MPLS

QSR-1920, QSR-2920, QSR-3920

Оглавление

1. MPLS BASIS

1.1. Overview

MPLS (Multiprotocol Label Switching) integrates the simplicity of the L2 switching and the flexibility of the L3 route selection, providing the connection-oriented feature for the connectionless IP network.

Compared with the traditional IP network, MPLS has the following technical advantages:

- Perform the packet forwarding based on the label, simplify the forwarding mechanism, and improve the forwarding efficiency
- Expand the service functions flexibly by bringing in the label, realizing the route selection, traffic engineering, QoS, VPN and other functions
- The label itself does not have the specific meaning and it can map the target IP address, fiber channel, wave length, even the VC channel in SDH/SONET

The following describes some important basic concepts of MPLS.

1. FEC

FEC (Forwarding Equivalence Class) indicates the packet set of complying with the same forwarding path in the network (the destination addresses of the packets can be different). The packets of the same FEC are processed by the LSR in the same mode during the forwarding. The ingress LSR of the MPLS searches for the corresponding label value according to FEC for the IP packet entering the MPLS domain, and encapsulates in the packet, forming the label packet and transmitting in the MPLS network.

2. Label

In the MPLS network, the MPLS packet is forwarded according to the label varied by the packet. The label is inserted between the L3 and L2 packet headers, called MPLS label header. The format is shown in Figure 1-1:

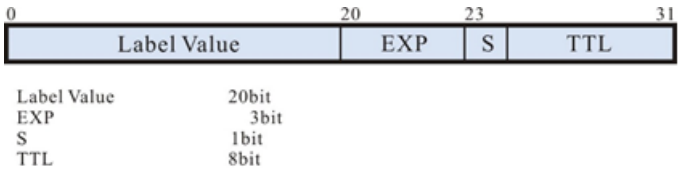

Figure 1-1 MPLS label structure

One MPLS packet can bear multiple label headers and this structure is called label stack. The labels are organized according to the “Last in, first out” mode. The outermost label is called stack top label and the innermost label is called stack bottom label. Each label consists of the following fields:

- TTL: 8 bits, with the same functions the TTL field in the IP header
- Stack bottom (S): 1bit, the value 1 indicates that the corresponding label is the last label in the label stack (stack bottom); the value 0 indicates all other labels except for the stack bottom label.
- Service-class information: 3bit, reserved, not defined in the protocol, usually used as the service level.
- Label Value: 20bit, used to identify FEC. The label value 0-15 are the reserved label value. The specific meanings are as follows:

Table 1-1 The meaning of the reserved label value

Label Value	Meaning
0	IPv4 explicit null label
1	Router alarm label
2	IPv6 explicit null label
3	Implicit empty label
4 - 15	Reserved

3. Label switching router

LSR (Label Switching Router) indicates the device supporting the MPLS service. It can distribute the label and receive and transmit the packet with label on the data link.

4. LER

LER (Label Edge Router) indicates the LSR connecting other network at the MPLS network edge.

5. LSP

LSP (Label Switched Path) indicates the forwarding path of the packets of the same FEC in the MPLS network.

6. MPLS network node

The MPLS network includes the following important network nodes:

- Ingress node: The ingress LER of the MPLS network, encapsulating the label for the packet entering the MPLS network
- Transit node: The internal LSR of the MPLS network, search for the MPLS forwarding table according to the label, execute the label operation, and send the packet to the egress LER along the LSP
- Egress node: The egress LER of the MPLS network, responsible for removing the label and sending the packet to the destination network

7. Label forwarding table

LFIB (Label Forwarding Information Base), similar to the EIB of IP, used to forward the MPLS packet, including the following types:

- NHLFE (Next Hop Label Forwarding Entry): Record the MPLS forwarding operation mode and forwarding information
- FTN (FEC to NHLFE): Used to search for FTN according to the FEC of the packet at the Ingress node and map to the NHLFE
- ILM (Incoming Label Map): Used to search for ILM according to the incoming label and map to the NHLFE

1.2. MPLS Basis Function Configuration

Table 1-2 MPLS basis function configuration list

Configuration Task	
Configure the MPLS basic functions	Enable the global MPLS function
	Enable the MPLS function on the interface
	Configure the label distributing range
Configure the MPLS forwarding control	Configure the interface MPLS MTU
	Configure the packet load mode
	Configure the packet TTL copy mode
	Configure the packet TTL timeout processing mode

1.2.1. Configure MPLS Basic Functions

On the router taking part in the MPLS forwarding, it is necessary to enable the global and interface MPLS function.

Configuration Condition

Before configuring the MPLS basic functions, first complete the following tasks:

- Configure the link-layer protocol, ensuring the normal communication of the link layer
- Configure the network-later address of the interface, making the neighboring network node reachable at the network layer
- Configure the static route or IGP protocol, ensuring the LSRs communication with each other at the network layer

Enable Global MPLS Function

Table 1-3 Enable the global MPLS function

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enable the global MPLS function	**mpls ip**	Mandatory By default, the MPLS function is not enabled.

Enable Interface MPLS Function

Table 1-4 Enable the interface MPLS function

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the interface configuration mode	**interface** *interface_name*	-
Enable the interface MPLS function	**mpls ip**	Mandatory By default, the interface MPLS function is not enabled.

Configure Label Distributing Range

Table 1-5 Configure the label distributing range

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Configure the range of the local distributing label	**mpls label range** *min-label max-label*	Optional By default, the range of the permitted distributed label values is 24000~1048575.

Caution:

- Usually, it is not necessary to configure the range of the local distributed labels. If configuring the function after configuring the protocol of distributing the label resource (such as LDP and BGP), it is necessary to save and restart the device.

1.2.2. Configure MPLS Forwarding Control

Configuration Condition

Before configuring the MPLS forwarding control, complete the following task:

- Enable the MPLS basic functions globally and on the interface, ensuring that the MPLS packet can be received and sent.

Configure Interface MPLS MTU

In the MPLS network, the length of the packet encapsulated with the MPLS label may exceed the egress interface MTU and as a result, the packet needs to execute the fragment processing or be dropped. Therefore, define MPLS MTU and compare the length of the packet encapsulated with the MPLS label with the MPLS MTU of the egress interface. According to whether the interface is configured with MPLS MTU, there are the following processing actions:

- The egress interface of the packet is configured with MPLS MTU. If the ingress packet is the IP packet, that is, IP to MPLS forwarding, and the length of the packet being encapsulated with the MPLS label is larger than the MPLS MTU of the egress interface, fragment according to the interface MPLS MTU (not set DF bit) or send the error packet with unreachable ICMP destination (set the DF bit). If the ingress packet is the MPLS packet, that is, MPLS to MPLS forwarding, and the length of the packet is larger than the MPLS MTU of the egress interface, drop the packet.
- The egress interface of the packet is not configured with MPLS MTU. If the ingress packet is the IP packet, that is, IP to MPLS forwarding, and the length of the packet being encapsulated with the MPLS label is larger than the MTU of the egress interface, fragment according to the interface MTU (not set DF bit) or send the error packet with unreachable ICMP destination (set the DF bit). If the ingress packet is the MPLS packet, that is, MPLS to MPLS forwarding, directly forward no matter whether the packet length is larger than the egress interface MTU.

Table 1-6 Configure the interface MPLS MTU

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the specified interface	**interface** *interface_name*	-
Configure the interface MPLS MTU	**mpls mtu** *mtu-size*	Mandatory By default, the interface is not configured with MPLS MTU.

Note:

- The minimum value of the MPLS MTU configured on the interface is 64 bytes. For different interface types, the maximum value may be different and it is the maximum link MTU value supported by the current interface.
- The MPLS MTU configuration on the interface is valid only for the egress MPLS packet of the interface, but not valid for the egress IP packet of the interface.
- If the ingress packet is the IP packet, that is, IP to MPLS forwarding and when fragmenting according to the MPLS MTU of the egress interface, first fragment the IP packet (the fragment size is MPLS MTU value minus the length of the label stack), and then encapsulate the MPLS label stack for each fragment and forward.

Configure Packet Load Mode

In the MPLS network, you can use the command to set the multi-path packet load forwarding mode. There are two modes:

- Per-packet load mode: The packet is forwarded from the load path. The number of the packets forwarded from the load paths are basically the same.
- Per-label load mode: Select the load path according to the ingress label of the packet. The packets with the same label select the same load path to forward.

Table 1-7 Configure the packet load mode

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Configure the load mode of the MPLS packet	**mpls load-balancing** { **per-label** | **per-packet** }	Optional By default, adopt the per-label load mode to forward.

Note:

- When adopting the per-label load mode and if the packet has multiple layers of ingress labels, all ingress labels serve as the evidence of selecting the load path.
- The **mpls load-balancing** command is valid only when the ingress packet is the MPLS packet. If the ingress packet is IP packet, forward according to the IP load mode.

Configure Packet TTL Copy Mode

When the IP packet encapsulates the label at the Ingress node of the MPLS network, the system reduce the TTL value of the IP packet by 1 and copy to the TTL field of the MPLS label by default. The user also can configure the command to set the TTL field of the MPLS label to 255, but do not copy the TTL value of the IP packet any more.

Table 1-8 Configure the TTL copy mode of the packet

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Configure the TTL copy mode of the MPLS packet to not copy the TTL value in the IP packet	**no mpls ttl-propagate** [**forwarded** | **local**]	Optional By default, the forward packet and local sent packet reduce the TTL value in the IP packet by 1 and copy to the TTL field of the MPLS label.

Configure Packet TTL Timeout Processing Mode

When the LSR receives the MPLS packet with TTL 1, the LSR will generate the TTL timeout message of ICMP. There are two modes of LSR returning the ICMP timeout message to the sender of the packet:

- Forward the ICMP message along the previous LSP. At the Egress node, search for the route of the packet sender and return the ICMP message to the packet sender.
- On the LSR device discovering the TTL timeout, query the route of the packet sender and return the ICMP message to the packet sender.

You can configure the label layers via the **mpls ttl-expiration** command. After discovering the TTL timeout of the MPLS packet, compare the ingress label layers with the configured label

layers to determine the sending mode of the ICMP message. If the layers of the ingress labels do not exceed the configured label layers, adopt the second mode to return the ICMP message to the packet sender. Otherwise, adopt the first mode.

Table 1-9 Configure the packet TTL timeout processing mode

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Configure the label layers processed by the packet TTL timeout	**mpls ttl-expiration** *labels-num*	Optional By default, the label layers processed by the packet TTL timeout is 1.

1.2.3. MPLS Basis Monitoring and Maintaining

Table 1-10 MPLS basis monitoring and maintaining

Command	Description
clear mpls forwarding-table statistics	Clear the packet statistics of the MPLS service
show mpls forwarding-table ilm [*A.B.C.D* [*mask*]] | **in-label** *in-label* | **ipv4** | **sr** | **mcast** [*in-label*] | **vrf** *vrf-name*] [**detail**]	Display the ILM forwarding table information
show mpls forwarding-table statistics { **packet** | **record** }	Display the statistics information of the MPLS forwarding packet and the statistics of various types of the forwarding tables
show mpls forwarding-table tunnel	Display the forwarding table information of the MPLS TE tunnel
show mpls interface [*interface_name*] **statistics**	Display the information about the interface configured with the MPLS function
show mpls label range	Display the label distributing range
show mpls label used-block-data [**detail**]	Display the MPLS label block distributing information

2. MPLS LDP

2.1. Overview

LDP (Label Distribution Protocol) is one basic signaling protocol of MPLS, used to distribute and advertise the label and set up the LSP (Label Switching Path) dynamically.

Besides distributing the label, LDP also has some features:

- Support the label filter: Adopt the ACL to advertise and receive the label selectively, so as to save the resources and reduce the network load.
- Support loopback detection: Adopt he loopback detection to avoid the LSP loop.
- Support the MD5 authentication: Improve the security of the information exchange between LSRs
- Support the GR capability: When the device control plane fails, the data transmission is not interrupted.
- Support the BFD linkage: Realize the fast convergence of the LDP protocol via the BFD fast detection.

2.2. MPLS LDP Function Configuration

Table 2-1 LDP function configuration list

Configuration Task	
Configure the LDP basic function	Enable the LDP IPv4
Configure the LDP neighbor parameters	Configure the direct-connected session parameters
	Configure the remote session parameters
Configure the LDP MD5 authentication	Configure the LDP MD5 authentication
Configure the LDP control attributes	Configure the label accept filter
	Configure the label advertise filter
	Configure the label re-advertise
	Configure the PHP feature

Configuration Task	
Configure the LDP control attributes	Configure the loopback detection
	Configure the session re-connection
Configure LDP GR	Configure LDP GR
Configure the LDP to link with BFD	Configure the LDP to link with the BFD

2.2.1. Configure LDP Basic Functions

Configuration Condition

Before configuring the LDP basic functions, first complete the following tasks:

- Configure the link layer protocol, ensuring the normal communication of the link layer
- Configure the network layer address of the interface, making the neighbor network nodes reachable at the network layer
- Configure the static route or IGP protocol, ensuring that the LSRs can communicate with each other at the network layer
- Enable the MPLS basic functions on the interface and globally, ensuring that the MPLS packet can be received and sent.

Enable the LDP IPv4

Table 2-2 Enable the LDP protocol

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enable the LDP globally and enter the LDP configuration mode	**mpls ldp**	Mandatory By default, do not enable the LDP protocol globally. After enabling LDP globally, LDP IPv4 will be auto enabled globally.
Exit the LDP configuration mode	**exit**	-

Step	Command	Description
Enter the interface configuration mode	**interface** *interface-name*	-
Enable the LDP IPv4 on the interface	**mpls ldp**	Mandatory By default, the interface does not enable the LDP IPv4.

2.2.2. Configure LDP Neighbor Parameters

Configuration Condition

Before configuring the LDP neighbor parameters, first complete the following tasks:

- Configure the LDP basic functions

Configure Direct-connected Session Parameters

The session set up between the direct-connected peers is called LDP direct-connected session.

Table 2-3 Configure the direct-connected session parameters

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the LDP configuration mode	**mpls ldp**	-
Configure Router ID	**router-id** *ip-address*	Mandatory By default, select the interface IPv4 address of the local device, first selecting the loopback port IPv4 address.
Enter the LDP IPv4 address family configuration mode	**address-family ipv4**	-

Step	Command	Description
Configure the LDP IPv4 transmission address	**transport-address** *ip-address*	Optional By default, first select the Router ID as the LDP IPv4 transmission address.
Exit the LDP IPv4 address family configuration mode	**exit**	-
Configure the interval of sending the Keepalive message	**keepalive interval** *value*	Optional The default value is 60s and the value range is 1-65535s.
Configure the keepalive message timeout	**keepalive timeout** *value*	Optional The default value is 180s and the value range is 1-65535s.
Configure the interval of sending the link Hello	**discovery hello interval** *value*	Optional The default value is 5s and the value range is 1-65535s.
Configure the keepalive timer timeout of the link Hello	**discovery hello holdtime** *value*	Optional The default value is 15s and the value range is 1-65535s.
Exit the LDP configuration mode	**exit**	-
Enter the interface mode	**interface** *interface-name*	-
Configure the interval of sending the interface link Hello	**mpls ldp discovery hello interval** *value*	Optional The default value is 5s and the value range is 1-65535s.

Step	Command	Description
Configure the keepalive timer timeout of the interface link Hello	**mpls ldp discovery hello holdtime** *value*	Optional The default value is 15s and the value range is 1-65535s.

Note:

- To set up the LDP session between the peers, it is necessary to ensure that the LDP protocol is enabled on two peers.
- Before setting up a session with the direct-connected peer, the user needs to ensure that the transmission address route from the local transmission address to the peer transmission address is reachable. Otherwise, the session connection cannot be set up.
- Modifying Router ID or transmission address will cause the re-setup of the session. Therefore, it is suggested to modify Router ID or transmission address carefully.
- In the LDP IPv6 single stack environment, it is necessary to manually configure the router ID of LDP and ensure that it is unique in the MPLS domain. The input form is still the IPv4 address in dotted decimal form, but it is independent of any IPv4 address of the machine.
- When the system automatically selects the local LDP IPv4 transmission address, the router ID is preferred. If the router ID address is unavailable, the IPv4 address of loopback interface is preferred. If there is no IPv4 address of loopback interface available, select the available IPv4 address of other interfaces.
- The sending interval of the link Hello and keepalive time can be configured globally and also can be configured on the interface. When being configured globally, but not configured on the interface, the sending interval and keepalibe time of the interface link Hello adopt the global configured time. When being configured on the interface and globally, the sending interval and keepalive time of the interface link Hello adopt the configured time on the interface.

