display the statistics about different types of tunnels.

```
<HUAWEI> display tunnel statistics
TunnelType                        Number
-----------------------------------------------------------
ldp                               2
```

Table 11-9 Description of the **display tunnel statistics** command output

Item	Description
TunnelType	Indicates the tunnel types.
Number	Indicates the number of tunnels.

11.2.10 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* [**add-ert-first**]

VPN instance view:

undo export route-policy

VPN instance IPv4 address family view:

undo export route-policy

VPN instance IPv6 address family view:

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 200 case-sensitive characters except spaces. When double quotation marks are used to include the string, spaces are allowed in the string.
add-ert-first	Adds ERTs to VPN routes before these routes are matched against an export routing policy.	-

Views

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

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can implement a more accurate advertisement of the routes of the VPN instance address family based on the export Route-Policy than that based on the extended community attribute. The export Route-Policy is used to filter the routing information and to set the routing attributes of the routes that pass the filtering.

The **export route-policy** command advertises local routes of the VPN instance address family to other VPN instances address family. The **peer route-policy** command or the **filter-policy** command run in the BGP VPN instance address family view filters routes of the VPN instance address family advertised to or received from CE neighbors.

By default, ERTs are added to VPN routes before these routes are matched against an export routing policy. If the export routing policy contains RT-related filtering rules, these rules cannot apply to these routes. If you want to apply the RT-related filtering rules defined in an export routing policy to VPN routes, run the **add-ert-first** command to configure the system to add ERTs to VPN routes before matching these routes against the export routing policy.

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.

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
```

11.2.11 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*

VPN instance view:

undo import route-policy

VPN instance IPv4 address family view:

undo import route-policy

VPN instance IPv6 address family view:

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 200 case-sensitive characters except spaces. When double quotation marks are used to include 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

When no import Route-Policy is configured, routes that match the export VPN target attribute of the received routes and the import VPN target attribute of the local VPN instance address family are added to the VPN instance address family. To control the import of the routes into the VPN instance address family more accurately, you can use the import Route-Policy. The import Route-Policy is used to filter the imported routing information and to set the routing attributes of the routes that pass the filtering.

The **import route-policy** command controls the VPN routes that are cross added to the VPN instance address family. The **peer route-policy** command or the **filter-policy** command run in the BGP VPN instance address family view filters routes of the VPN instance address family advertised to or received from CE neighbors.

Prerequisites

The **route-distinguisher** command has been executed to set the RD of the VPN instance.

Precautions

The current VPN instance address family can be associated with only one import Route-Policy. If the **import route-policy** command is run several times, the latest configuration overrides the previous configurations.

If the route policy to be associated with the VPN instance address family does not exist, you need to configure the route policy.

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
```

11.2.12 import-rib (BGP-VPN instance view)

Function

The **import-rib** command enables a device to import BGP routes of a public network instance or a VPN instance to the BGP routing table of a specified VPN instance.

The **undo import-rib** command restores the default configuration.

By default, a device does not import BGP routes of a public network instance or a VPN instance to the BGP routing table of a specified VPN instance.

Format

import-rib { **public** | **vpn-instance** *vpn-instance-name* } [**include-label-route**] [**valid-route**] [**route-policy** *route-policy-name*]

undo import-rib { **public** | **vpn-instance** *vpn-instance-name* } [**include-label-route**] [**valid-route**] [**route-policy** *route-policy-name*]

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Specifies the name of a VPN instance.	The value is a string of 1 to 31 case-sensitive characters except spaces. When double quotation marks are used to include the string, spaces are allowed in the string. The value _public_ is reserved and cannot be used as the VPN instance name.

Parameter	Description	Value
public	Indicates the public network instance.	-
include-label-route	Includes labeled routes received from BGP peers as well as locally and remotely leaked VPN routes.	-
valid-route	Imports valid BGP routes to be imported from a public network instance or a VPN instance.	-
route-policy *route-policy-name*	Specifies a route-policy to filter routes to be imported.	The name is a string of 1 to 200 case-sensitive characters except spaces. When double quotation marks are used to include the string, spaces are allowed in the string.

Views

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

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To enable VPN users to communicate with public network users, you can run the following commands to configure BGP route import between VPN and public network instances:

- Run the **import-rib vpn-instance** *vpn-instance-name* [**include-label-route**] [**valid-route**] [**route-policy** *route-policy-name*] command to enable a device to import BGP routes of a VPN instance to the BGP routing table of a public network instance.
- Run the **import-rib public** [**include-label-route**] [**valid-route**] [**route-policy** *route-policy-name*] command to enable a device to import BGP routes of a public network instance to the BGP routing table of a VPN instance.

To enable users in one VPN to communicate with users in another VPN, run the **import-rib vpn-instance** *vpn-instance-name* command to configure route import between VPN instances.

If you run the **import-rib** command without specifying the **valid-route** parameter, the device will import only active valid BGP routes from a VPN instance or public network instance. To enable the device to import all valid BGP routes, specify the **valid-route** parameter when running the **import-rib** command.

If a BGP route newly imported to the BGP routing table of a VPN instance shares the same prefix with a BGP route in the table, the VPN instance compares the two routes and delivers only the preferred route to the IP routing table to guide traffic forwarding. If you want a newly imported BGP route to be preferred, specify the **route-policy** *route-policy-name* parameter, so that the VPN instance changes the route attributes based on the route-policy.

Precautions

If the **route-policy** *route-policy-name* parameter is specified in the **import-rib** command, the **if-match interface** command will become ineffective.

Example

# Enable a device to import valid BGP routes of a public network instance to the BGP routing table of the specified VPN instance.

```
<HUAWEI> system-view
[~HUAWEI] bgp 100
[*HUAWEI-bgp] ipv4-family vpn-instance vpna
[*HUAWEI-bgp-vpna] import-rib public valid-route
```

11.2.13 import-rib route next-hop-invariable

Function

The **import-rib route next-hop-invariable** command configures a VPN instance to retain the original next hops of imported routes when advertising these routes to its IBGP peers.

The **undo import-rib route next-hop-invariable** command restores the default configuration.

By default, a VPN instance changes the next hops of imported routes to its own next hop when advertising these routes to its IBGP peers.

Format

import-rib route next-hop-invariable

undo import-rib route next-hop-invariable

Parameters

None

Views

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

Default Level

2: Configuration level

Usage Guidelines

To enable a VPN instance to retain the original next hops of imported routes when advertising these routes to its IBGP peers, run the **import-rib route next-hop-invariable** command for the VPN instance.

Example

# Enable a VPN instance to retain the original next hops of imported routes when advertising these routes to its IBGP peers.

```
<HUAWEI> system-view
[~HUAWEI] bgp 100
[*HUAWEI-bgp] ipv4-family vpn-instance vpna
[*HUAWEI-bgp-vpna] import-rib route next-hop-invariable
```

11.2.14 import-rib vpn-instance

Function

The **import-rib vpn-instance** command enables a device to import BGP routes of a VPN instance to the BGP routing table of a public network instance.

The **undo import-rib vpn-instance** command restores the default configuration.

By default, a device does not import BGP routes of a VPN instance to the BGP routing table of a public network instance.

Format

import-rib vpn-instance *vpn-instance-name* [**include-label-route**] [**valid-route**] [**route-policy** *route-policy-name*]

undo import-rib vpn-instance *vpn-instance-name* [**include-label-route**] [**valid-route**] [**route-policy** *route-policy-name*]

Parameters

Parameter	Description	Value
vpn-instance-name	Specifies the name of a VPN instance.	The value is a string of 1 to 31 case-sensitive characters except spaces. When double quotation marks are used to include the string, spaces are allowed in the string. The value _public_ is reserved and cannot be used as the VPN instance name.
include-label-route	Includes labeled routes received from BGP peers as well as locally and remotely leaked VPN routes.	-

Parameter	Description	Value
valid-route	Imports all valid BGP routes of the VPN instance.	-
route-policy *route-policy-name*	Specifies a route-policy to filter routes to be imported.	The name is a string of 1 to 200 case-sensitive characters except spaces. When double quotation marks are used to include the string, spaces are allowed in the string.

Views

BGP view, BGP-VPN IPv4 unicast address family view, BGP-VPN IPv6 unicast address family view, BGP-VPN multi-instance IPv4 address family view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To enable VPN users to communicate with public network users, you can run the following commands to configure BGP route import between VPN and public network instances:

- Run the **import-rib vpn-instance** *vpn-instance-name* [**include-label-route**] [**valid-route**] [**route-policy** *route-policy-name*] command to enable a device to import BGP routes of a VPN instance to the BGP routing table of a public network instance.
- Run the **import-rib public** [**include-label-route**] [**valid-route**] [**route-policy** *route-policy-name*] command to enable a device to import BGP routes of a public network instance to the BGP routing table of a VPN instance.

If you run the **import-rib vpn-instance** command without specifying the **valid-route** parameter, the device will import only active valid BGP routes from the VPN instance to the public network instance. To enable the device to import all valid BGP routes, specify the **valid-route** parameter when running the **import-rib vpn-instance** command.

If a BGP route newly imported to the BGP routing table of a VPN instance shares the same prefix with a BGP route in the table, the VPN instance compares the two routes and delivers only the preferred route to the IP routing table to guide traffic forwarding. If you want a newly imported BGP route to be preferred, specify the **route-policy** *route-policy-name* parameter, so that the VPN instance changes the route attributes based on the route-policy.

Precautions

If the **route-policy** *route-policy-name* parameter is specified in the **import-rib vpn-instance** command, the **if-match interface** command will become ineffective.