Configure Remote Session Parameters

The session set up with the target peer is called LDP remote session. The LDP remote session is mainly applied to Martini MPLS L2VPN and Martini VPLS. Currently, only LDP IPv4 supports the remote session.

Table 2-4 Configure the remote session parameters

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the LDP configuration mode	**mpls ldp**	-

Step	Command	Description
Configure Router ID	**router-id** *ip-address*	Optional By default, select the interface IPv4 address of the local device, and the IPv4 address of the looback port is preferred.
Enter the LDP IPv4 address family configuration mode	**address-family ipv4**	-
Create the LDP IPv4 target peer	**targeted-peer** *peer-address*	Mandatory By default, do not create the target peer.
Configure the LDP IPv4 transmission address	**transport-address** *ip-address*	Optional By default, first select the Router ID as the LDP IPv4 transmission address.
Exit the LDP IPv4 address family configuration mode	**exit**	-
Configure the interval of sending the Keepalive message	**keepalive interval** *value*	Optional The default value is 60s and the value range is 1-65535s.
Configure the keepalive timer timeout of the Keepalive message	**keepalive timeout** *value*	Optional The default value is 180s and the value range is 1-65535s.
Configure the interval of sending the target Hello	**discovery targeted-hello interval** *value*	Optional The default value is 10s and the value range is 1-65535s.

Step	Command	Description
Configure the keepalive timer timeout of the target Hello	**discovery targeted-hello holdtime** *value*	Optional The default value is 90s and the value range is 1-65535s.

Note:

- The configured sending interval of the Keepalive message and the timeout of the keepalive timer are applicable to the direct-connected session and remote session.
- The configured router ID and transmission address are also applicable to the direct-connected session and remote session.
- Before setting up the session with the target peer, the user needs to ensure that the address route to the peer is reachable and also needs to confirm that the target peer to the local end is also created at the peer. Otherwise, the remote session cannot be set up.

2.2.3. Configure LDP MD5 Authentication

Configuration Condition

Before configuring the LDP neighbor parameters, complete the following tasks:

- Configure the LDP basic functions

Configure LDP MD5 Authentication

To improve the security of the LDP session, the LDP session based on the TCP connection supports configuring the MD5 authentication. The session can be set up only when the local and the peer passwords are consistent.

Table 2-5 Configure LDP MD5 authentication

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the LDP configuration mode	**mpls ldp**	-
Enter the LDP IPv4 address family configuration mode	**address-family ipv4**	-

Step	Command	Description
Configure the LDP IPv4 MD5 authentication	**peer** *peer-ipv4-address* **password** [**0** | **7**] *string*	Mandatory By default, do not configure the LDP IPv4 MD5 authentication password.
Exit the LDP IPv4 address family configuration mode	**exit**	-

2.2.4. Configure LDP Control Attribute

Configuration Condition

Before configuring the LDP control attribute, first complete the following task:

- Configure the LDP basic functions

Configure Label Accept Filter

The label accept filter is used to filter the labels received from the FEC downstream, only accepting the labels of the FEC passing the ACL check. The function can reduce the scale of the MPLS forwarding table. To configure the label accept filter, you need to first configure the ACL, and then adopt the label accept filter command to reference in the LDP.

Besides, because most MPLS networks only need the labels of the IPv4 FEC with the 32-bit mask length, LDP divides FEC to 32-bit mask and non-32-bit mask according to the mask length. By default, the system only accepts the labels of the FEC with the 32-bit mask length. To reduce the control complexity, provide the separate command to control the 32-bit prefix and non-32-bit prefix.

Table 2-6 Configure the label accept filter

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the LDP configuration mode	**mpls ldp**	-
Enter the LDP IPv4 address family configuration mode	**address-family ipv4**	-

Step	Command	Description
Configure the IPv4 label accept filter	**accept-labels for** *ipv4-prefix-accesslist-name*	Optional By default, do not configure the IPv4 label accept filter.
Configure only accepting the labels of the IPv4 FEC with 32-bit mask length	**accept-labels for 32bit-mask-fec-only**	Optional By default, only accept the labels of the IPv4 FEC with the 32-bit mask length.
Exit the LDP IPv4 address family configuration mode	**exit**	-

Note:

- The ACL matching the FEC is independent of whether the FEC tag mapping is based on the session reception of the corresponding address family.
- The labels of the FEC not passing the ACL filter will not be installed with FTN, but still saves and installs ILM.
- By default, only accept the labels of the IPv4 FEC with the 32-bit mask length, so usually use the no format to configure accepting the labels of the FEC with any mask length.
- The command accept-labels for 32bit-mask-fec-only/no accept-labels for 32bit-mask-fec-only and the accept-labels for *ipv4-prefix-accesslist-name* command can be configured at the same time. If the accept-labels for 32bit-mask-fec-only command is configured (the default configuration of the system), the FTN of all IPv4 FECs with 32-bit mask passing the ACL filter in the accept-labels for *ipv4-prefix-accesslist-name* command can be installed, but the FTN of all IPv4 FECs with non-32-bit mask will not be installed (even the IPv4 FEC with non-32-bit mask passing the filter of the ACL in the accept-labels for *ipv4-prefix-accesslist-name* command). If the command is configured, the FTN of all IPv4 FECs passing the filter of the ACL in the accept-labels for *ipv4-prefix-accesslist-name*command will be installed.

Configure Label Advertise Filter

The label advertise filter is used to filter the advertised labels. The function can prevent the LSR from advertising lots of labels, so as to reduce the network load. To configure the label advertise filter, you need to first configure the ACL, and then adopt the label advertise filter command to reference in the LDP.

Table 2-7 Configure the label advertise filter

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-

Step	Command	Description
Enter the LDP configuration mode	**mpls ldp**	-
Enter the LDP IPv4 address family configuration mode	**address-family ipv4**	-
Configure the IPv4 label advertise filter	**advertise-labels for** *ipv4-prefix-accesslist-name* **to** *ipv4-peer-accesslist-name*	Optional By default, do not configure the IPv4 label advertise filter.
Configure advertising the labels of some IPv4 FECs to all upstream devices	**advertise-labels for** *ipv4-prefix-accesslist-name* **to any**	Optional By default, do not configure the IPv4 label advertise filter.
Configure not advertising the IPv4 label to any upstream device	**advertise-labels for any to none**	Optional By default, do not configure not advertising the IPv4 label to any upstream device.
Configure only advertising the label of the IPv4 FEC with the 32-bit mask length	**advertise-labels for 32bit-mask-fec-only**	Optional By default, only advertise the label of the IPv4 FEC with the 32-bit mask length.
Exit the LDP IPv4 address family configuration mode	**exit**	-

Note:

- The ACL matching the FEC is independent of whether the FEC-tag mapping is advertised based on the session of the corresponding address family.
- When matching the ACL of the peer, it is compared with the LDP router ID of the peer.
- By default, LDP only advertises the labels of the FEC with the 32/128-bit mask length, so usually use the no format to configure advertising the labels of the FEC with any mask length to the upstream device.
- In the LDP IPv4 address family configuration mode, the **advertise-labels for any to none** command and the **advertise-labels for** *ipv4-prefix-accesslist-name* **to any** command can be seen as the special format of the **advertise-labels** *ipv4-prefix-accesslist-name* **to** *ipv4-peer-accesslist-name* command. **any** indicates permit any, and **none** indicates deny any. The three commands all can be called passing the ACL control

LDP IPv4 label advertising and can be configured with the **advertise-labels for 32bit-mask-fec-only** command.

- If the **advertise-labels for 32bit-mask-fec-only** command is configured (by default), all IPv4 FECs with non-32-bit mask refuse advertising the label, while the IPv4 FEC with the 32-bit mask performs the label advertising according to the ACL check result. If the **no advertise-labels for 32bit-mask-fec-only** command is configured, all IPv4 FECs with any mask length perform the label advertising according to the ACL check result.

Configure Label Re-advertising

After configuring the label advertising, the LDP periodically re-advertises all labels to the upstream neighbor.

Table 2-8 Configure the label re-advertising

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the LDP configuration mode	**mpls ldp**	-
Configure the label re-advertising	**du-readvertise**	Mandatory By default, do not re-advertise the label mapping.
Configure the re-advertising interval	**du-readvertise timer** *value*	Optional The default value is 30 and the value range is 1-65535s.

Configure Label Distribution Control Mode

The label allocation control mode of LDP refers to the processing mode adopted by LSR when allocating labels during the establishment of LSP.

Independent label allocation control means that the local LSR can independently allocate a label, bind it to an FEC, and notify the upstream LSR without waiting for the downstream label

The orderly label allocation control means that for the label mapping of an FEC on the LSR, the LSR can send the label mapping of the FEC to the upstream only when the LSR already has the label mapping message of the next hop of the FEC, or the LSR is the outgoing node of the FEC.

Table 2-9 Configure the label distribution control mode

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the LDP configuration mode	**mpls ldp**	-
Configure the ordered label distribution control mode	**label-distribution ordered**	Optional By default, it is the independent label distribution control mode.
Configure the indepdendent label distribution control mode	**label-distribution independent**	Optional By default, it is the independent label distribution control mode.

Configure PHP Features

When a device serves as the Egress node, distribute the implicit null label (the label value is 3) to the last second-hop node by default. After configuring the **explicit-null** command, the Egress node distributes the explicit null label to the last second-hop node (IPv4 explicit null label value is 0, IPv6 explicit null label value is 2). If the Egress node distributes the implicit null label, the last second-hop node will pop up the label. If the Egress node distributes the explicit null label, the last second-hop node will not pop up the label.

Table 2-10 Configure the PHP features

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the LDP configuration mode	**mpls ldp**	-
Configure the Egress node to distribute the explicit null label to the upstream device	**explicit-null**	Optional By default, the Egress node distributes the implicit null label.

Note:

- To configure or delete the **explicit-null** command, you need to use the **clear mpls ldp session** command to re-set the session so that the command can take effect.

Configure Loopback Detection

There are two LSP loop detection modes. One is max. hop mode and the other is path vector mode.

The max. hop mode is the hops contained in the message of transmitting the label. When passing one LSR, the value is added by one. When the value reaches the maximum value of the detection, it is regarded that there is loop and the setup of the LSP is terminated.

The path vector mode is to record the LSR ID information in the message of transmitting the label. When passing one hop, the device checks whether its own LSR ID is recorded. If its own LSR ID is not recorded, add its own LSR ID to the record. If there is the LSR ID in the record, it is regarded that there is loop and the setup of the LSP is terminated.

Table 2-11 Configure the loop detection

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the LDP configuration mode	**mpls ldp**	-
Configure the loop detection	**loop-detection**	Mandatory By default, do not configure the loop detection.
Configure the maximum hops of the loop detection	**maxhops** *value*	Optional After configuring the loopback detection, the default threshold of the detection hops is 255 and the value range is 1-255.

Note:

- The loop detection configurations on the LDP peers should be consistent. Otherwise, the LDP session cannot be set up.
- After configuring the loop detection, the LDP adopts the max. hops and path vector to detect the LSP loop. The default value of the maximum hops is 255.

Configure Session Re-connection

When setting up the TCP connection with the peer fails, the LDP tries to re-set up. The process is called session re-connection.

Table 2-12 Configure the session re-connection

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the LDP configuration mode	**mpls ldp**	-
Configure not permitting increasing the re-connection delay	**reconnection-delay-disable**	Optional By default, permit increasing the re-connection delay.
Configure the re-connection interval	**reconnect-interval** *value*	Optional The default value is 15s and the value range is 1-15s.

Note:

- After configuring the command **dual-stack transport-connection poll** to enable the LDP session dual-stack polling setup capability, automatically disable the LDP session re-connection capability.
- The initial delay of the LDP re-connecting the peer is 15s. If permitting increasing the re-connection delay and after initiating the TCP connection to the peer failed, the delay time doubles successively, that is, 15s, 30s, 60s, 120s. The maximum value cannot exceed 120s. If the initial delay time of the LDP re-connecting the peer is 1s, the re-connection delay time is 1s, 2s, 4s…., and the maximum value also cannot exceed 120s. If not permitting increasing the re-connection delay, the re-connection interval is always the configured initial re-connection interval.

2.2.5. Configure mLDP P2MP

Configuration Conditions

Before configuring mLDP P2MP, first complete the following task:

- Configure the LDP basic functions

Configure mLDP P2MP

Configuring mLDP P2MP is used to enable the P2MP function. The P2MP session can be set up only when the both parties enable the P2MP function. Currently, only support IPv4 mLDP P2MP.

Table 2-13 Configure mLDP P2MP

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the LDP configuration mode	**mpls ldp**	-
Configure mLDP P2MP	**mldp p2mp**	Mandatory By default, do not enable the P2MP function.

Note:

- The LDP IPv6 address family does not support mLDP, the LDP IPv6 related command and mldp p2mp command can be configured at the same time, but as a result, LDP IPv6 does not take effect.
- When the P2MP function is not enabled, using the mldp p2mp command will make all sessions be reset.
- When the P2MP function is enabled, using the no mldp p2mp command will make all sessions be reset.

Configure mLDP MBB

By default, if the route to the root node changes and a new upstream node is selected, the old LSP will be removed immediately. At this time, the new LSP has not been established, which will result in the loss of traffic. Enable the MBB function, the route to the root node changes, select the new upstream node, and the old LSP will be removed after the new LSP is set up successfully, reducing the loss of traffic.

Table 2-14 Configure mLDP MBB

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the LDP configuration mode	**mpls ldp**	-
Configure mLDP MBB	**mldp make-before-break [timeout** *value***]**	Mandatory By default, do not enable the MBB function. By default, the MBB timeout is 10s.

Note:

- When mLDP P2MP is enabled and MBB is not enabled, using the **mldp make-before-break** command will make all sessions be reset.
- When mLDP P2MP and MBB are enabled, using the **no mldp make-before-break** command will make all sessions be reset.
- When the two parties failed to negotiate the P2MP capability, do not negotiate the MBB capability.

2.2.6. Configure LDP GR

Configuration Condition

Before enabling the LDP GR function, first complete the following tasks:

- Configure the LDP basic functions
- The IGP protocol enables the GR function

Configure LDP GR

The MPLS forwarding plane is separate from the control plane. When the control plane becomes abnormal, LDP GR reserves the MPLS label forwarding entry and the LSR still forwards the packet according to the entry, so as to ensure that the data transmission is not interrupted. Currently, only support LDP IPv4 GR.

During the GR process, the devices in the MPLS network are divided to two roles:

- GR restarter: GR restart router, indicating the device with dual control cards that still can keep forwarding data when restarting the control layer protocol because the user switches over the control card manually or the device fails.
- GR helper: The neighbor of GR restarter, keeping the neighbor relationship with the restarted GR restarter and negotiating the GR capability with the GR restarter. After the GR restarter restarts, help it restore the forwarding status before restarting.

The work process of the LDP GR is as follows:

- When the session is set up between the neighbors, negotiate the time value of the GR timer between the LSRs enabled with the GR function.
- After GR restarter restarts, GR helper detects that the session with the GR restarter is down, all label mappings learned by the session are marked as stale, and reserve the label mappings within the timeout of the GR neighbor keepalive timer.
- If the keepalive timer of the GR neighbor times out, the GR Helper deletes the label mappings marked as stale. If the LDP session is set up successfully within the timeout of the GR neighbor keepalive timer, GR restarter and GR helper interact the label mapping via the new setup LDP session within the LDP recovery time, update the label forwarding table, and clear the stale label of the forwarding entry. After the LDP recovery timer times out, GR helper deletes the label mapping still marked as stale.
- The timeout of the holding timer of the MPLS forwarding status indicates that the GR process ends.

Table 2-15 Configure LDP GR

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the LDP configuration mode	**mpls ldp**	-
Enable the GR capability	**graceful-restart**	Mandatory By default, do not enable the GR function.
Configure the holding timer timeout of the GR forwarding status	**graceful-restart timer forwarding-holding** *value*	Optional The default value is 300s and the value range is 30-300s.
Configure the GR recovery timer timeout	**graceful-restart timer max-recovery** *value*	Optional The default value is 120s and the value range is 15-600s.
Configure the keepalive timer timeout of the GR neighbor	**graceful-restart timer neighbor-liveness** *value*	Optional The default value is 120s and the value range is 5-300s.

Note:

- Before the LDP session is set up, it is necessary to configure GR on the peers of the two sides of the session so that the GR capability can be negotiated successfully. Before enabling the GR capability, the setup LDP session does not have the GR capability.

2.2.7. Configure LDP to Link with BFD

Configuration Condition

Before configuring LDP to link with BFD, first complete the following tasks:

- Configure the LDP basic functions
- Enable the LDP protocol on the interface that needs to configure LDP to link with BFD

Configure LDP to Link with BFD

When the link fault happens between two neighboring devices, the time of the LDP detecting the neighbor line fault is long. After detecting the line fault, the LDP session is down and the MPLS forwarding is interrupted. LDP links with BFD and can fast detect the line fault of the LDP

neighbor, improving the performance of the MPLS network. Currently, only support LDP IPv4 to link with BFD.