Example

# Enable a device to import BGP routes of VPN instance **vpna** to the BGP routing table of a public network instance.

```
<HUAWEI> system-view
[~HUAWEI] bgp 100
[*HUAWEI-bgp] import-rib vpn-instance vpna
```

11.2.15 ip binding vpn-instance

Function

The **ip binding vpn-instance** command associates an interface on a PE with a VPN instance.

The **undo ip binding vpn-instance** command disables the association between a VPN instance and an interface.

By default, an interface is a public network interface and is not associated with any VPN instance.

Format

ip binding vpn-instance *vpn-instance-name*

undo ip binding vpn-instance *vpn-instance-name*

Parameters

Parameter	Description	Value
vpn-instance-name	Specifies the name of the VPN instance that is associated with the interface.	The value is a string of 1 to 31 case-sensitive characters except spaces. When double quotation marks are used to include the string, spaces are allowed in the string. The value _public_ is reserved and cannot be used as the VPN instance name.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After a VPN instance is created, you need to associate the PE interface connecting to the VPN with the VPN instance. Then, the interface is used as a private network interface on which a private network address and a private network routing protocol can be configured.

A VPN instance is usually bound to a loopback interface to test whether two private networks can communicate. Before binding a VPN instance to a loopback interface, bind the instance to a VLANIF interface or a physical interface. In application, a VPN instance must be bound to a VLANIF interface, a physical interface or a tunnel interface.

Prerequisites

The **ip vpn-instance** command has been executed to create a VPN instance

Precautions

After an interface is associated with a VPN instance or an interface is unassociated from a VPN instance, the Layer 3 features on this interface, such as the IP address and routing protocol, are deleted. The Layer 3 features need to be reconfigured if required.

The ip binding vpn-instance command also allows you to bind an interface to a VPN instance with no enabled address families. After the binding, you cannot configure Layer 3 features, such as IP addresses and routing protocols, on the interface.

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.

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 and IPv6 related configurations on this interface are removed!
```

# Associate the 10GE1/0/1 interface with the VPN instance named **vrf1**.

```
<HUAWEI> system-view
[~HUAWEI] ip vpn-instance vrf1
[~HUAWEI-vpn-instance-vrf1] ipv4-family
[~HUAWEI-vpn-instance-vrf1-af-ipv4] route-distinguisher 100:1
[~HUAWEI-vpn-instance-vrf1-af-ipv4] quit
[*HUAWEI-vpn-instance-vrf1] quit
[*HUAWEI] interface 10ge 1/0/1
[*HUAWEI-10GE1/0/1] undo portswitch
[*HUAWEI-10GE1/0/1] ip binding vpn-instance vrf1
Info: All IPv4 and IPv6 related configurations on this interface are removed!
```

11.2.16 ip frr (VPN instance IPv4 address family 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

undo ip frr

Parameters

None

Views

VPN instance view, VPN instance IPv4 address family view

Default Level

2: Configuration level

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.

Prerequisites

The **route-distinguisher** command has been executed to set the RD of the VPN instance.

Precautions

After the **ip frr** command is run, the system automatically selects an inactive route as the backup of an active route.

NOTICE

The **ip frr** enables routes of different routing protocols to back up each other. A routing loop may occur during a switchover between routes. Therefore, exercise caution when using this command.

Example

# Enable IP FRR of a private network in the VPN instance.

```
<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] ip frr
```

11.2.17 ip import-rib vpn-instance

Function

The **ip import-rib vpn-instance** command enables a device to import routes in a VPN instance to the public network routing table.

The **undo ip import-rib vpn-instance** command restores the default setting.

By default, a device does not import routes in a VPN instance to the public network routing table.

Format

ip import-rib vpn-instance *vpn-instance-name* **protocol direct** [**route-policy** *route-policy-name*]

undo ip import-rib vpn-instance *vpn-instance-name* **protocol direct**

ip import-rib vpn-instance *vpn-instance-name* **protocol static** [**valid-route**] [**route-policy** *route-policy-name*]

undo ip import-rib vpn-instance *vpn-instance-name* **protocol static**

ip import-rib vpn-instance *vpn-instance-name* **protocol** { **isis** *process-id* | **ospf** *process-id* } [**valid-route**] [**route-policy** *route-policy-name*]

undo ip import-rib vpn-instance *vpn-instance-name* **protocol** { **isis** *process-id* | **ospf** *process-id* } [**valid-route**] [**route-policy** *route-policy-name*]

Parameters

Parameter	Description	Value
vpn-instance-name	Specifies the name of a VPN instance.	The value is a string of 1 to 31 case-sensitive characters except spaces. When double quotation marks are used to include the string, spaces are allowed in the string. The value _public_ is reserved and cannot be used as the VPN instance name.
protocol	Specifies a protocol type of routes to be imported to a public network routing table.	-
direct	Imports direct routes, excluding direct VLINK routes.	-
static	Imports static routes.	-
isis *process-id*	Imports IS-IS routes of the specified process. The *process-id* parameter specifies the IS-IS process ID.	The value is an integer ranging from 1 to 4294967295.
ospf *process-id*	Imports OSPF routes of the specified process. The *process-id* parameter specifies the OSPF process ID.	The value is an integer ranging from 1 to 4294967295.
route-policy *route-policy-name*	Specifies the Route-Policy filter to filter routes to be imported.	The name is a string of 1 to 200 case-sensitive characters except spaces. When double quotation marks are used to include the string, spaces are allowed in the string.
valid-route	Imports valid routes of a specified route type.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Users of a VPN instance can communicate with those of another VPN instance provided that the two VPN instances have matching VPN targets, but cannot communicate with public network users in a BGP/MPLS IP VPN scenario. To enable VPN users to communicate with public network users, you must configure route import between the VPN instance and public network instance. To enable a device to import IPv4 routes in a VPN instance to the public network IPv4 routing table, run the **ip import-rib vpn-instance** command.

Precautions

If you run the **ip import-rib vpn-instance** command on a device without the **valid-route** parameter, the device will import the optimal route of the specified type in the VPN instance to the corresponding public network IPv4 routing table. If the imported route is preferred in this routing table, the device will advertise the route to other devices and deliver the route to the public network IPv4 routing tables of the devices to guide traffic forwarding.

If you run the **ip import-rib vpn-instance** command with the **valid-route** parameter, the device will import valid routes of the specified type in the VPN instance to the corresponding public network IPv4 routing table. If the imported routes are preferred in this routing table, the device will advertise these routes to other devices and deliver these routes to the public network IPv4 routing tables of the devices to guide traffic forwarding.

Example

# Enable the device to import valid IS-IS routes in the VPN instance **vrf1** to the public network routing table.