Table 2-16 Configure LDP to link with BFD

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the LDP configuration mode	**mpls ldp**	-
Configure globally enabling LDP to link with BFD	**bfd all-interfaces**	Optional By default, do not globally enable the LDP to link with BFD.
Exit the LDP configuration mode	**exit**	-
Enter the interface configuration mode	**interface** *interface-name*	-
Configure the interface to enable LDP to link with BFD	**mpls ldp bfd**	Optional By default, do not enable the LDP to link with BFD on the interface.
Configure the interface to disable LDP from linking with BFD	**mpls ldp bfd disable**	Optional By default, permit the interface to enable LDP to link with BFD

Note:

- For the BFD configuration, refer to the BFD chapter in the configuration manual “Reliability”.
- The current LDP only supports single-hop detection result of linking with BFD, but does not support the multi-hop detection result.
- On the interface, the **mpls ldp bfd disable** command is exclusive with the **mpls ldp bfd** command and has higher priority than the **bfd all-interfaces** command in the MPLS LDP mode. The influence of the configuration combination between them for the enabling result of the interface LDP and BFD linkage is shown in the following table.

Table 2-17 Influence for the enabling result of the interface LDP and BFD linkage

bfd all-interfaces	mpls ldp bfd	mpls ldp bfd disable	Whether one interface enables LDP to link with BFD
Configured	Not configured or no	Not configured or no	Enabled
Configured	Not configured or no	Configured	Disabled
Configured	Configured	Not configured or no	Enabled
Not configured or no	Not configured or no	Not configured or no	Disabled
Not configured or no	Not configured or no	Configured	Disabled
Not configured or no	Configured	Not configured or no	Enabled

2.2.8. Configure LDP Fast Re-routing

Configuration Condition

Before configuring LDP fast re-routing, first complete the following tasks:

- Configure the LDP basic functions
- Enable the fast re-routing function of the IGP protocol

Configure LDP Fast Re-routing

LDP faster re-route (FRR) is one protection technology for LDP LSP, depending on the LDP free label keeping mode and IP FRR. When IP FRR has the backup route, LDP will reserve the label advertised by the backup downstream, and set up the standby LSP for the active LSP. When the interface or master LSP fails, LDP will respond fast, and the flow is switched to the pre-setup standby LSP for forwarding, so as to reduce the data loss. Currently, only support LDP IPv4 fast re-routing.

Table 2-18 Configure LDP fast re-routing

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the LDP configuration mode	**mpls ldp**	-
Enter the LDP IPv4 configuration mode	**address-family ipv4**	-
Configure the installation policy of the fast re-route standby LSP	**fast-reroute for** *prefix-accesslist-name*	Optional By default. Do not configure the installation policy of the fast re-route standby LSP.
Configure the fast re-route only to install the standby LSP of the FEC with the 32-bit mask length	**fast-reroute for 32bit-mask-fec-only**	Optional By default, only install the standby LSP of the FEC with the 32-bit mask length.
Exit the LDP IPv4 configuration mode	**exit**	-
Enable the LDP graceful delete function	**graceful-delete**	Mandatory By default, do not enable the LDP graceful delete function.
Configure the time value of the LDP graceful delete timer	**graceful-delete timer** *value*	Optional By default, the time of the LDP graceful delete timer is 10s.

2.2.9. Configure LDP Dual-stack Function

Configuration Conditions

Before configuring the LDP dual-stack function, first complete the following tasks:

- Configure LDP basic functions

- Configure LDP to enable IPv4
- Configure LDP to enable IPv6

Configure LDP Dual-stack Function

LDP dual-stack function includes session dual-stack polling establishment and dual-stack compatibility check.

The dual stack polling establishment capability of LDP session refers to: try to establish an LDP session using an address cluster. If the LDP session based on the address cluster is not established successfully after the dual stack session polling time is exceeded, try to establish an LDP session based on another address family instead;

The LDP dual-stack compatibility check capability refers to the compatibility check of the received LDP Hello message according to the provisions of RFC7552. In order to be compatible with dual-stack LDPs not implemented in strict accordance with RFC7552, the LDP dual stack compatibility check capability is not enabled by default.

Table 2-19 Configure the LDP dual-stack function

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the LDP configuration mode	**mpls ldp**	-
Enable the LDP dual-stack compatibility check capability	**dual-stack tlv-compliance**	Optional By default, do not enable the LDP dual-stack compatibility check capability.
Enable the LDP session dual-stack polling establishment capability	**dual-stack transport-connection poll**	Optional By default, do not enable LDP session dual-stack polling establishment capability.
Configure the LDP session dual-stack polling time	**dual-stack transport-connection poll wait-time** *value*	Optional By default, it is 15s and the value range is 5-120s.

2.2.10. LDP Monitoring and Maintaining

Table 2-20 LDP monitoring and maintaining command list

Command	Description
clear mpls ldp adjacency { **all** | *ipv4-address* }	Reset LDP IPv4 adjacencies
clear mpls ldp error-statistics	Clear the LDP error statistics information
clear mpls ldp session { **all** | *peer-ipv4-address* }	Reset the LDP IPv4 session
clear mpls ldp statistics	Clear the statistics information of the received and sent LDP packets
clear mpls ldp statistics advertise-labels [**for** *ipv4-prefix-accesslist-name* [**to** *ipv4-peer-accesslist-name*]]	Clear the statistics information of the LDP IPv4 label advertising
show mpls ldp adjacency	Display the adjacency information of LDP IPv4
show mpls ldp adjacency delay	Display the IPv4 adjacency information of the LDP delay delete
show mpls ldp advertise-labels	Display the control information of the LDP IPv4 label advertising
show mpls ldp downstream [*ipv4-prefix-address prefixlen*]	Display the downstream status machine information of LDP IPv4 FEC
show mpls ldp error-statistics	Display the LDP error statistics information
show mpls ldp fec [*ipv4-prefix-address prefixlen*]	Display the IPv4 FEC information of the LDP
show mpls ldp fec number	Display the IPv4 FEC quantity of LDP

Command	Description
show mpls ldp fec ote *tunnel-id*	Display the FEC information of LDP over TE
show mpls ldp interface [*interface-name*]	Display the LDP IPv4 interface information
show mpls ldp lsp [**advertise-list** | *ipv4-prefix prefixlen* [**advertise-list**]]	Display the LDP IPv4 LSP information
show mpls ldp memory	Display the LDP memory status information
show mpls ldp parameter [**detail**]	Display the LDP parameter information
show mpls ldp session [**statistics** | *ipv4-peer-address* [**detail**]]	Display the LDP IPv4 session information
show mpls ldp statistics advertise-labels	Display the statistics information of the LDP IPv4 label advertising
show mpls ldp statistics message	Display the statistics information of the LDP message
show mpls ldp targeted-peers	Display the IPv4 target peer information of the LDP
show mpls ldp upstream [*ipv4-prefix prefixlen*]	Display the upstream status machine information of LDP IPv4 FEC

2.3. MPLS LDP Typical Configuration Example

2.3.1. Configure LDP Basic Functions

Network Requirements

- The whole network uses OSPF to interact the route.
- The device enables MPLS IP and MPLS LDP; set up the LDP session between Device1 and Device2, Device2 and Device3.

Network Topology

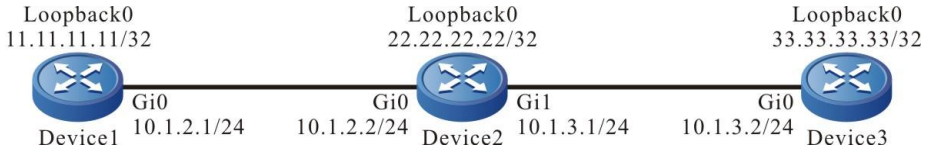

Figure 2-1 Networking of configuring the LDP basic functions

Configuration Steps

Step 1: Configure the IP address of the interface (omitted).

Step 2: Configure OSPF.

#Configure OSPF on Device1.

```
Device1#configure terminal
Device1(config)#router ospf 100
Device1(config-ospf)#network 10.1.2.0 0.0.0.255 area 0
Device1(config-ospf)#network 11.11.11.11 0.0.0.0 area 0
Device1(config-ospf)#exit
```

Configure OSPF on Device2.

```
Device2#configure terminal
Device2(config)#router ospf 100
Device2(config-ospf)#network 10.1.2.0 0.0.0.255 area 0
Device2(config-ospf)#network 10.1.3.0 0.0.0.255 area 0
Device2(config-ospf)#network 22.22.22.22 0.0.0.0 area 0
Device2(config-ospf)#exit
```

Configure OSPF on Device3.

```
Device3#configure terminal
Device3(config)#router ospf 100
Device3(config-ospf)#network 10.1.3.0 0.0.0.255 area 0
Device3(config-ospf)#network 33.33.33.33 0.0.0.0 area 0
Device3(config-ospf)#exit
```

#View the route table on the device.

Take Device1 as an example:

```
Device1#show ip route
Codes: C - Connected, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external
```

```
C   10.1.2.0/24 is directly connected, 06:19:07, gigabitethernet0
O   10.1.3.0/24 [110/2] via 10.1.2.2, 06:05:08, gigabitethernet0
C   127.0.0.0/8 is directly connected, 102:05:13, lo0
C   11.11.11.11/32 is directly connected, 06:18:54, loopback0
O   22.22.22.22/32 [110/2] via 10.1.2.2, 06:12:40, gigabitethernet0
O   33.33.33.33/32 [110/3] via 10.1.2.2, 06:02:59, gigabitethernet0
```

You can see that there is the route to the Loopback0 interface of Device2 and Device3 in the route table of Device1.

Note:

- For the checking method of Device2 and Device3, refer to Device1.

Step 3: Enable MPLS IP and MPLS LDP.

#Enable MPLS IP and MPLS LDP globally on Device1; enable MPLS IP and MPLS LDP on the interface at the same time.

```
Device1(config)#mpls ip
Device1(config)#mpls ldp
Device1(config-ldp)#router-id 11.11.11.11
Device1(config-ldp)#address-family ipv4
Device1(config-ldp-af4)#transport-address 11.11.11.11
Device1(config-ldp-af4)#exit
Device1(config-ldp)#exit
Device1(config)#interface gigabitethernet0
Device1(config-if-gigabitethernet0)#mpls ip
Device1(config-if-gigabitethernet0)#mpls ldp
Device1(config-if-gigabitethernet0)#exit
```

#Enable MPLS IP and MPLS LDP globally on Device2; enable MPLS IP and MPLS LDP on the interface at the same time.

```
Device2(config)#mpls ip
Device2(config)#mpls ldp
Device2(config-ldp)#router-id 22.22.22.22
Device2(config-ldp)#address-family ipv4
Device2(config-ldp-af4)#transport-address 22.22.22.22
Device2(config-ldp-af4)#exit
Device2(config-ldp)#exit
Device2(config)#interface gigabitethernet0
Device2(config-if-gigabitethernet0)#mpls ip
```

```
Device2(config-if-gigabitethernet0)#mpls ldp
Device2(config-if-gigabitethernet0)#exit
Device2(config)#interface gigabitethernet1
Device2(config-if-gigabitethernet1)#mpls ip
Device2(config-if-gigabitethernet1)#mpls ldp
Device2(config-if-gigabitethernet1)#exit
```

#Enable MPLS IP and MPLS LDP globally on Device3; enable MPLS IP and MPLS LDP on the interface at the same time.

```
Device3(config)#mpls ip
Device3(config)#mpls ldp
Device3(config-ldp)#router-id 33.33.33.33
Device3(config-ldp)#address-family ipv4
Device3(config-ldp-af4)#transport-address 33.33.33.33
Device3(config-ldp-af4)#exit
Device3(config-ldp)#exit
Device3(config)#interface gigabitethernet0
Device3(config-if-gigabitethernet0)#mpls ip
Device3(config-if-gigabitethernet0)#mpls ldp
Device3(config-if-gigabitethernet0)#exit
```

Note:

- **router-id** and **transport-address** can be configured manually or generated automatically. Usually, they are configured to be the same. If **router-id** and **transport-address** are not configured manually, the device selects automatically. From the up interfaces, first select the one with the maximum IP address in the Loopback interfaces. If the device is not configured with the Loopback interface address, select the maximum IP address in the common interfaces.

Step 4: Check the result.

#View the LDP session information on the device.

Take Device1 as an example:

```
Device1#show mpls ldp session
Peer IP Address   Peer Type   My Role  State        DS Cap   DeadTime
22.22.22.22       Multicast   Passive  OPERATIONAL  Disabled 00:02:01
Statistics for ldp sessions:
    Multicast sessions: 1
    Targeted sessions: 0
```

The content of the State list is displayed as OPERATIONAL, and you can see that Device1 and Device2 set up the LDP session successfully.

#View the route label information on the device.

Take Device1 as an example:

```
Device1#show ip route 22.22.22.22 detail
Codes: C - Connected, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external


O   22.22.22.22/32 [110/2] via 10.1.2.2, label 3, 14:29:21, gigabitethernet0
                           10.1.2.2 [0], gigabitethernet0

Device1#show ip route 33.33.33.33  detail
Codes: C - Connected, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external


O   33.33.33.33/32 [110/3] via 10.1.2.2, label 24017, 14:29:21, gigabitethernet0
                   10.1.2.2 [0], gigabitethernet0
```

You can see that Device1 has the label information of the route to the loopback0 interface address of Device2 and Device3.

#View the LSP information on the device.

Take Device1 as an example:

```
Device1#show mpls ldp lsp

FEC IPV4:10.1.2.0/24 -> 0.0.0.0, gigabitethernet0

FEC IPV4:10.1.3.0/24 -> 10.1.2.2, gigabitethernet0

FEC IPV4:11.11.11.11/32 -> 0.0.0.0, loopback0
  Downstream state: Established Label: none        RequestID: 0 Peer: EGRESS Attr:
None
   Upstream state: Established Label: impl-null  RequestID: 0 Peer: 22.22.22.22 Attr:
None

FEC IPV4:22.22.22.22/32 -> 10.1.2.2, gigabitethernet0
```

```
Downstream state: Established Label: impl-null  RequestID: 0 Peer: 22.22.22.22
Attr: None


FEC IPV4:33.33.33.33/32 -> 10.1.2.2, gigabitethernet0
Downstream state: Established Label: 17  RequestID: 0 Peer: 22.22.22.22 Attr:
None
```

You can see that there is the FEC LSP information of the loopback0 interface address of Device2 and Device3 on Device1.

Note:

- For the checking method of Device2 and Device3, refer to Device1.

2.3.2. Configure LDP Remote Session

Network Requirements

- The whole network uses OSPF to interact the route.
- Device1 and Device3 enable MPLS IP and MPLS LDP; set up the LDP remote session between Device1 and Device3.

Network Topology

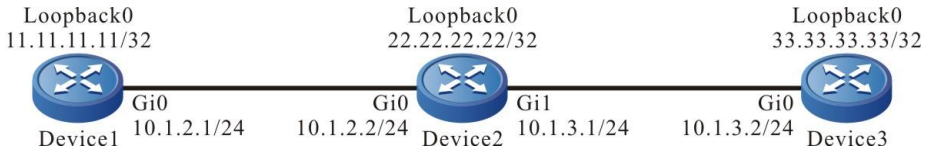

Figure 2-2 Networking of configuring the LDP remote session

Configuration Steps

Step 1: Configure the IP address of the interface (omitted).

Step 2: Configure OSPF.

#Configure OSPF on Device1.

```
Device1#configure terminal
Device1(config)#router ospf 100
Device1(config-ospf)#network 10.1.2.0 0.0.0.255 area 0
Device1(config-ospf)#network 11.11.11.11 0.0.0.0 area 0
Device1(config-ospf)#exit
```

#Configure OSPF on Device2.

```
Device2#configure terminal
Device2(config)#router ospf 100
Device2(config-ospf)#network 10.1.2.0 0.0.0.255 area 0
Device2(config-ospf)#network 10.1.3.0 0.0.0.255 area 0
Device2(config-ospf)#network 22.22.22.22 0.0.0.0 area 0
Device2(config-ospf)#exit
```

#Configure OSPF on Device3.

```
Device3#configure terminal
Device3(config)#router ospf 100
Device3(config-ospf)#network 10.1.3.0 0.0.0.255 area 0
Device3(config-ospf)#network 33.33.33.33 0.0.0.0 area 0
Device3(config-ospf)#exit
```

#View the route table on the device.

Take Device1 as an example:

```
Device1#show ip route
Codes: C - Connected, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external
```

```
C   10.1.2.0/24 is directly connected, 06:19:07, gigabitethernet0
O   10.1.3.0/24 [110/2] via 10.1.2.2, 06:05:08, gigabitethernet0
C   127.0.0.0/8 is directly connected, 102:05:13, lo0
C   11.11.11.11/32 is directly connected, 06:18:54, loopback0
O   22.22.22.22/32 [110/2] via 10.1.2.2, 06:12:40, gigabitethernet0
O   33.33.33.33/32 [110/3] via 10.1.2.2, 06:02:59, gigabitethernet0
```

You can see that there is the route to the loopback0 interface of Device2 and Device3 in the route table of Device1.

Note:

- For the checking method of Device2 and Device3, refer to Device1.

Step 3: Enable MPLS IP and MPLS LDP, and configure the remote LDP session.

#Enable MPLS IP and MPLS LDP globally on Device1; enable MPLS IP and MPLS LDP on the interface at the same time; configure the remote LDP peer.

```
Device1(config)#mpls ip
Device1(config)#mpls ldp
Device1(config-ldp)#router-id 11.11.11.11
Device1(config-ldp)#address-family ipv4
Device1(config-ldp-af4)#transport-address 11.11.11.11
Device1(config-ldp-af4)#targeted-peer 33.33.33.33
Device1(config-ldp-af4)#exit
Device1(config-ldp)#exit
```

```
Device1(config)#interface gigabitethernet0
Device1(config-if-gigabitethernet0)#mpls ip
Device1(config-if-gigabitethernet0)#mpls ldp
Device1(config-if-gigabitethernet0)#exit
```

#Enable MPLS IP and MPLS LDP globally on Device3; enable MPLS IP and MPLS LDP on the interface at the same time; configure the remote LDP peer.

```
Device3(config)#mpls ip
Device3(config)#mpls ldp
Device3(config-ldp)#router-id 33.33.33.33
Device3(config-ldp)#address-family ipv4
Device3(config-ldp-af4)#transport-address 33.33.33.33
Device3(config-ldp-af4)#targeted-peer 11.11.11.11
Device3(config-ldp-af4)#exit
Device3(config-ldp)#exit
Device3(config)#interface gigabitethernet0
Device3(config-if-gigabitethernet0)#mpls ip
Device3(config-if-gigabitethernet0)#mpls ldp
Device3(config-if-gigabitethernet0)#exit
```

Step 4: Check the result.

#View the remote LDP session information on Device1 and Device3.

Take Device1 as an example:

```
Device1#show mpls ldp session
Peer IP Address   Peer Type    My Role   State        DS Cap   DeadTime
33.33.33.33       Targeted     Passive   OPERATIONAL  Disabled 00:02:57
Statistics for ldp sessions:
    Multicast sessions: 0
    Targeted sessions: 1
```

The content of the State list is displayed as OPERATIONAL, the content of the Peer Type list is displayed as Trageted, and you can see that Device1 and Devic3 successfully set up the remote LDP session.

#View the LDP adjacency on Device1 and Device3.

Take Device1 as an example:

```
Device1#show mpls ldp adjacency
IP Address      Interface Name              DS Cap    Deadtime  LDP-Identifier
33.33.33.33     /                           Disable   00:01:20  33.33.33.33:0
```

In the LDP adjacency table of Device1, you can see the Targeted adjacency 33.33.33.33 of the interface "/".

#View the remote peer on Device1 and Device3.

Take Device1 as an example:

```
Device1#show mpls ldp targeted-peers
IP Address        State
33.33.33.33       Active
```

You can see that there is the Device3 information in the remote peer table of Device1.

Note:

- For the checking method of Device3, refer to Device1.
- The LDP remote session is usually used in the MPLS L2VPN environment.

2.3.3. Configure MPLS LDP to Link with BFD

Network Requirements

- The whole network uses OSPF to interact the route; the device enables MPLS IP and MPLS LDP; Device1 and Device3 configure MPLS LDP to link with BFD.
- When the line between Device1 and Device3 fails, the MPLS service data between Device1 and Device3 can be switched fast.

Network Topology

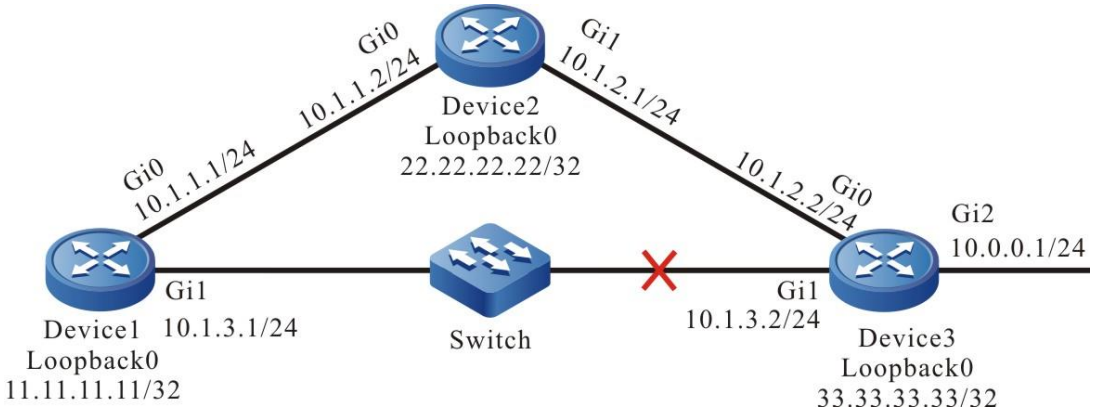

Figure 2-3 Networking of configuring MPLS LDP to link with BFD

Configuration Steps

Step 1: Configure the IP address of the interface (omitted).

Step 2: Configure OSPF.

#Configure OSPF on Device1.

```
Device1#configure terminal
Device1(config)#router ospf 100
Device1(config-ospf)#network 10.1.1.0 0.0.0.255 area 0
Device1(config-ospf)#network 10.1.3.0 0.0.0.255 area 0
Device1(config-ospf)#network 11.11.11.11 0.0.0.0 area 0
```

```
Device1(config-ospf)#exit
```

#Configure OSPF on Device2.

```
Device2#configure terminal
Device2(config)#router ospf 100
Device2(config-ospf)#network 10.1.1.0 0.0.0.255 area 0
Device2(config-ospf)#network 10.1.2.0 0.0.0.255 area 0
Device2(config-ospf)#network 22.22.22.22 0.0.0.0 area 0
Device2(config-ospf)#exit
```

#Configure OSPF on Device3.

```
Device3#configure terminal
Device3(config)#router ospf 100
Device3(config-ospf)#network 10.0.0.0 0.0.0.255 area 0
Device3(config-ospf)#network 10.1.2.0 0.0.0.255 area 0
Device3(config-ospf)#network 10.1.3.0 0.0.0.255 area 0
Device3(config-ospf)#network 33.33.33.33 0.0.0.0 area 0
Device3(config-ospf)#exit
```

#View the route table on the device.

Take Device1 as an example:

```
Device1#show ip route
Codes: C - Connected, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external



O   10.0.0.0/24 [110/2] via 10.1.3.2, 00:12:57, gigabitethernet1
C   10.1.1.0/24 is directly connected, 02:22:00, gigabitethernet0
O   10.1.2.0/24 [110/2] via 10.1.1.2, 02:00:31, gigabitethernet0
                [110/2] via 10.1.3.2, 00:12:57, gigabitethernet1
C   10.1.3.0/24 is directly connected, 02:21:47, gigabitethernet1
C   127.0.0.0/8 is directly connected, 483:17:24, lo0
C   11.11.11.11/32 is directly connected, 02:16:48, loopback0
O   22.22.22.22/32 [110/2] via 10.1.1.2, 02:00:21, gigabitethernet0
O   33.33.33.33/32 [110/2] via 10.1.3.2, 00:12:57, gigabitethernet1
```

You can see that there is the route to the direct-connected segment 10.0.0.0/24 of Device3 in the route table of Device1, and first select the line between Device1 and Device3 to communicate.

Note:

- For the checking method of Device3 and Device2, refer to Device1.

Step 3: Enable MPLS IP and MPLS LDP.

#Enable MPLS IP and MPLS LDP globally on Device1; enable MPLS IP and MPLS LDP on the interface at the same time; in the MPLS LDP, cancel distributing and receiving the label only for the FEC with 32-bit mask.

```
Device1(config)#mpls ip
Device1(config)#mpls ldp
Device1(config-ldp)#router-id 11.11.11.11
Device1(config-ldp)#address-family ipv4
Device1(config-ldp-af4)#transport-address 11.11.11.11
Device1(config-ldp-af4)#no advertise-labels for 32bit-mask-fec-only
Device1(config-ldp-af4)#no accept-labels for 32bit-mask-fec-only
Device1(config-ldp-af4)#exit
Device1(config-ldp)#exit
Device1(config)#interface gigabitethernet0
Device1(config-if-gigabitethernet0)#mpls ip
Device1(config-if-gigabitethernet0)#mpls ldp
Device1(config-if-gigabitethernet0)#exit
Device1(config)#interface gigabitethernet1
Device1(config-if-gigabitethernet1)#mpls ip
Device1(config-if-gigabitethernet1)#mpls ldp
Device1(config-if-gigabitethernet1)#exit
```

#Enable MPLS IP and MPLS LDP globally on Device2; enable MPLS IP and MPLS LDP on the interface at the same time; in the MPLS LDP, cancel distributing and receiving the label only for the FEC with 32-bit mask.

```
Device2(config)#mpls ip
Device2(config)#mpls ldp
Device2(config-ldp)#router-id 22.22.22.22
Device2(config-ldp)#address-family ipv4
Device2(config-ldp-af4)#transport-address 22.22.22.22
Device2(config-ldp-af4)#no advertise-labels for 32bit-mask-fec-only
Device2(config-ldp-af4)#no accept-labels for 32bit-mask-fec-only
Device2(config-ldp-af4)#exit
Device2(config-ldp)#exit
Device2(config)#interface gigabitethernet0
Device2(config-if-gigabitethernet0)#mpls ip
```

```
Device2(config-if-gigabitethernet0)#mpls ldp
Device2(config-if-gigabitethernet0)#exit
Device2(config)#interface gigabitethernet1
Device2(config-if-gigabitethernet1)#mpls ip
Device2(config-if-gigabitethernet1)#mpls ldp
Device2(config-if-gigabitethernet1)#exit
```

#Enable MPLS IP and MPLS LDP globally on Device3; enable MPLS IP and MPLS LDP on the interface at the same time; in the MPLS LDP, cancel distributing and receiving the label only for the FEC with 32-bit mask.

```
Device3(config)#mpls ip
Device3(config)#mpls ldp
Device3(config-ldp)#router-id 33.33.33.33
Device3(config-ldp)#address-family ipv4
Device3(config-ldp-af4)#transport-address 33.33.33.33
Device3(config-ldp-af4)#no advertise-labels for 32bit-mask-fec-only
Device3(config-ldp-af4)#no accept-labels for 32bit-mask-fec-only
Device3(config-ldp-af4)#exit
Device3(config-ldp)#exit
Device3(config)#interface gigabitethernet0
Device3(config-if-gigabitethernet0)#mpls ip
Device3(config-if-gigabitethernet0)#mpls ldp
Device3(config-if-gigabitethernet0)#exit
Device3(config)#interface gigabitethernet1
Device3(config-if-gigabitethernet1)#mpls ip
Device3(config-if-gigabitethernet1)#mpls ldp
Device3(config-if-gigabitethernet1)#exit
Device3(config)#interface gigabitethernet2
Device3(config-if-gigabitethernet2)#mpls ip
Device3(config-if-gigabitethernet2)#mpls ldp
Device3(config-if-gigabitethernet2)#exit
```

#View the LDP session information on the device.

Take Device1 as an example:

```
Device1#show mpls ldp session
Peer IP Address   Peer Type    My Role  State        DS Cap    DeadTime
22.22.22.22       Multicast    Passive  OPERATIONAL  Disabled  00:02:54
33.33.33.33       Multicast    Passive  OPERATIONAL  Disabled  00:02:41
Statistics for ldp sessions:
```

```
Multicast sessions: 2
Targeted sessions: 0
```

The content of the State list is displayed as OPERATIONAL, and you can see that Device1 sets up the LDP session with Device2, Device3 successfully.

#View the MPLS forwarding table on the device.

Take Device1 as an example:

```
Device1#show ip route 10.0.0.1  detail
Codes: C - Connected, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
    U - Per-user Static route
    O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external



O   10.0.0.0/24 [110/2] via 10.1.3.2, label 3, 14:29:21, gigabitethernet1
                  10.1.3.2 [0], gigabitethernet1


Device1#show mpls forwarding-table
Pro: L - LDP, O - OSPF, B - MP-BGP, R - RSVP, M - Mapped-Route, S - Static
Label,ML - mLDP (ML FEC: Root address/OT/OV), RM - RSVP P2MP (RM FEC: P2MP
ID/TID)


Pro Ident       FEC              Inlabel Outlabel Outgoing          Next hop
L   global      22.22.22.22/32     24018   3      gigabitethernet0    10.1.1.2
L   global      10.0.0.0/24        24020   3      gigabitethernet1    10.1.3.2
L   global      33.33.33.33/32     24021   3      gigabitethernet1    10.1.3.2
```

You can see that there is label information of the route to the direct-connected segment 10.0.0.0/24 of Device3 on Device1, and first select the line between Device1 and Device3 to communicate.

Note:

- By default, the device enables distributing and receiving the label only for the FEC with 32-bit mask in the MPLS LDP process.
- For the checking method of Device3 and Device2, refer to Device1.

Step 4: Configure OSPF, LDP to link with BFD.

#On Device1, configure OSPF, LDP to link with BFD.

```
Device1(config)#interface gigabitethernet1
Device1(config-if-gigabitethernet1)#ip ospf bfd
```

```
Device1(config-if-gigabitethernet1)#mpls ldp bfd
Device1(config-if-gigabitethernet1)#exit
```

#On Device3, configure OSPF, LDP to link with BFD.

```
Device3(config)#interface gigabitethernet1
Device3(config-if-gigabitethernet1)#ip ospf bfd
Device3(config-if-gigabitethernet1)#mpls ldp bfd
Device3(config-if-gigabitethernet1)#exit
```

Step 5: Check the result.

#View the BFD session information of Device1, Device3.

Take Device1 as an example:

```
Device1#show bfd session detail
Total session number: 1
OurAddr          NeighAddr          LD/RD          State          Holddown
interface
10.1.3.1         10.1.3.2           6/4            UP             5000
gigabitethernet1
Type:direct
Local State:UP  Remote State:UP  Up for: 0h:36m:4s  Number of times UP:1
Send Interval:1000ms  Detection time:5000ms(1000ms*5)
Local Diag:0  Demand mode:0  Poll bit:0
MinTxInt:1000  MinRxInt:1000  Multiplier:5
Remote MinTxInt:1000  Remote MinRxInt:1000  Remote Multiplier:5
Registered protocols:OSPF  LDP
Agent session info:
  Sender:slot 0  Recver:slot 0
```

You can see that OSPF, LDP links with BFD successfully and the session is set up normally.

#After the line between Device1 and Device2 fails, BFD can fast detect, and inform OSPF and LDP to converge fast. View the route table and route label information of the device.

Take Device1 as an example:

```
Device1#show ip route
Codes: C - Connected, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external
```

```
O   10.0.0.0/24 [110/3] via 10.1.1.2, 00:12:48, gigabitethernet0
```

```
C   10.1.1.0/24 is directly connected, 03:25:20, gigabitethernet0
O   10.1.2.0/24 [110/2] via 10.1.1.2, 03:01:43, gigabitethernet0
O   10.1.3.0/24 [110/3] via 10.1.1.2, 00:12:48, gigabitethernet0
C   127.0.0.0/8 is directly connected, 365:35:46, lo0
C   11.11.11.11/32 is directly connected, 03:12:42, loopback0
O   22.22.22.22/32 [110/2] via 10.1.1.2, 03:08:46, gigabitethernet0
O   33.33.33.33/32 [110/3] via 10.1.1.2, 00:12:48, gigabitethernet0

Device1#show ip route 10.0.0.1 detail
Codes: C - Connected, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external

O   10.0.0.0/24 [110/2] via 10.1.3.2, label 24021, 14:29:21, gigabitethernet0
                        10.1.3.2 [0], gigabitethernet0
```

In the route table, you can see that the route 10.0.0.0/24 selects the line between Device1 and Device2 to communicate.

Note:

- For the checking method of Device3, refer to Device1.