```
<HUAWEI> system-view
[~HUAWEI] ip import-rib vpn-instance vrf1 protocol isis 1 valid-route
```

# Enable the device to import direct routes in the VPN instance **vrf1** to the public network routing table.

```
<HUAWEI> system-view
[~HUAWEI] ip import-rib vpn-instance vrf1 protocol direct
```

11.2.18 ip vpn-instance

Function

The **ip vpn-instance** command creates a VPN instance and displays the VPN instance view.

The **undo ip vpn-instance** command deletes a specified VPN instance.

By default, no VPN instance is configured.

Format

ip vpn-instance *vpn-instance-name*

undo ip vpn-instance *vpn-instance-name*

Parameters

Parameter	Description	Value
vpn-instance-name	Specifies the name of a VPN instance.	The value is a string of 1 to 31 case-sensitive characters except spaces. When double quotation marks are used to include the string, spaces are allowed in the string. The value _public_ is reserved and cannot be used as the VPN instance name.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To configure a VPN instance, run the **ip vpn-instance** command.

Precautions

After the **ip vpn-instance** command is run, a virtual routing and forwarding (VRF) table is created on the device and consumes resources on the device.

After the **undo ip vpn-instance** command is used to delete a VPN instance, all configurations of the 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 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 can 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 IPv4 or IPv6 address family of the VPN instance using the **vpn-target** command. The VPN target controls route learning between VPN instances.

- Bind the VPN instance to the PE or MCE interface connected to the VPN using the **ip binding vpn-instance** command. By binding an interface to a VPN instance, you can change the interface to a VPN interface. Packets entering this interface then are forwarded according to the forwarding information of the VPN instance.

Example

# Create a VPN instance named **vrf1**.

```
<HUAWEI> system-view
[~HUAWEI] ip vpn-instance vrf1
[*HUAWEI-vpn-instance-vrf1]
```

11.2.19 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 [**unicast**]

undo ipv4-family [**unicast**]

Parameters

Parameter	Description	Value
unicast	Displays the unicast address family view.	-

Views

VPN instance view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In BGP/MPLS IP VPN networking, after running the **ip vpn-instance** command to create a VPN instance, you can run the **ipv4-family** command to enable the IPv4 address family for the VPN instance 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.

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]
```

11.2.20 ipv6 frr (VPN instance IPv6 address family view)

Function

The **ipv6 frr** command enables IPv6 FRR of a private network in the VPN instance IPv6 address family view.

The **undo ipv6 frr** command disables IPv6 FRR of a private network in the VPN instance IPv6 address family view.

By default, IPv6 FRR of a private network is disabled in the VPN instance IPv6 address family view.

Format

ipv6 frr

undo ipv6 frr

Parameters

None

Views

VPN instance IPv6 address family view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When there are private network routes generated by multiple types of routing protocols in a VPN instance enabled with the IPv6 address family, the **ipv6 frr** command can be used to enable IPv6 FRR to immediately switch traffic among routes and ensure the normal forwarding of traffic if certain routes are faulty.

Prerequisites

The **ip vpn-instance** command has been executed to create a VPN instance

Configuration Impact

After the **ipv6 frr** command is run, the system automatically selects an inactive route as the backup of an active route.

Precautions

NOTICE

The **ipv6 frr** enables routes of different routing protocols to back up each other. A routing loop may occur during a switchover between routes. Therefore, exercise caution when using this command.