2.3.4. Configure LDP Fast Re-route

Network Requirements

- The whole network uses OSPF to interact the route.
- The device enables MPLS IP and MPLS LDP; set up the LDP session between Device1 and Device2, Device3, Device2 and Device3, Device3 and Device4.
- On Device1, configure IP FRR.

Network Topology

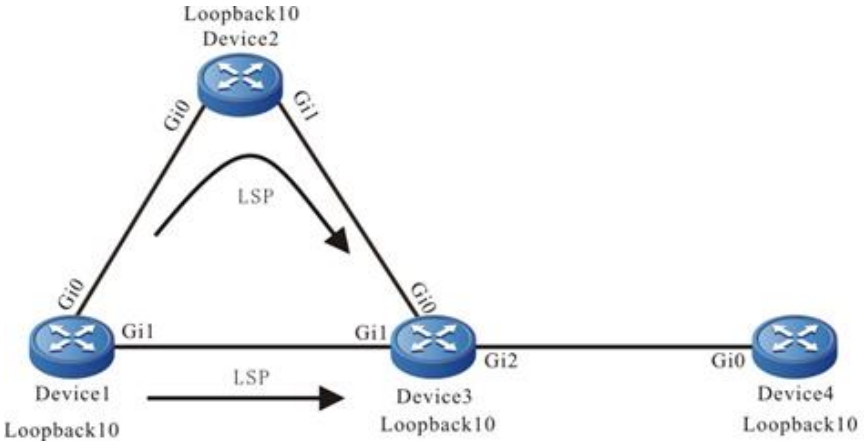

Figure 2-4 Networking of configuring LDP FRR basic functions

Device	Interface	IP Address	Device	Interface	IP Address
Device1	Gi0	1.1.1.1/24	Device3	Gi0	3.1.1.1/24
	Gi1	2.1.1.1/24		Gi1	2.1.1.2/24
	Loopback10	10.1.1.1/32		Gi2	4.1.1.1/24
Device2	Gi0	1.1.1.2/24		Loopback10	10.3.3.3/32
	Gi1	3.1.1.2/24	Device4	Gi0	4.1.1.2/24
	Loopback10	10.2.2.2/32		Loopback10	10.4.4.4/32

Configuration Steps

Step 1: Configure the IP address of the interface (omitted).

Step 2: Configure the global OSPF, and advertise the global route.

#On Device1, configure the global OSPF.

```
Device1#configure terminal
Device1(config)#router ospf 100
Device1(config-ospf)#network 1.1.1.0 0.0.0.255 area 0
Device1(config-ospf)#network 2.1.1.0 0.0.0.255 area 0
Device1(config-ospf)#network 10.1.1.1 0.0.0.0 area 0
Device1(config-ospf)#exit
```

#On Device2, configure the global OSPF.

```
Device2#configure terminal
```

```
Device2(config)#router ospf 100
Device2(config-ospf)#network 1.1.1.0 0.0.0.255 area 0
Device2(config-ospf)#network 3.1.1.0 0.0.0.255 area 0
Device2(config-ospf)#network 10.2.2.2 0.0.0.0 area 0
Device2(config-ospf)#exit
```

#On Device3, configure the global OSPF.

```
Device3#configure terminal
Device3(config)#router ospf 100
Device3(config-ospf)#network 2.1.1.0 0.0.0.255 area 0
Device3(config-ospf)#network 3.1.1.0 0.0.0.255 area 0
Device3(config-ospf)#network 4.1.1.0 0.0.0.255 area 0
Device3(config-ospf)#network 10.3.3.3 0.0.0.0 area 0
Device3(config-ospf)#exit
```

#On Device4, configure the global OSPF.

```
Device4#configure terminal
Device4(config)#router ospf 100
Device4(config-ospf)#network 4.1.1.0 0.0.0.255 area 0
Device4(config-ospf)#network 10.4.4.4 0.0.0.0 area 0
Device4(config-ospf)#exit
```

#After configuration, query the global route table on the device.

Take Device1 as an example:

```
Device1#show ip route
Codes: C - Connected, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external



C   1.1.1.0/24 is directly connected, 04:15:41, gigabitethernet0
L   1.1.1.1/32 is directly connected, 04:15:41, gigabitethernet0
C   2.1.1.0/24 is directly connected, 1d:00:10:09, gigabitethernet1
L   2.1.1.1/32 is directly connected, 1d:00:10:09, gigabitethernet1
O   3.1.1.0/24 [110/2] via 1.1.1.2, 00:50:24, gigabitethernet0
                  [110/2] via 2.1.1.2, 00:52:24, gigabitethernet1
LC  10.1.1.1/32 is directly connected, 1d:00:12:27, loopback10
O   10.2.2.2/32 [110/2] via 1.1.1.2, 00:48:23, gigabitethernet0
O   10.3.3.3/32 [110/2] via 2.1.1.2, 00:52:24, gigabitethernet1
```

```
O   10.4.4.4/32 [110/3] via 2.1.1.2, 00:01:02, gigabitethernet1
```

In the global route table of Device1, there is the route information of Device2, Device3, and Device4 loopback ports.

Note:

- For the checking methods of Device2, Device3, and Device4, refer to Device1.

Step 3: Enable MPLS IP and MPLS LDP.

#On Device1, enable the global MPLS IP and MPLS LDP, and meanwhile, enable the MPLS IP and MPLS LDP on the interface. By default, LSP only set up the standby LSP for the FEC with the 32-bit mask length. To set up the standby LSP for the FEC with non-32-bit mask length, it is necessary to configure the command no fast-reroute for 32bit-mask-fec-only to enable the graceful delete function.

```
Device1(config)#mpls ip
Device1(config)#mpls ldp
Device1(config-ldp)#router-id 10.1.1.1
Device1(config-ldp)#graceful-delete
Device1(config-ldp)#address-family ipv4
Device1(config-ldp-af4)#transport-address 10.1.1.1
Device1(config-ldp-af4)#exit
Device1(config-ldp)#exit
Device1(config)#interface gigabitethernet0
Device1(config-if-gigabitethernet0)#mpls ip
Device1(config-if-gigabitethernet0)#mpls ldp
Device1(config-if-gigabitethernet0)#exit
Device1(config)#interface gigabitethernet1
Device1(config-if-gigabitethernet1)#mpls ip
Device1(config-if-gigabitethernet1)#mpls ldp
Device1(config-if-gigabitethernet1)#exit
```

#On Device2, enable the global MPLS IP and MPLS LDP, and meanwhile, enable the MPLS IP and MPLS LDP on the interface.

```
Device2(config)#mpls ip
Device2(config)#mpls ldp
Device2(config-ldp)#router-id 10.2.2.2
Device2(config-ldp)#address-family ipv4
Device2(config-ldp-af4)#transport-address 10.2.2.2
Device2(config-ldp-af4)#exit
Device2(config-ldp)#exit
Device2(config)#interface gigabitethernet0
Device2(config-if-gigabitethernet0)#mpls ip
```

```
Device2(config-if-gigabitethernet0)#mpls ldp
Device2(config-if-gigabitethernet0)#exit
Device2(config)#interface gigabitethernet1
Device2(config-if-gigabitethernet1)#mpls ip
Device2(config-if-gigabitethernet1)#mpls ldp
Device2(config-if-gigabitethernet1)#exit
```

#On Device3, enable the global MPLS IP and MPLS LDP, and meanwhile, enable the MPLS IP and MPLS LDP on the interface.

```
Device3(config)#mpls ip
Device3(config)#mpls ldp
Device3(config-ldp)#router-id 10.3.3.3
Device3(config-ldp)#address-family ipv4
Device3(config-ldp-af4)#transport-address 10.3.3.3
Device3(config-ldp-af4)#exit
Device3(config-ldp)#exit
Device3(config)#interface gigabitethernet0
Device3(config-if-gigabitethernet0)#mpls ip
Device3(config-if-gigabitethernet0)#mpls ldp
Device3(config-if-gigabitethernet0)#exit
Device3(config)#interface gigabitethernet1
Device3(config-if-gigabitethernet1)#mpls ip
Device3(config-if-gigabitethernet1)#mpls ldp
Device3(config-if-gigabitethernet1)#exit
Device3(config)#interface gigabitethernet2
Device3(config-if-gigabitethernet2)#mpls ip
Device3(config-if-gigabitethernet2)#mpls ldp
Device3(config-if-gigabitethernet2)#exit
```

#On Device4, enable the global MPLS IP and MPLS LDP, and meanwhile, enable the MPLS IP and MPLS LDP on the interface.

```
Device4(config)#mpls ip
Device4(config)#mpls ldp
Device4(config-ldp)#router-id 10.4.4.4
Device4(config-ldp)#address-family ipv4
Device4(config-ldp-af4)#transport-address 10.4.4.4
Device4(config-ldp-af4)#exit
Device4(config-ldp)#exit
Device4(config)#interface gigabitethernet0
Device4(config-if-gigabitethernet0)#mpls ip
```

```
Device4(config-if-gigabitethernet0)#mpls ldp
Device4(config-if-gigabitethernet0)#exit
```

#After configuration, query the LDP session information on the device.

Take Device1 as an example:

```
Device1#show mpls ldp session
Peer IP Address    Peer Type    My Role   State        DS Cap    DeadTime
10.3.3.3           Multicast    Passive   OPERATIONAL  Disabled  00:02:34
10.2.2.2           Multicast    Passive   OPERATIONAL  Disabled  00:02:09
Statistics for ldp sessions:
    Multicast sessions: 2
    Targeted sessions: 0
```

You can see that Device1 and Device2, Device3 set up the LDP sessions successfully.

#On the device, query the MPLS forwarding table.

Take Device1 as an example:

```
Device1#show mpls forwarding-table
Pro: L - LDP, O - OSPF, B - MP-BGP, R - RSVP, M - Mapped-Route, S - Static
Label,ML - mLDP (ML FEC: Root address/OT/OV), RM - RSVP P2MP (RM FEC: P2MP
ID/TID)

Pro Ident      FEC            Inlabel Outlabel Outgoing          Next hop
L   global     10.2.2.2/32    24120   3        gigabitethernet0  1.1.1.2
L   global     10.3.3.3/32    24121   3        gigabitethernet1  2.1.1.2
L   global     10.4.4.4/32    24122   3        gigabitethernet1  2.1.1.2
```

There is the information about the routes to the loopback ports of Device2, Device3, and Device4 on Device1.

Note:

- For the checking methods of Device2, Device3, and Device4, refer to Device1.

Step 4: Configure IP FRR.

#On Device1, configure route-map, specify the backup egress interface as Gi1, and configure the match rule, permitting all prefixes to generate the backup route. And then, apply the route-map in OSPF.

```
Device1(config)#route-map ldp_frr
Device1(config-route-map)#match ip address 1
Device1(config-route-map)#set fast-reroute backup-interface gigabitethernet 1
backup-nexthop 2.1.1.2
Device1(config-route-map)#exit
Device1(config)#ip access-list standard 1
```

```
Device1(config-std-nacl)#permit host 10.4.4.4
Device1(config-std-nacl)#exit
Device1(config)#router ospf 100
Device1(config-ospf)#fast-reroute route-map ldp_frr
Device1(config-ospf)#exit
```

Step 5: Check the result.

#On Device1, query the label information of the master route.

```
Device1#show  ip route 10.4.4.4 detail
Codes: C - Connected, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
    U - Per-user Static route
    O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external
```

```
O   10.4.4.4/32 [110/3] via 2.1.1.2, label 3, 00:18:01, gigabitethernet1
                        2.1.1.2 [0], gigabitethernet1
```

#On Device, query the label information of the standby route.

```
Device1#show ip frr route 10.4.4.4  detail
Codes: C - Connected, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
    U - Per-user Static route
    O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external
```

```
O   10.4.4.4/32 [110/4294967295] via 1.1.1.2, label 24016, 00:18:14, gigabitethernet0
      1.1.1.2 [0], gigabitethernet0
```

```
#On Device1, query the generated BFD session.
Device1#show  bfd session
OurAddr          NeighAddr          LD/RD          State      Holddown
Interface
2.1.1.1          2.1.1.2            65/65          UP         500        gigabitethernet1
```

You can see that there is the FRR route to 10.4.4.4 on Device1, and the BFD session is also generated, used to detect whether the LSP link fails.

2.3.5. Configure IPv6 LDP Basic Functions

Network Requirements

- The whole network uses OSPF to interact the route.

- The device enables MPLS IP and IPv6 MPLS LDP; set up the IPv6 LDP session between Device1 and Device2, Device2 and Device3.

Network Topology

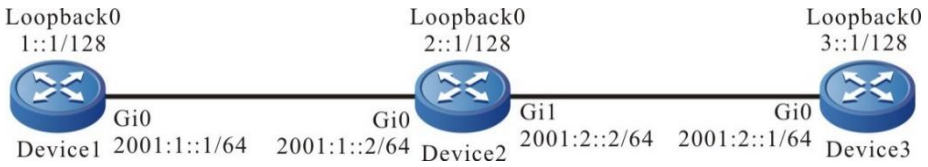

Figure 2-5 Networking of configuring LDP basic functions

Step 1: Configure the IP address of the interface (omitted).

Step 2: Configure OSPFv3.

#Configure OSPFv3 on Device1.

```
Device1#configure terminal
Device1(config)#ipv6 router ospf 100
Device1(config-ospf6)#router-id 1.1.1.1
Device1(config-ospf6)#exit
Device1(config)#interface gigabitethernet 0
Device1(config-if-gigabitethernet0)#ipv6 router ospf 100 area 0
Device1(config-if-gigabitethernet0)#exit
```

#Configure OSPFv3 on Device2.

```
Device2#configure terminal
Device2(config)#ipv6 router ospf 100
Device2(config-ospf6)#router-id 2.2.2.2
Device2(config-ospf6)#exit
Device2(config)#interface gigabitethernet0
Device2(config-if-gigabitethernet0)#ipv6 router ospf 100 area 0
Device2(config-if-gigabitethernet0)#exit
Device2(config)#interface gigabitethernet1
Device2(config-if-gigabitethernet1)#ipv6 router ospf 100 area 0
Device2(config-if-gigabitethernet1)#exit
```

#Configure OSPFv3 on Device3.

```
Device3#configure terminal
Device3(config)#ipv6 router ospf 100
Device3(config-ospf6)#router-id 3.3.3.3
Device3(config-ospf6)#exit
Device3(config)#interface gigabitethernet0
Device3(config-if-gigabitethernet0)#ipv6 router ospf 100 area 0
Device3(config-if-gigabitethernet0)#exit
```

#View the route table on the device.

Take Device1 as an example:

```
Device1#show ipv6 route
Codes: C - Connected, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management



L   ::1/128 [0/0]
      via ::, 3d:00:05:42, lo0
LC  1::1/128 [0/0]
      via ::, 3d:00:04:55, loopback0
O   2::1/128 [110/1]
      via fe80::201:7aff:fe94:9a32, 3d:00:00:56, gigabitethernet0
O   3::1/128 [110/2]
      via fe80::201:7aff:fe94:9a32, 3d:00:01:56, gigabitethernet0
C   2001:1::/64 [0/0]
      via ::, 3d:00:01:51, gigabitethernet0
L   2001:1::1/128 [0/0]
      via ::, 3d:00:01:51, gigabitethernet0
O   2001:2::/64 [110/1]
      via fe80::201:7aff:fe94:9a32, 3d:00:02:00, gigabitethernet0
```

You can see that there are routes to loopback0 interfaces of Device2 and Device3 in the routing table of Device1.

Note:

- For the checking method of Device2 and Device3, refer to Device1.

Step 3: Enable MPLS IP and IPv6 MPLS LDP.

#On Device1, enable MPLS IP and IPv6 MPLS LDP globally, and enable MPLS IP and IPv6 MPLS LDP on the interface at the same time.

```
Device1(config)#mpls ip
Device1(config)#mpls ldp
Device1(config-ldp)#router-id 1.1.1.1
Device1(config-ldp)#address-family ipv6
Device1(config-ldp-af6)#transport-address 1::1
Device1(config-ldp-af6)#exit
Device1(config-ldp)#exit
```

```
Device1(config)#interface gigabitethernet0
Device1(config-if-gigabitethernet0)#mpls ip
Device1(config-if-gigabitethernet0)#mpls ldp ipv6
Device1(config-if-gigabitethernet0)#exit
```

#On Device2, enable MPLS IP and IPv6 MPLS LDP globally, and enable MPLS IP and IPv6 MPLS LDP on the interface at the same time.

```
Device2(config)#mpls ip
Device2(config)#mpls ldp
Device2(config-ldp)#router-id 2.2.2.2
Device2(config-ldp)#address-family ipv6
Device2(config-ldp-af6)#transport-address 2::1
Device2(config-ldp-af6)#exit
Device2(config-ldp)#exit
Device2(config)#interface gigabitethernet0
Device2(config-if-gigabitethernet0)#mpls ip
Device2(config-if-gigabitethernet0)#mpls ldp ipv6
Device2(config-if-gigabitethernet0)#exit
Device2(config)#interface gigabitethernet1
Device2(config-if-gigabitethernet1)#mpls ip
Device2(config-if-gigabitethernet1)#mpls ldp ipv6
Device2(config-if-gigabitethernet1)#exit
```

#On Device3, enable MPLS IP and IPv6 MPLS LDP globally, and enable MPLS IP and IPv6 MPLS LDP on the interface at the same time.

```
Device3(config)#mpls ip
Device3(config)#mpls ldp
Device3(config-ldp)#router-id 3.3.3.3
Device3(config-ldp)#address-family ipv6
Device3(config-ldp-af6)#transport-address 3::1
Device3(config-ldp-af6)#exit
Device3(config-ldp)#exit
Device3(config)#interface gigabitethernet0
Device3(config-if-gigabitethernet0)#mpls ip
Device3(config-if-gigabitethernet0)#mpls ldp ipv6
Device3(config-if-gigabitethernet0)#exit
```

Note:

- router-id and transport-address can be configured manually or generated automatically. If router-id and transport-address are not configured manually, the device will select

automatically. From the interfaces in the up state, first select the largest IP address in the loopback interfaces; If the loopback interface address is not configured for the device, select the largest IP address in the normal interfaces. router-id must be configured manually for IPv6 single stack environment.

Step 4: Check the result.

#On the device, view the LDP session information.

Take Device1 as an example:

```
Device1#show mpls ldp ipv6 session
Peer IPv6 Address                Peer Type     My Role   State        DS Cap
DeadTime
2::1                             Multicast     Passive   OPERATIONAL  Disabled    00:02:54
Statistics for ldp ipv6 sessions:
    Multicast sessions: 1
    Targeted sessions: 0
```

From the display of the State column as OPERATIONAL, it can be seen that Device1 and Device2 successfully established an LDP session.

#View the routing label information on the device.

Take Device1 as an example:

```
Device1#show ipv6 route 2::1
Codes: C - Connected, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
    U - Per-user Static route
    O - OSPF, OE-OSPF External, M - Management



O   2::1/128 [110/1]
    via fe80::201:7aff:fe94:9a32 [1], label 3, 3d:00:02:50, gigabitethernet0
      fe80::201:7aff:fe94:9a32 [0], gigabitethernet0

Device1#show ipv6 route 3::1
Codes: C - Connected, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
    U - Per-user Static route
    O - OSPF, OE-OSPF External, M - Management



O   3::1/128 [110/2]
    via fe80::201:7aff:fe94:9a32 [1], label 24016, 3d:00:03:50, gigabitethernet0
```

```
fe80::201:7aff:fe94:9a32 [0], gigabitethernet0
```

You can see the route label information to loopback0 interface addresses of Device2 and Device3 on Device1.

#View THE LSP information on each device.

Take Device1 as an example:

```
Device1#show mpls ldp ipv6 lsp

FEC IPV6:1::1/128 -> ::, loopback0
 Downstream state: Established Label: none RequestID: 0 Peer: EGRESS Attr: None
  Upstream state: Established Label: impl-null(3) RequestID: 0 Peer: 2::1 Attr: None

FEC IPV6:2::1/128 -> fe80::201:7aff:fe94:9a32, gigabitethernet0
 Downstream state: Established Label: impl-null(3) RequestID: 0 Peer: 2::1 Attr: None

FEC IPV6:3::1/128 -> fe80::201:7aff:fe94:9a32, gigabitethernet0
 Downstream state: Established Label: 24016 RequestID: 0 Peer: 2::1 Attr: None

FEC IPV6:2001:1::/64 -> ::, gigabitethernet0

FEC IPV6:2001:2::/64 -> fe80::201:7aff:fe94:9a32, gigabitethernet0
```

It can be seen that there is the LSP information of the corresponding FEC of the loopback0 interface addresses of Device2 and Device3 on Device1.

3. MPLS L3VPN

3.1. Overview

MPLS L3VPN is one network technology of permitting the service provider to use its IP backbone network to provide the L3 VPN service for the user. In the MPLS L3VPN network, BGP is used to release the VPN route information in the backbone network of the service provider. MPLS is used to forward the VPN service from one VPN site to another site.

VRF (VPN Routing/Forwarding Instance) is one basic concept in the MPLS L3VPN network technology. Each VRF can be seen as one virtual router and owns one separate route table. Meanwhile, VRF has the separate address space, one group of interface set belonging to the VRF, and one group of route protocol only used by the VRF. The VRF technology can be used to separate different VPN users and solve the problem of the network address overlapping.

The following figure is the diagram of the MPLS L3VPN network architecture.

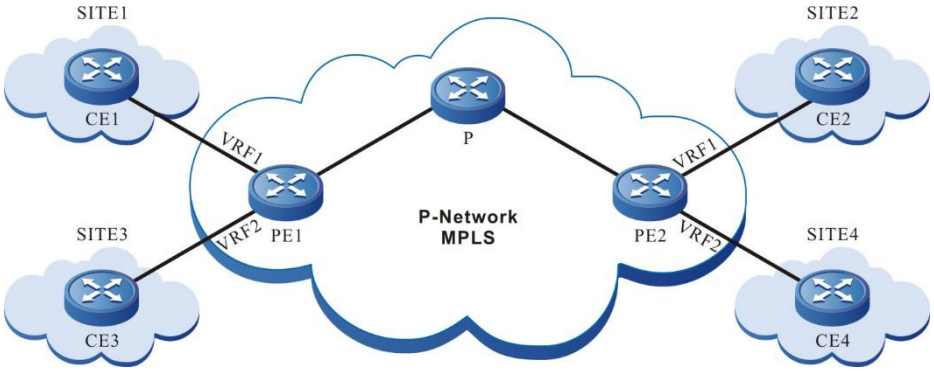

Figure 3-1 MPLS L3VPN networking

In the above figure, each PE contains two VRFs, connecting two sites. The two interfaces connecting the sites belong to two VRFs respectively. Site 1 and site 2 belong to one VPN. Site 3 and site 4 belong to the other VPN.

3.2. MPLS L3VPN Function Configuration

Table 3-1 MPLS L3VPN function configuration list

Configuration Task	
Configure the VPN basic functions	Configure the VPN instance
	Configure PE-PE route exchange
	Configure PE-CE route exchange
Configure M-VRF	Configure M-VRF
Configure the VPN route label distributing	Configure the VPN route label distributing

Configuration Task	
Configure the VPN cross-domain	Configure the Option-A cross-domain
	Configure the Option-B cross-domain
	Configure the Option-C cross-domain
Configure the VPN user to access Internet	Configure CE to access Internet
	Configure PE to access Internet
Configure the AS covering	Configure the AS covering
Configure the OSPF sham link	Configure the OSPF sham link
Configure VPN ORF	Configure VPN ORF

3.2.1. Configure VPN Basic Functions

Configuration Condition

Before configuring the VPN basic functions, first complete the following tasks:

- Configure the IGP of the MPLS backbone network, making the IP between the PE devices reachable
- Configure the MPLS basic capability and LDP of the MPLS backbone network, and set up LSP between PE devices

Configure VPN Instance

VRF can separate the routes between different VPNs, between VPN and public network. When configuring L3VPN, it is necessary to configure the VPN instance on the PE device and associate the Site in the VPN instance.

1. Configure VRF

VRF is used to separate different VPN users. In different VRFs, permit the address overlapping. When the VRF route is transmitted in the service provider network, it is sure to solve the problem of address overlapping. This requires that each VRF needs one local unique RD. When PE sends the VRF route to the remote PE, add RD to the front of each IPv4 prefix, forming the unique VPNv4 address.

Table 3-2 Configure VRF

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Create one VRF and enter the VRF configuration mode	**ip vrf** *vrf-name*	Mandatory By default, do not configure any VRF.
Configure the VRF RD	**rd** *route-distinguisher*	Mandatory By default, do not configure the RD of the VRF.

Note:

- After configuring VRF, you should configure RD at the same time so that VRF can be used.
- After configuring the VRF RD, you cannot directly delete or modify it. When it is necessary to delete or modify, use the **no ip vrf** command to delete VRF, and then configure RD. The RD cannot be the same as the other VRF RD of the device.

2. Configure VRF to associate with the interface

The PE device connects with the CE via the local configured VRF. The interface connected with the CE needs to associate with the corresponding VRF.

Table 3-3 Configure the VRF to associate with the interface

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the interface configuration mode	**interface** *interface-name*	-
Configure the interface to associate with VRF	**ip vrf forwarding** *vrf-name*	Mandatory By default, the interface does not associate with any VRF.
Configure the interface IP address	**ip address** *ip-address* { *network-mask* | *mask-len* }	Mandatory By default, the interface is not configured with the IP address.

Note:

- After configuring the **ip vrf forwarding** command in the interface, the existing IP address of the interface will be deleted automatically and needs to be configured again.

3. Configure the VRF attribute

When the local PE receives the VPNv4 route information sent by the remote PE device, the local PE device needs to confirm in which local VRF the VPNv4 route is placed. To control the distributing of the VPNv4 route, each VRF needs one or multiple RT attributes. There are two kinds of RT attributes: Export RT and Import RT. When the PE initiates the VPNv4 route, carry the Export RT attribute. When the PE decides which VRF the VPNv4 route is imported to, use the Export RT attribute carried by the route to match with the Import RT of the local VRF.

Besides that the VRF RT attribute can control the distributing of the VPNv4 route, the route policy on VRF also can control the route distributing. Two route policies can be configured: Import map and Import map. Import map uses the route map to control whether the route can import the VRF. Export map uses the route map to change the attributes of the route initiated from the VRF.

Table 3-4 Configure the VRF attributes

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Create one VRF and enter the VRF configuration mode	**ip vrf** *vrf-name*	Mandatory By default, do not configure any VRF.
Configure the VRF RT	**route-target** [**both** | **export** | **import**] { *ASN:nn* | *IP-address:nn* }	Optional By default, do not configure the Export, Import RT attributes of the VRF.
Configure the VRF ingress route policy	**import map** *rtmap-name*	Optional By default, do not configure the VRF ingress route policy.
Configure the VRF egress route policy	**export map** *rtmap-name*	Optional By default, do not configure the VRF egress route policy.

Note:

- The Import map policy is valid for the local route and remote VPN route.
- The Export map policy is valid only for the local route.

- Export map cannot perform the route filter, but can only modify the attributes of the VPN route released by the VRF. The attributes that can be modified include: community, extcommunity, and local-preference.
- When the PE imports the VPNv4 to the VRF, the RT match rule has higher priority than Import map, that is, first match the RT rule, and then match the Import map

Configure PE-PE Route Exchange

In the MPLS L3VPN network, the PEs exchange the VPNv4 route via MP-IBGP. The configuration modes of the two PEs are the same.

Table 3-5 Configure PE-PE route exchange

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enable the BGP protocol and enter the BGP configuration mode	**router bgp** *autonomous-system*	-
Configure the PE neighbor	**neighbor** { *neighbor-address* | *peer-group-name* } **remote-as** *as-number*	Mandatory By default, do not configure any PE neighbor.
Configure the source address used by setting up the PE neighbor	**neighbor** { *neighbor-address* | *peer-group-name* } **update-source** { *interface* | *ip-address* }	Mandatory By default, use the egress interface address to the PE neighbor route as the source address.
Enter the BGP VPNv4 configuration mode	**address-family vpnv4** [**unicast**]	-
Activate the VPNv4 address family of the PE neighbor	**neighbor** { *neighbor-address* | *peer-group-name* } **activate**	Mandatory By default, the BGP neighbors can only receive and send the IPv4 unicast route.

Step	Command	Description
Configure sending the extended community attributes to the PE neighbor	**neighbor** { *neighbor-address* | *peer-group-name* } **send-community** [**both** | **extended** | **standard**]	Optional By default, the VPNv4 address family of the activated neighbor will automatically configure sending the extended community attribute.
Configure VPNv4 route suppression function	**bgp dampening [ibgp]** [*reach-half-life* [*reuse-value suppress-value max-suppress-time* [*unreach-half-life*]] | **route-map** *rtmap-name*]	Optional By default, do not enable the VPNv4 route suppression function.

Note:

- Many route features in the BGP VPNv4 address family are the same as the route features in the BGP IPv4 unicast address family. Whether to select the features is decided by the networking demands. For details, refer to the MPLS L3VPN chapter of the technical manual.

Configure PE-CE Route Exchange

PE and CE can use the static route, RIP, OSPF, ISIS and BGP route protocol to exchange the route. Which protocol is adopted depends on the actual network environment. The PE configuration is the same as the CE configuration mode.

1. Configure PE-CE to use static route

Table 3-6 Configure PE-CE to use the static route

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Configure the static route to the CE	**ip route vrf** *vrf-name destination-ip-address destination-mask nexthop-ip-address*	Mandatory By default, do not configure the static route to the CE.
Enable the BGP protocol and enter the BGP configuration mode	**router bgp** *autonomous-system*	-

Step	Command	Description
Enter the BGP IPv4 VRF configuration mode	**address-family ipv4 vrf** *vrf-name*	Mandatory By default, it is in the BGP IPv4 unicast configuration mode.
Configure BGP to re-distribute the static route	**redistribute static** [**route-map** *map-name* / **metric** *value*]	Optional By default, do not configure BGP to re-distribute the static route.

2.Configure PE-CE to use RIP

Table 3-7 Configure PE-CE to use RIP

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enable the RIP protocol and enter the RIP configuration mode	**router rip**	Mandatory By default, do not enable RIP.
Enter the VRF address family configuration mode of the RIP protocol	**address-family ipv4 vrf** *vrf-name*	Mandatory By default, do not enable the VRF address family of the RIP protocol.
Configure the RIP version in the VRF address family mode	**version** {1 | 2}	Mandatory By default, the RIP version is 1. Usually modify it to version 2.
Configure RIP to cover the connected interface of the PE and CE	**network** [*network-address* | *interface*]	Mandatory By default, RIP does not cover the connected interface of the PE and CE.

Step	Command	Description
Exit the VRF address family configuration mode of the RIP protocol	**exit-address-family**	-
Exit the RIP configuration mode	**exit**	-
Enable the BGP protocol and enter the BGP configuration mode	**router bgp** *autonomous-system*	-
Enter the BGP IPv4 VRF configuration mode	**address-family ipv4 vrf** *vrf-name*	Mandatory By default, it is in the BGP IPv4 unicast configuration mode.
Configure the BGP to re-distribute RIP	**redistribute rip** [**route-map** *map-name* / **metric** *value*]	Optional By default, do not re-distribute the RIP protocol route.

3.Configure PE-CE to use OSPF

Table 3-8 Configure PE-CE to use OSPF

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Create one OSPF process and enter the OSPF configuration mode	**router ospf** *process-id* **vrf** *vrf-name*	Mandatory In VRF, enable the OSPF process. By default, the system does not enable the OSPF protocol. When enabling OSPF in the VRF, the OSPF process belonging to one VRF can only manage the interfaces belonging to the VRF.

Step	Command	Description
Configure OSPF to cover the connected interface of the PE and CE	**network** *ip-address wildcard-mask* **area** *area-id*	Mandatory By default, the interface does not belong to any OSPF process or area. One interface can only belong to one OSPF process and area.
Exit the OSPF configuration mode	**exit**	-
Enable the BGP protocol and enter the BGP configuration mode	**router bgp** *autonomous-system*	-
Enter the BGP IPv4 VRF configuration mode	**address-family ipv4 vrf** *vrf-name*	Mandatory By default, it is in the BGP IPv4 unicast configuration mode.
Configure BGP to re-distribute OSPF	**redistribute ospf** *as-number* [**route-map** *map-name* / **metric** *value* / **match** *level*]	Optional By default, do not re-distribute the OSPF protocol route.

4.Configure PE-CE to use ISIS

Table 3-9 Configure PE-CE to use ISIS

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the IS-IS configuration mode	**router isis** [*instance-name*]	-
Configure the network entity title for ISIS	**net** *entry-title*	Mandatory By default, ISIS does not have the network entity title.