Example

# Enable IPv6 FRR of a private network in a VPN instance.

```
<HUAWEI> system-view
[~HUAWEI] ip vpn-instance vpn1
[*HUAWEI-vpn-instance-vpn1] ipv6-family
[*HUAWEI-vpn-instance-vpn1-af-ipv6] route-distinguisher 100:1
[*HUAWEI-vpn-instance-vpn1-af-ipv6] ipv6 frr
```

11.2.21 ipv6 import-rib vpn-instance

Function

The **ipv6 import-rib vpn-instance** command enables a device to import IPv6 routes in a VPN instance routing table to the public network IPv6 routing table.

The **undo ipv6 import-rib vpn-instance** command restores the default configuration.

By default, a device does not import IPv6 routes in a VPN instance routing table to the public network IPv6 routing table.

Format

ipv6 import-rib vpn-instance *vpn-instance-name* **protocol direct** [**route-policy** *route-policy-name*]

undo ipv6 import-rib vpn-instance *vpn-instance-name* **protocol direct**

ipv6 import-rib vpn-instance *vpn-instance-name* **protocol static** [**valid-route**] [**route-policy** *route-policy-name*]

undo ipv6 import-rib vpn-instance *vpn-instance-name* **protocol static**

ipv6 import-rib vpn-instance *vpn-instance-name* **protocol** { **isis** *process-id* | **ospfv3** *process-id* } [**valid-route**] [**route-policy** *route-policy-name*]

undo ipv6 import-rib vpn-instance *vpn-instance-name* **protocol** { **isis** *process-id* | **ospfv3** *process-id* } [**valid-route**] [**route-policy** *route-policy-name*]

Parameters

Parameter	Description	Value
vpn-instance-name	Specifies the name of a VPN instance.	The value is a string of 1 to 31 case-sensitive characters except spaces. When double quotation marks are used to include the string, spaces are allowed in the string. The value _public_ is reserved and cannot be used as the VPN instance name.
protocol	Specifies a protocol type of routes to be imported to the public network IPv6 routing table.	-
direct	Imports direct routes, excluding direct VLINK routes.	-
static	Imports static routes.	-
isis *process-id*	Imports IS-IS routes of the specified process. The *process-id* parameter specifies the process ID.	The value is an integer ranging from 1 to 4294967295.
ospfv3 *process-id*	Imports OSPFv3 routes of the specified process. The *process-id* parameter specifies the process ID.	The value is an integer ranging from 1 to 4294967295.
route-policy *route-policy-name*	Specifies a route-policy to filter routes to be imported.	The name is a string of 1 to 200 case-sensitive characters except spaces. When double quotation marks are used to include the string, spaces are allowed in the string.
valid-route	Imports only the valid routes of the specified route type.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In BGP/MPLS IPv6 VPN networking, IPv6 users of two VPNs with matching VPN targets can communicate, but IPv6 VPN users cannot communicate with IPv6 public network users. To enable IPv6 VPN users to communicate with IPv6 public network users, you must configure IPv6 route import between VPN and public network instances. To enable a device to import IPv6 routes from a VPN instance to the public network instance, run the **ipv6 import-rib vpn-instance** command.

Precautions

If you run the **ipv6 import-rib vpn-instance** command on a device without specifying the **valid-route** parameter, the device will import the optimal IPv6 route of the specified type from the specified VPN instance to the public network routing table. If the imported route is preferred in this routing table, the device will advertise the route to other devices and deliver the route to the IPv6 routing table to guide traffic forwarding.

If you run the **ipv6 import-rib vpn-instance** command with the **valid-route** parameter, the device will import the valid IPv6 routes of the specified type from the specified VPN instance to the public network instance routing table. If the imported routes are preferred in this routing table, the device will advertise these routes to other devices and deliver these routes to the IPv6 routing table to guide traffic forwarding.

Example

# Enable a device to import valid OSPFv3 routes of VPN instance **vrf1** to the public network IPv6 routing table.

```
<HUAWEI> system-view
[~HUAWEI] ipv6 import-rib vpn-instance vrf1 protocol ospfv3 1 valid-route
```

# Enable a device to import IPv6 direct routes of VPN instance **vrf1** to the public network IPv6 routing table.

```
<HUAWEI> system-view
[~HUAWEI] ipv6 import-rib vpn-instance vrf1 protocol direct
```

11.2.22 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 [**unicast**]

undo ipv6-family [**unicast**]

Parameters

Parameter	Description	Value
unicast	Displays the unicast address family view.	-

Views

VPN instance view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

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.

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]
```

11.2.23 peer soo

Function

The **peer soo** command configures the Site of Origin (SoO) attribute for an EBGP peer in a BGP VPN instance.

The **undo peer soo** command deletes the SoO.

By default, no SoO attribute is configured for an EBGP peer in a BGP VPN instance.

Format

peer { *group-name* | *ipv4-address* | *ipv6-address* } **soo** *site-of-origin*

undo peer { *group-name* | *ipv4-address* | *ipv6-address* } **soo**

Parameters

Parameter	Description	Value
group-name	Specifies the name of a BGP peer group.	The name is a string of 1 to 47 case-sensitive characters except spaces. When double quotation marks are used to include 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 value is a 32-digit hexadecimal number, in the format X:X:X:X:X:X:X:X.

Parameter	Description	Value
Site-of-origin	Specifies the SoO attribute, which is a BGP extended community attribute and can be expressed in any of the following formats: ● 2-byte AS number: 4-byte user-defined number, for example, 1:3. The AS number ranges from 0 to 65535. The user-defined number ranges from 0 to 4294967295. The AS number and the user-defined number cannot both be 0. That is, a SoO cannot be 0:0. ● IPv4-address: 2-byte user-defined number, for example, 192.168.122.15:1. The IP address ranges from 0.0.0.0 to 255.255.255.255. The user-defined number ranges from 0 to 65535. ● Integral 4-byte AS number:2-byte user-defined number, for example, 65537:3. An AS number ranges from 65536 to 4294967295. A user-defined number ranges from 0 to 65535. The AS number and user-defined number cannot be both 0s. That is, a SoO cannot be 0:0. ● 4-byte AS number in dotted notation:2-byte user-defined number, for example, 0.0:3 or 0.1:0. A 4-byte AS number in dotted notation is in the format of *x.y*, where *x* and *y* are integers that range from 0 to 65535 and from 0 to 65535, respectively. A user-defined number ranges from 0 to 65535. The AS number and user-defined number cannot be both 0s. That is, a SoO cannot be 0.0:0.	-

Views

BGP-VPN instance IPv4 address family view, BGP-VPN instance IPv6 address family view, BGP multi-instance VPN instance IPv4 address family view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In a BGP/MPLS IP VPN scenario, if the ASs to which two VPN sites belong use private AS numbers, the AS numbers of the two VPN sites may be the same. As a result, different sites of the same VPN cannot communicate. The **peer substitute-**

as command can be used to enable AS number substitution on PEs to address this problem.

Enabling AS number substitution will cause another problem. Several CEs at a VPN site may establish EBGP connections with different PEs of a BGP/MPLS IP VPN backbone network, and a routing protocol has been configured on the CEs. If AS number substitution is enabled on PEs, the AS numbers carried by VPN routes of this site will be replaced on the PEs. As a result, routes advertised from a CE to a PE may be re-advertised to this VPN site after the routes traverse the backbone network, causing a routing loop. The **peer soo** command can be run on the PEs to address this problem.

After the **peer soo** command is run on a PE to configure the SoO attribute for a specified CE, the PE adds the attribute to a route sent from the CE and advertises the route to the remote PE. The remote PE checks the SoO attribute of the route before sending it to its attached CE. If the SoO attribute is the same as the local SoO attribute on the remote PE, the remote PE does not send the route to its attached CE, preventing a routing loop in a VPN site.

Precautions

The **peer soo** command is used only in the scenarios where PEs and CEs establish EBGP peer relationships.

Example

# Configure the SoO attribute for EBGP peers in a BGP VPN instance.

```
<HUAWEI> system-view
[~HUAWEI] bgp 100
[*HUAWEI-bgp] ipv4-family vpn-instance vpna
[*HUAWEI-bgp-vpna] peer 192.168.15.2 soo 10.2.2.2:45
```

11.2.24 peer substitute-as

Function

The **peer substitute-as** command enables AS number substitution. This command enables a device to replace the AS number of the peer specified in the AS_Path attribute with the local AS number.

The **undo peer substitute-as** command disables AS number substitution.

By default, AS number substitution is disabled.

Format

peer { *group-name* | *ipv4-address* | *ipv6-address* } **substitute-as**

undo peer { *group-name* | *ipv4-address* | *ipv6-address* } **substitute-as**

Parameters

Parameter	Description	Value
group-name	Specifies the name of a peer group.	The name is a string of 1 to 47 case-sensitive characters except spaces. When double quotation marks are used to include the string, spaces are allowed in the string.
ipv4-address	Specifies the IPv4 address of a peer.	It is in dotted decimal notation.
ipv6-address	Specifies the IPv6 address of a peer.	The address is in the format of X:X:X:X:X:X:X:X.

Views

BGP-VPN instance IPv4 address family view, BGP-VPN instance IPv6 address family view, BGP-IPv4 unicast address family view, BGP-IPv6 unicast address family view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In a BGP/MPLS IP VPN scenario, if the ASs to which two VPN sites belong use private AS numbers, the AS numbers of the two VPN sites may be the same. 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.

On a BGP public network, two devices have the same AS number and the same EBGP peer. After one of the two devices learns a route of the other device from the EBGP peer, the route is discarded because it carries an AS number that is the same as the local one. To address this problem, run the **peer substitute-as** command on the EBGP peer.

Pre-configuration Tasks

Run the **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
[*HUAWEI-bgp-vpn1] peer 10.1.1.2 as-number 200
[*HUAWEI-bgp-vpn1] peer 10.1.1.2 substitute-as
```

11.2.25 policy vpn-target

Function

The **policy vpn-target** command enables a device to perform VPN target-based filtering for received VPN routes or label blocks.