Step	Command	Description
Configure the VRF attribute of the ISIS	**vrf** *vrf-name*	Optional By default, the ISIS process is in the global VRF.
Return to the global configuration mode	**exit**	-
Enter the interface configuration mode	**interface** *interface-name*	-
Configure the interface to associate the VRF instance	**ip vrf forwarding** *vrf-name*	Mandatory By default, the interface does not associate any VRF.
The interface enables the IS-IS protocol	**ip router isis** [*instance-name*]	Mandatory By default, the interface does not enable the IS-IS protocol.
Return to the global configuration mode	**exit**	-
Enable the BGP protocol and enter the BGP configuration mode	**router bgp** *autonomous-system*	-
Enter the BGP IPv4 VRF configuration mode	**address-family ipv4 vrf** *vrf-name*	Mandatory By default, the system is in the BGP IPv4 unicast configuration mode.
Configure BGP to re-distribute ISIS	**redistribute isis** [*instance-name*] [**route-map** *map-name* / **metric** *value* / **match** *level*]	Optional By default, do not re-distribute the IS-IS protocol route.

5.Configure PE-CE to use BGP

Table 3-10 Configure PE-CE to use BGP

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enable the BGP protocol and enter the BGP configuration mode	**router bgp** *autonomous-system*	-
Enter the BGP IPv4 VRF configuration mode	**address-family ipv4 vrf** *vrf-name*	Mandatory By default, the system is in the BGP IPv4 unicast configuration mode.
Configure CE as the EBGP neighbor	**neighbor** { *neighbor-address* | *peer-group-name* } **remote-as** *as-number*	Mandatory By default, do not configure any CE neighbor.

Configure BGP to Use RT for ORF Filter Function

This function only works in VPN-TARGET address family mode and is enabled by default. Do not support configuring the neighbor peer group. According to RFC 4684, it is not recommended to disable. After BGP learns RT NLRI, as long as the prefix information has the RT information, it can use the learned RT NLRI information to perform the corresponding policy control. It can also allow users not to give RT policy control. This command provides this option, command asynchronous processing.

Table 3-11 Configure BGP to use RT for the ORF filter function

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the BGP configuration mode	**router bgp** *autonomous-system*	-
Enter the VPN-TARGET address family configuration mode	**address-family ipv4 vpn-target**	Mandatory By default, BGP does not enter the VPN-TARGET address family mode.
Configure the neighbor to use RT for the ORF filter function	**neighbor** *neighbor-address* **constraint-rt-filter enable**	Optional By default, using RT for the ORF filter is enabled by default.
Configure the neighbor not to use RT for the ORF filter function	**neighbor** *neighbor-address* **constraint-rt-filter disable**	Mandatory By default, disable using RT for the ORF filter.

Note:

- Configure whether to permit the RT ORF function, only working in the filtering when advertising the VPN route. For example, when receiving the peer RT NLRI, no matter whether to enable the RT-Filter function, it needs to start the VPN route update releasing timer, and update the VPN route. You need to judge whether to enable RT-Filter only when performing the egress filter for VPN. In this way, for CISCO-like devices, there is no problem if not sending the Refresh packet after activating the VPN-Target address family.

Configure BGP to Set the RT Filter Table Installation Items of EBGP Neighbor

For the VPN-RT routes learned from the EBGP neighbor, besides the best route, permit the non-best route to install the RT filter table of the neighbor.

Table 3-12 Configure the BGP max, load balance items

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the BGP configuration mode	**router bgp** *autonomous-system*	-
Enter the VPN-TARGET address family configuration mode	**address-family ipv4 vpn-target**	Mandatory By default, BGP does not enter the VPN-TARGET address family mode.
Set the RT filter table installation items of the EBGP neighbor	**rt-filter external-path** *path-number*	Mandatory By default, only install one best route.

3.2.2. Configure M-VRF

Configuration Condition

Before configuring M-VRF, first complete the following task:

- Configure the link-layer protocol of the connecting interfaces of the M-VRF device with the PE and site and keep connected

Configure M-VRF

M-VRF is one cheap method of expanding the VPN function to the CE. When the customer has multiple services, do not need to divide multiple services to one CE, but configure multiple VRFs on the M-VRF device, virtualizing multiple CEs and separating each service. The following describes one M-VRF example.

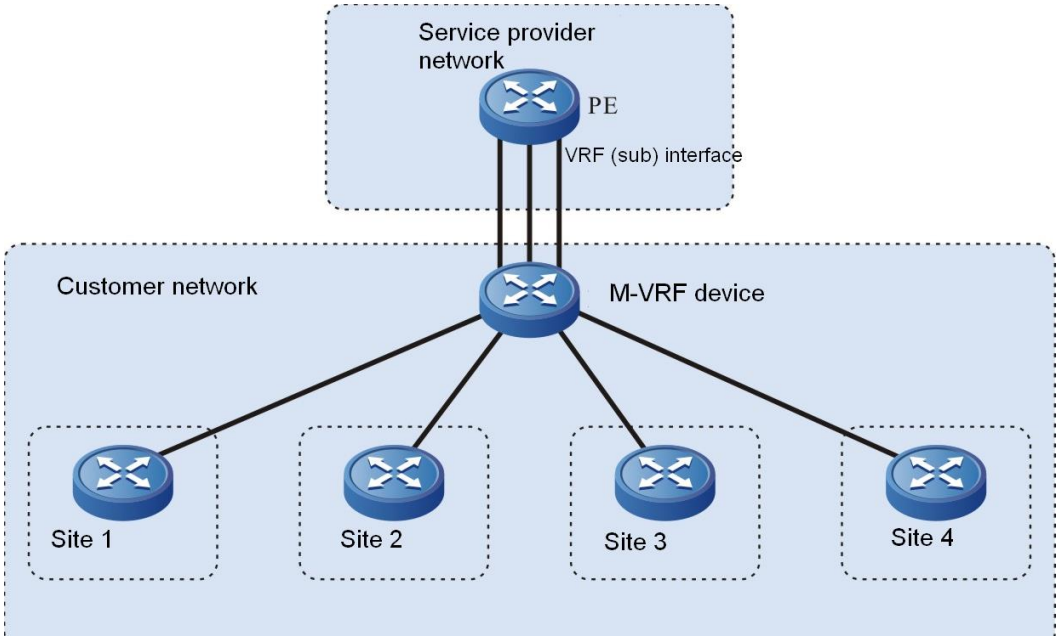

Figure 3-2 Networking of configuring M-VRF

On the M-VRF device, each VRF has one interface to connect the site and the other interface connects the PE. Usually, the M-VRF device is connected with the PE via the Ethernet link. Each VRF uses one interface (or sub interface).

1.Configure the route exchange between the M-VRF device and PE

The route exchange between the M-VRF device and the CE can use the static route, RIP, OSPF, ISIS and BGP route protocol. The following example uses the RIP to exchange the route.

Table 3-13 Configure the route exchange between the M-VRF device and PE

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Create one VRF and enter the VRF configuration mode	**ip vrf** *vrf-name*	Mandatory By default, do not configure any VRF.
Configure the VRF RD	**rd** *route-distinguisher*	Mandatory By default, do not configure the VRF RD.
Exit the VRF configuration mode	**exit**	-

Step	Command	Description
Enter the interface configuration mode	**interface** *interface_name*	-
Configure the interface to associate with the VRF	**ip vrf forwarding** *vrf-name*	Mandatory By default, the interface is not associated with any VRF.
Configure the interface IP address	**ip address** *ip-address* { *network-mask* | *mask-len* }	Mandatory By default, the interface is not configured with the IP address.
Exit the interface configuration mode	**exit**	-
Enable the RIP protocol and enter the RIP configuration mode	**router rip**	Mandatory By default, do not enable RIP.
Enter the VRF address family configuration mode of the RIP protocol	**address-family ipv4 vrf** *vrf-name*	Mandatory By default, the RIP protocol does not enable the VRF address family.
Configure the RIP version in the VRF address family mode	**version** {1 | 2}	Mandatory By default, RIP version is 1.
Configure RIP to cover the connected interface of the M-VRF device and PE	**network** [*network-address* | *interface*]	Mandatory By default, RIP does not cover the connected interface of the M-VRF device and PE.

Note:

- On the M-VRF device, each VRF should be configured according to the above steps.
- For the configuration of the PE, refer to the part of “Configure VPN basic functions”.

2.Configure the route exchange between the M-VRF device and site

The route exchange between the M-VRF device and the site, you can use the static route, RIP, OSPF, ISIS and BGP route protocol. The following example uses the static route.

Table 3-14 Configure the route exchange between the M-VRF and site

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Create one VRF and enter the VRF configuration mode	**ip vrf** *vrf-name*	Mandatory By default, do not configure any VRF.
Configure the VRF RD	**rd** *route-distinguisher*	Mandatory By default, do not configure the VRF RD.
Exit the VPN instance configuration mode	**exit**	-
Enter the interface configuration mode	**interface** *interface_name*	-
Configure the interface to associate with the VRF	**ip vrf forwarding** *vrf-name*	Mandatory By default, the interface does not associate with any VRF.
Configure the interface IP address	**ip address** *ip-address* { *network-mask* | *mask-len* }	Mandatory By default, the interface is not configured with the IP address.
Exit the interface configuration mode	**exit**	-
Configure the static route to the site	**ip route vrf** *vrf-name destination-ip-address destination-mask nexthop-ip-address*	Mandatory By default, do not configure the static route to the site.

Note:

- On the M-VRF device, each VRF should be configured according to the above steps.
- The configuration mode on the site is the same as the common static route configuration.

Configure VPN Route Label Distributing

Configuration Condition

Before configuring the VPN route label distributing mode, first complete the following task:

- Configure VPN basic functions

Configure VPN Route Label Distributing

BGP has two modes of distributing the label for the VPN route: per-route label distributing mode and per-VRF label distributing mode. When adopting the per-route mode, BGP distributes different labels for each VPN route. When adopting per-VRF mode, BGP distributes the same label for the VPN routes in one VRF, but distributes different labels for the routes in different VRFs.

By default, BGP adopts the per-VRF label distributing mode. The mode can save the label resources. When there are lots of local released VPN routes, the per-VRF label distributing mode can reduce the generating of the ILM entries and improve the performance.

Table 3-15 Configure the VPN route label distributing

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enable the BGP protocol and enter the BGP configuration mode	**router bgp** *autonomous-system*	-
Configure the per-route label distributing mode	**no unque-label-per-vrf**	Optional By default, enable the per-VRF label distributing mode.

3.2.3. Configure VPN Cross-Domain

Configuration Condition

Before configuring the VPN cross-domain, first complete the following tasks:

- Configure the VPN basic functions
- Configure the ASBR direct-connected IP address, making the IP between ASBRs reachable

Configure Option-A Cross-Domain

Option-A cross-domain is also called VRF-to-VRF and it is the simplest mode of realizing the VPN access between AS. VRF-to-VRF takes another ASBR as the CE device to process the VPNv4 connectivity between AS. The following describes one VRF-to-VRF.

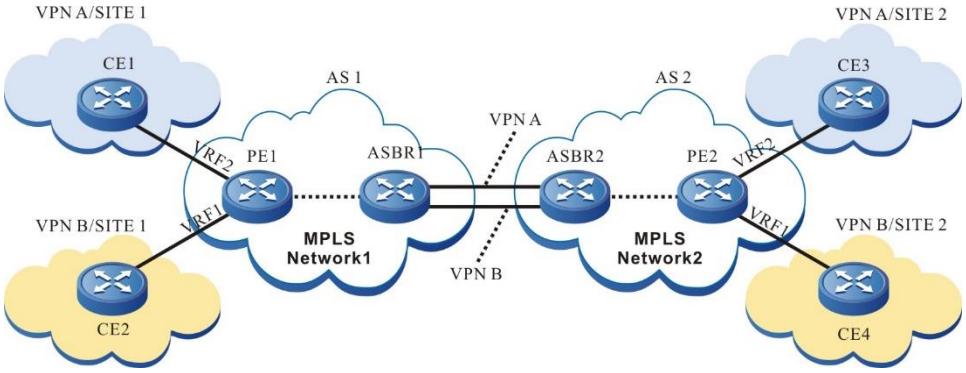

Figure 3-3 Configure Option-A cross-domain (VRF-to-VRF)

In the above figure, VPN site 1 and site 2 are connected to two different service providers respectively: AS1 and AS2. The service providers are connected via ASBR. Two AS areas configure the MPLS L3VPN network. The VPN crossing the AS needs the local ASBR to serve as the PE device of the VPN and the peer ASBR to serve as the CE device of the VPN. Meanwhile, on two ASBR devices, configure the VRF of the VPN. In this way, the VPN route transmits the VPNv4 route via MP-IBGP in the AS. ASBR transmits the unicast route in the VRF of the VPN, so as to realize the inter-connection of site 1 and site 2.

The advantage of the VRF-to-VRF mode is that it is necessary to run MPLS between ASBR. The disadvantage is that ASBR needs to maintain all VPN routes and distribute the interface and link for each cross-domain VPN. Therefore, the expansibility is poor.

For the configuration of the VRF-to-VRF cross-domain mode, refer to the part of “Configure VPN Basic Functions”.

Configure Option-B Cross-Domain

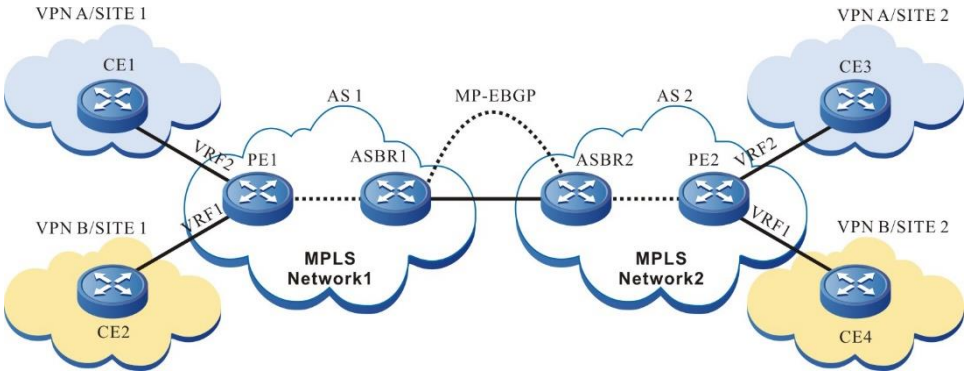

Figure 3-4 Configure Option-B cross-domain (MP-EBGP carries the VPNv4 route)

Option-B cross-domain needs to run MP-EBGP between ASBR. After ASBR learns all VPN routes of the local AS PE, distribute the new label for the VPN route, and then advertise the route information and new label to the peer ASBR. ASBR needs to maintain all VPN routes received from the local PE and the peer ASBR.

Option-B cross-domain does not need ASBR to configure the VRF for each VPN, does not need to import the VPNv4 route, and does not need to distribute the interface for each VPN, but ASBR still needs to maintain all VPNv4 routes, and distribute the new label for each label. Install the ILM entry of the old and new label translation at the local. Therefore, ASBR has the good load capability.

Table 3-16 Configure Option-B cross-domain

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enable the MPLS forwarding globally	**mpls ip**	Mandatory By default, do not enable the MPLS forwarding.
Enter the interface configuration mode	**interface** *interface_name*	-
Enable the MPLS forwarding on the interface	**mpls ip**	Mandatory Configure on the interconnection interfaces of the two ASBR. By default, do not enable the MPLS forwarding on the interface.
Return to the global configuration mode	**exit**	-
Enable the BGP protocol and enter the BGP configuration mode	**router bgp** *autonomous-system*	-
Configure the peer ASBR as the EBGP neighbor	**neighbor** { *neighbor-address* | *peer-group-name* } **remote-as** *as-number*	Mandatory By default, do not configure any EBGP neighbor.
Enter the BGP VPNv4 configuration mode	**address-family vpnv4** [**unicast**]	Mandatory By default, the system is in the BGP IPv4 unicast configuration mode.
Activate the MP-EBGP neighbor to advertise the VPN route	**neighbor** { *neighbor-address* | *peer-group-name* } **activate**	Mandatory By default, BGP only advertises the IPv4 unicast route.

Step	Command	Description
Configure changing the next hop when advertising the route to the PE	**neighbor** { *neighbor-address* | *peer-group-name* } **next-hop-self**	Mandatory By default, do not configure changing the next hop when advertising the route to the PE.

Note:

- The above just lists the basic configuration of the Option-B cross-domain on ASBR. For the configuration of the ASBR and the PE, P devices in the AS, refer to the part of “Configure VPN Basic Functions”.

3.2.4. Configure VPN User to Access Internet

Configuration Condition

Before configuring the VPN user to access Internet, first complete the following task:

- Configure VPN basic functions

Configure CE to Access Internet

In the actual application environment, the customer does not hope the VPN user to access Internet directly, but requires controlling the connection of the VPN user with Internet via the security devices, such as firewall. Each VPN site sends the Internet data flow to the central site. The VPN member forwards the data flow of the accessed Internet to the central site by importing one default route of accessing Internet (the next hop is the central site CE). The central site forwards the data flow of the accessed Internet to the enterprise firewall. Perform the necessary access control and NAT processing in the firewall according to the made security policy. At last, the firewall forwards the data flow to Internet. The following figure describes one instance of using CE to access Internet.