The **undo policy vpn-target** command disables a device from performing VPN target-based filtering for received VPN routes or label blocks.

By default, a device performs VPN target-based filtering for received VPN routes or label blocks.

Format

policy vpn-target

undo policy vpn-target

Parameters

None

Views

BGP-VPNv4 address family view, BGP-VPNv6 address family view, BGP-EVPN address family view, BGP multi-instance EVPN address family view, L2VPN-AD address family view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

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.

Precautions

Running the **undo policy vpn-target** command allows all VPN routes or label blocks from PEs to be 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
```

11.2.26 prefix limit

Function

The **prefix limit** command sets a limit on the maximum number of prefixes supported in the existing VPN instance address family, preventing the PE from importing excessive VPN route prefixes.

The **undo prefix limit** command restores the default setting.

By default, the maximum number of VPN route prefixes is not limited.

Format

prefix limit *number* { *alert-percent* [**route-unchanged**] | **simply-alert** }

undo prefix limit

Parameters

Parameter	Description	Value
number	Specifies the maximum number of prefixes supported in the VPN instance address family.	The value is an integer ranging from 1 to 4294967295.
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.

Parameter	Description	Value
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, 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

The **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.

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
```

11.2.27 route-distinguisher

Function

The **route-distinguisher** command configures a route distinguisher (RD) for a VPN instance address family.

The **undo route-distinguisher** command deletes the RD configuration in a specified VPN instance address family.

By default, no RD is configured for the VPN instance address family.

Format

route-distinguisher *route-distinguisher*

undo 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. The 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.

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.

RDs cannot be modified but can be deleted after being configured. After an RD is deleted, all configurations in the VPN instance IPv4 address family or the IPv6 address family of the corresponding VPN instance will be deleted.

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
```

11.2.28 routing-table limit

Function

The **routing-table limit** command sets the maximum number of routes that the current VPN instance address family supports.

The **undo routing-table limit** command restores the maximum number of routes that the current VPN instance address family can support to the default setting.

By default, there is no limit on the maximum number of routes that the current VPN instance address family can support, but the total number of private network and public network routes on a device cannot exceed the allowed maximum number of unicast routes.

Format

routing-table limit *number* { *alert-percent* | **simply-alert** }

undo routing-table limit

Parameters

Parameter	Description	Value
number	Specifies the maximum number of routes supported by a VPN instance.	The value is an integer that ranges from 1 to 4294967295.

Parameter	Description	Value
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, VPN instance IPv6 address family view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To prevent excessive routes from being imported into the routing table of the IPv4 or IPv6 address family of a VPN instance, run the **routing-table limit** command to limit the maximum number of routes in the routing table. If the number of routes in the routing table of the IPv4 or IPv6 address family of a VPN instance exceeds the upper threshold, the excessive routes cannot be advertised to the peer. After the **undo routing-table limit** command is run, the excessive routes will be added to the VPN instance's routing table.

Precautions

If the **simply-alert** parameter is specified and the number of routes exceeds the upper threshold, only an alarm is generated, and the excessive routes are still added to the routing table.

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
```

11.2.29 rr-filter

Function

The **rr-filter** command creates a reflection policy for an RR.

The **undo rr-filter** command cancels the configuration.

By default, no reflection policy is created for an RR.

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 an RR group. You can specify only one extended community filter each time.	The value is an integer in the range from 1 to 399.
extcomm-filter-name	Specifies the name of the extended community filter supported by an RR group. You can specify only one extended community filter each time.	The extcomm-filter-name must already exist.

Views

BGP-VPNv4 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 whose RT extended community attribute meets the matching rules can be reflected. This allows load balancing among RRs.

Example

# Create an RR group, and enable the automatic filtering for VPNv4 route update packets on the outbound interface. The group should be created on the basis of the permitted RT extended community attributes.

```
<HUAWEI> system-view
[~HUAWEI] bgp 100
[*HUAWEI-bgp] ipv4-family vpnv4
[*HUAWEI-bgp-af-vpnv4] rr-filter 10
```

11.2.30 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** *trap-name*]

undo snmp-agent trap enable feature-name l3vpn [**trap-name** *trap-name*]

Parameters

Parameter	Description	Value
trap-name *trap-name*	Enables the traps of L3VPN events of specified types.	The traps are as follows: ● hwipv4routeexceed ● hwipv4routeexceedclear ● hwipv4routethresholdexceed ● hwipv4routethresholdexceedclear ● hwipv6routeexceed ● hwipv6routeexceedclear ● hwipv6routethresholdexceed ● hwipv6routethresholdexceedclear ● hwl3vpnvrfroutemidthreshcleared ● hwl3vpnvrfv6down ● hwl3vpnvrfv6up ● mplsl3vpnnumvrfroutemaxthreshcleared ● mplsl3vpnvrfdown ● mplsl3vpnvrfnumvrfroutemaxthreshexceeded ● mplsl3vpnvrfroutemidthreshexceeded ● mplsl3vpnvrfup

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 mplsl3vpnvrfdown
```

# 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 mplsl3vpnvrfdown
```

11.2.31 supernet label-route advertise

Function

The **supernet label-route advertise disable** command disables a BGP device from advertising BGP supernet labeled routes.

The **undo supernet label-route advertise disable** or **supernet label-route advertise enable** command restores the default configuration.

By default, BGP supernet labeled routes can be preferentially selected and advertised.

Format

supernet label-route advertise disable

supernet label-route advertise enable

undo supernet label-route advertise disable

Parameters

None

Views

BGP view, BGP-IPv4 unicast address family view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A BGP supernet route has the same destination address and next hop address or has a more detailed destination address than the next hop address. Any route that meets one of the following conditions is a BGP supernet route.

- If you perform bitwise AND operations on the destination address mask with the destination address and next hop address, respectively, the calculated network addresses are the same, and the destination address mask is greater than or equal to the next hop address mask.

- If you perform bitwise AND operations on the destination address mask with the destination address and next hop address, respectively, the calculated network addresses are different. However, if you perform bitwise AND operations on the next hop address mask with the destination address and next hop address, respectively, the calculated network addresses are the same.

For example, the route destined for 10.6.6.6 in the following command output is a BGP supernet route.

```
<HUAWEI> display bgp routing-table
 BGP Local router ID is 1.1.1.2
  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
```

11.2.32 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** | **none** }

undo tunnel-protocol

Parameters

Parameter	Description	Value
gre	Indicates that the GRE tunnel protocol is configured on a tunnel interface.	-
none	Indicates that no tunnel protocol is configured on a tunnel interface.	-

Views

Tunnel interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

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

Precautions

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

Example

# Set the tunnel encapsulation mode of Tunnel2 to gre.

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

11.2.33 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**] [**evpn**]

undo vpn-target { **all** | *vpn-target* &<1-8> [**both** | **export-extcommunity** | **import-extcommunity**] [**evpn**] }

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 0s. That is, the 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. The AS number ranges from 65536 to 4294967295. The user-defined number ranges from 0 to 65535. The AS number and user-defined number cannot both be 0s. That is, the 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. The user-defined number also ranges from 0 to 65535. The AS number and user-defined number cannot both be 0s. That is, the 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**, and **import-extcommunity** is specified, **both** is adopted by default.	-

Parameter	Description	Value
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.	-
evpn	Specifies a VPN target for routes to be installed into the routing table of an EVPN instance.	-
all	Delete all the VPN targets of the VPN instance address family.	-

Views

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

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If a VPN instance is configured on a PE, the **vpn-target** command must be used to configure a VPN target for the address family of the VPN instance.

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 or VPNv6 route to be advertised to a remote MP-BGP peer. After receiving a VPNv4 or VPNv6 route, the MP-BGP peer compares the received export VPN target with the local import VPN target to determine whether the VPNv4 or VPNv6 route can be added to the routing table of the local VPN instance address family.

After **evpn** is configured, routes of a VPN instance can be added into the routing table of the EVPN instance configured with a matching VPN target.

Prerequisites

The RD of the VPN instance has been configured using the **route-distinguisher** command.

The **evpn** parameter can be specified only after the **evpn-overlay enable** command has been run.

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 using the **vpn-target** command.

After a VPN target is configured for the VPN instance address family, only the routes that match the VPN target will be accepted by the VPN instance address family

If all the VPN targets of the VPN instance address family are deleted using the **undo vpn-target** command, all routes learned by the VPN instance address family through route crossing will be deleted.

Multiple VPN targets can be configured for the VPN instance address family. 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, 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 VPNv6 routes matches the import VPN target of the local VPN instance address family, 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
```

11.2.34 vpn frr

Function

The **vpn frr** command enables VPN FRR.

The **undo vpn frr** command disables VPN FRR.

By default, VPN FRR is disabled.

Format

vpn frr

undo vpn frr

Parameters

None

Views

VPN instance view, VPN instance IPv4 address family view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If a PE is connected to two other PEs, you can run the **vpn frr** command in the VPN instance IPv4 address family view of the PE to enable VPN FRR, which improves network reliability. After VPN FRR is configured, traffic is automatically switched to the secondary LSP immediately after the primary LSP from the local PE to the remote PE becomes faulty.

Prerequisites

The RD of the VPN instance has been set using the **route-distinguisher** command.

Example

# Enable VPN FRR in the VPN instance IPv4 address family view.

```
<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] vpn frr
```