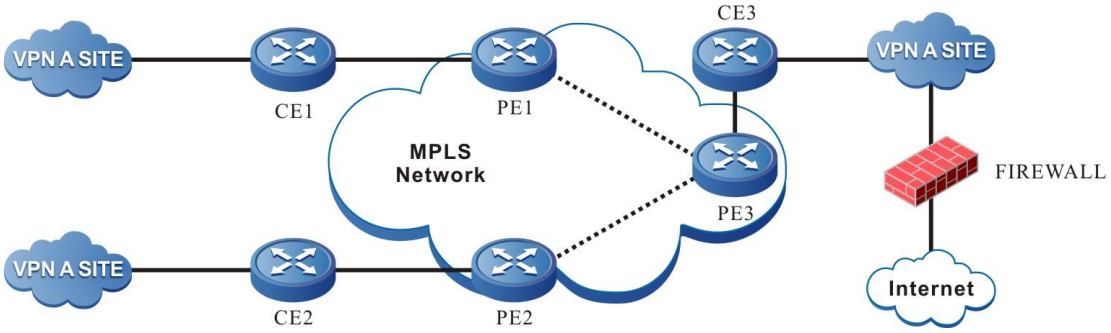

Figure 3-5 Configure CE to access Internet

In the above figure, CE3 serves as the central site of the customer controlling Internet access. You just need to configure the next hop as the default route of Internet gateway on CE3. The route is transmitted to the PE device via the route exchange of PE-CE, and then transmitted to the VPN site via MP-IBGP. In this way, each VPN site can access Internet via the default route (the next hop is PE3). The data of the accessed Internet first reaches CE3 via MPLS, and then reaches Internet via the configured default route on CE3.

The CE access mode just needs to be configured and deployed in the VPN, but does not need the carrier to take part in. The user can freely control the security policy of the internal user

accessing Internet. However, the mode requires the user to have strong security management capability, and the carrier cannot manage the user accessing Internet in a unified manner.

Table 3-17 Configure CE to access Internet

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
On the central site CE, configure the default route and the next hop is Internet gateway	**ip route** *destination-ip-address destination-mask nexthop-ip-address*	Mandatory By default, CE does not configure the default route of access Internet.

Note:

- For the configuration of the other device, refer to the part of “Configure VPN Basic Functions”.

Configure PE to Access Internet

Forward the traffic of the VPN user to the Internet gateway of the service provider network to provide the Internet access for the VPN user. The mode is called PE accessing Internet. To provide the Internet access for the VPN user, the global route table on the PE should be able to forward the VPN traffic. This need to create one static route in the VRF of the PE and the next hop is realized in the global route table mode. The following figure describes one instance of the PE accessing Internet.

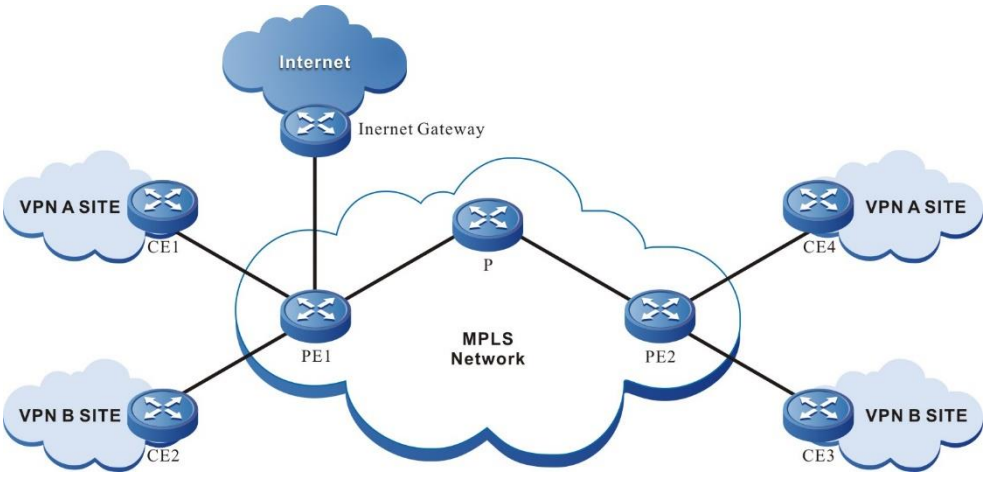

Figure 3-6 Configure CE to access Internet

In the above figure, VPN A has two users CE1 and CE2 to access Internet. First, configure one cross-VRF default static route of accessing Internet in the VRF route table of PE1 and PE2 respectively. The next hop of the cross-VRF default static route in PE1 is Internet gateway, and the next hop of the cross-VRF default static route in PE2 is PE1. To ensure that the packet returned from Internet can return to CE1 and CE4 successfully, you also need to configure one cross-VRF route to CE1 in the global route table of PE1 and the next hop is the CE1 in the VRF. In the global route table of PE2, you also need to configure one cross-VRF route to CE4, the next hop is CE4 in VRF, and advertise the route to the MPLS network via IGP.

Table 3-18 Configure the PE to access Internet

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
In the VRF route table of PE, configure the cross-VRF default static route of accessing Internet and the next hop is Internet gateway	**ip route vrf** *vrf-name destination-ip-address destination-mask nexthop-ip-address* **vrf global**	Mandatory By default, do not configure the deault static route of accessing Internet.
In the global route table of the PE, configure the cross-VRF static route to CE, and the next hop is CE	**ip route** *destination-ip-address destination-mask nexthop-ip-address* **vrf** *vrf-name*	Mandatory By default, do not configure PE-CE cross-VRF static route.

Note:

- The above is the key configuration of the PE (PE1 in the figure) connecting the Internet gateway. For the other PE (such as PE2 in the figure), configure the cross-VRF default static route of accessing Internet and the next hop need to point to the loopback port address of PE1 (the loopback port of setting up the BGP neighbor).

3.2.5. Configure AS Coverage

Configuration Condition

Before configuring the AS coverage, first complete the following task:

- Configure the VPN basic functions
- Configure the PE-CE route exchange to use EBGP

Configure AS Coverage

When the PE and CE routers run BGP, the customer VPN may hope to re-use the AS number in different sites. As a result, when CP receives the PE route, the route AS-PATH attribute will contain the AS number of the CE device and the CE will drops the route from the PE. To solve the problem, PE needs to enable the BGP AS cover function. After the PE device enables the AS cover function and advertises the route to the CE neighbor, and if there is the same AS number as CE in the route AS-PATH, PE uses its own AS number to replace the AS number of the CE neighbor contained in the route AS-PATH, and then advertises to the CE neighbor.

Table 3-19 Configure the AS coverage

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enable the BGP protocol and enter the BGP configuration mode	**router bgp** *autonomous-system*	-
Enter the BGP IPv4 VRF configuration mode	**address-family ipv4 vrf** *vrf-name*	Mandatory By default, the system is in the BGP IPv4 unicast configuration mode.
Configure the AS cover function	**neighbor** { *neighbor-address* | *peer-group-name* } **as-override**	By default, do not enable the AS cover function.

3.2.6. Configure OSPF False Link

Configuration Condition

Before configuring the OSPF sham link, first complete the following task:

- Configure the VPN basic functions, configure the route exchange between PE and CE to use OPSF

Configure OSPF False Link

In the MPLS L3VPN environment, when there is the direct-associated backup link (called backdoor link) between two CE of different sites, the route in the OSPF domain is prior to the external route re-distributed by BGP, and as a result, the traffic between CEs does not pass VPN, but first passes the backdoor link. To make the traffic between two CEs first pass VPN, it is necessary to set up one OSPF sham link between two PEs.

The source address and destination address of the sham link are reachable in the BGP domain, and cannot be covered and re-distributed by OSPF. The route to the destination address of the sham link can only be learned by the BGP.

The configuration steps of the OSPF sham link on the PE are as follows:

1.Configure the VRF loopback interface

Table 3-20 Configure the VRF loopback interface

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Create one loopback interface and enter the interface configuration mode	**interface loopback** *interface-number*	Mandatory By default, do not create a loopback interface.
Configure the loopback interface to associate VRF	**ip vrf forwarding** *vrf-name*	Mandatory By default, the interface does not associate with any VRF.
Configure the IP address of the loopback interface	**ip address** *ip-address* { *mask* | *mask-length* }	Mandatory By default, do not configure the interface IP address.
Exit the interface configuration mode	**exit**	-

2.Configure BGP to re-distribute OSPF and direct-connected route of the loopback interface

Table 3-21 Configure BGP to re-distribute OSPF and the direct-connected route of the loopback interface

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enable the BGP protocol and enter the BGP configuration mode	**router bgp** *autonomous-system*	-

Step	Command	Description
Enter the BGP IPv4 VRF configuration mode	**address-family ipv4 vrf** *vrf-name*	Mandatory By default, the system is in the BGP IPv4 unicast configuration mode.
Configure BGP to re-distribute the direct-connected route of the loopback interface	**redistribute connected** [**route-map** *map-name* / **metric** *value*]	Mandatory By default, BGP does not re-distribute the direct-connected route.
Configure BGP to re-distribute OSPF	**redistribute ospf** *as-number* [**match** *route-sub-type* / **route-map** *map-name* / **metric** *value*]	Mandatory By default, BGP does not re-distribute the OSPF route.
Exit the BGP IPv4 VRF configuration mode	**exit-address-family**	-
Exit the BGP configuration mode	**exit**	-

3.Configure the OSPF sham link

Table 3-22 Configure the OSPF sham link

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Create one OSPF process and enter the OSPF configuration mode	**router ospf** *process-id* [**vrf** *vrf-name*]	Mandatory Enable or enable the OSPF process in the VRF. By default, the system does not enable the OSPF protocol. When enabling OSPF in the VRF, the OSPF process belonging to one VRF can only manage the interfaces belonging to the VRF.

Step	Command	Description
Configure the segment covered by the OSPF area	**network** *ip-address wildcard-mask* **area** *area-id*	Mandatory By default, the interface does not belong to any OSPF process or area. One interface can only belong to one OSPF process and area.
Configure the OSPF sham link	**area** *area-id* **sham-link** *source-ip-address desinationt-ip-address* [**cost** *cost*]	Mandatory *source-ip-address* is the address of the local loopback interface. *desinationt-ip-address* is the peer loopback port address. By default, do not configure the OSPF sham link.

3.2.7. Configure VPN ORF

Configuration Condition

Before configuring the VPN ORF function, first complete the following tasks:

- Enable the BGP protocol
- Configure the neighbor of the BGP VPN address family and set up the session successfully

Configure VPN ORF

In the VPN environment of BGP, the route transmitter RR will send all VPN routes to the peer PE or the peer RR. After receiving VPN routes, the peer PE or RR will filter out the unnecessary VPN routes according to the local configured IMPORT RT. In the larger VPN network, a large number of unnecessary VPN route information will be advertised and filtered in the network, causing a great waste of resources. Especially, the performance of some edge PE devices is low. When receiving a large number of VPN routes, the performance cannot be satisfied, which affects the normal VPN services.

The VPN ORF function is to solve the problem. The basic principle of VPN ORF is that the BGP router participating in VPN route distribution advertises its IMPORT RT using MP-BGP, uses the best route selection algorithm of standard BGP-4 to get the route distribution map of IMPORT, and takes the IMPORT information as ORF to perform the egress filtering for the VPN route. In this way, for the unnecessary VPN route, perform the restriction advertising at the VPN route source. In the practical network planning, RR usually plays the role, and the RR router generally has high performance.

Table 3-23 Configure the VPN ORF function

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the BGP configuration mode	**router bgp** *autonomous-system*	-
Enter the VPN-Target address family	**address-family ipv4 vpn-target**	-
Activate the neighbor in the VPN-Target address family; as for the IPv4 peer, activate the VPN-Target address family of the peer, and exchange the VPN RT information	**neighbor {** *neighbor-address* **|** *peer-group-name***} active**	-
In the VPN-Target address family, add one neighbor to the peer group	**neighbor** { *neighbor-address* } **peer-group** { *group-name* }	Optional
In the PN-Target address family mode, enable the route reflection function	**neighbor {** *neighbor-address* **|** *peer-group-name* **} route-reflector-client**	Optional
In the VPN-Target address family mode, enable advertising the default route of RT NLRI	**neighbor** { *neighbor-address* **|** *peer-group-name* } **default-originate**	Optional

Caution:

- Activating the neighbor in the VPN-Target address family only supports the IPv4 neighbor, but you can perform the egress filtering for the VPNv4 or VPNv6 route at the same time.
- Activate the neighbor in the VPN-Target address family, and usually, the neighbor is also activated in the VPNv4 address family or VPNv6 address family.

3.2.8. Configure VPN Fast Re-route

Configuration Condition

Before configuring the VPN fast re-route function, first complete the following tasks:

- Enable the BGP protocol

- Configure the neighbor of the BGP VPN address family and set up the session successfully

Configure VPN Fast Re-route

In the L3VPN network, because of the link or device fault, the packets passing the fault point will be dropped or generate loop, and the caused flow interruption cannot be restored until the protocol is re-converged, which often lasts for several seconds. To reduce the flow interruption time, you configure the VPN fast re-route. Set the backup next-hop for the matched route by applying the route map. Once the master link fails, the flow passing the master link is immediately switched to the standby link, so as to realize the fast switching.

Table 3-24 Configure VPN fast re-route

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the BGP configuration mode	**router bgp** *autonomous-system*	-
Enter the BGP VRF address family	**address-family ipv4 vrf** *vrf-name*	-
Configure the BGP fast re-route	**fast-reroute route-map** *rtmap-name*	Optional By default, do not enable the fast re-route function.

Caution:

- After configuring the VPN fast re-route to apply the route map, you can set the BGP neighbor as the backup next-hop via the **set fast-reroute backup-nexthop** *nexthop-address* command in the route map. If configuring the non-BGP neighbor as the backup next-hop, the fast re-routing function cannot take effect.
- For the scenario of VPNv4 backing up VPNv4, pay attention to the RD limitation: It is not permitted that the original RDs of the two VPN routes are the same, but different from the VRF RD. That is to say, if the original RDs of the two VPN routes are the same, it is necessary to configure the same RD for the local VRF as the route. Otherwise, the FRR backup route cannot be generated.

3.2.9. MPLS L3VPN Monitoring and Maintaining

Table 3-25 MPLS L3VPN monitoring and maintaining

Command	Description
clear ip bgp { ***** | *neighbor-address* | *as-number* | **peer-group** *peer-group-name* | **external** } [**vrf** *vrf-name* | **ipv4 unicast** | **ipv4 multicast** | **vpnv4 unicast**]	Re-set the BGP neighbor.
clear ip bgp { ***** | *neighbor-address* | *as-number* | **peer-group** *peer-group-name* | **external** } [**vpnv4 unicast** | **vrf** *vrf-name*] { [**soft**] [**in** | **out**] }	Soft-reset the neighbor.
show ip bgp vpnv4 { **all** | **vrf** *vrf-name* | **rd** *route-distinguisher* } [*ip-address* | *ip-address/mask-length*]	Display the route database information in the BGP VPNv4 address family
show ip bgp vpnv4 { **all** | **vrf** *vrf-name* | **rd** *route-distinguisher* } **dampening** [**ibgp**]{ **dampened-paths** | **flap-statistics** | **parameters** }	Display the details of the BGP VPNv4 route dampening
show ip bgp [**vpnv4** { **all** | **vrf** *vrf-name* | **rd** *route-distinguisher* }] **labels**	Display the route label information in the BGP VPNv4 address family
show ip bgp vpnv4 { **all** | **vrf** *vrf_name* **| rd** *route-distinguisher* } **neighbors** [*ip-address*]	Display the neighbor details in the BGP VPNv4 address family
show ip bgp vpnv4 { **all** | **vrf** *vrf-name* | **rd** *route-distinguisher* } **summary**	Display all neighbor information in the BGP VPNv4 address family
show ip bgp vrf *vrf-name*	Display the BGP VRF information

3.3. MPLS L3VPN Typical Configuration Example

3.3.1. Configure Intra-domain MPLS L3VPN

Network Requirements

- The whole MPLS network includes two VPNs, VPN1 and VPN2. The two VPNs uses different Route-Target, so as to ensure that two VPNs cannot communicate with each other.

- CE1 and CE3 belong to VPN1; CE2 and CE4 belong to VPN2.
- CE and PE adopt OSPF to advertise the route.
- PEs adopt OSPF as IGP to make PEs communicate with each other. Configure MP-IBGP to exchange the VPN route information.

Network Topology

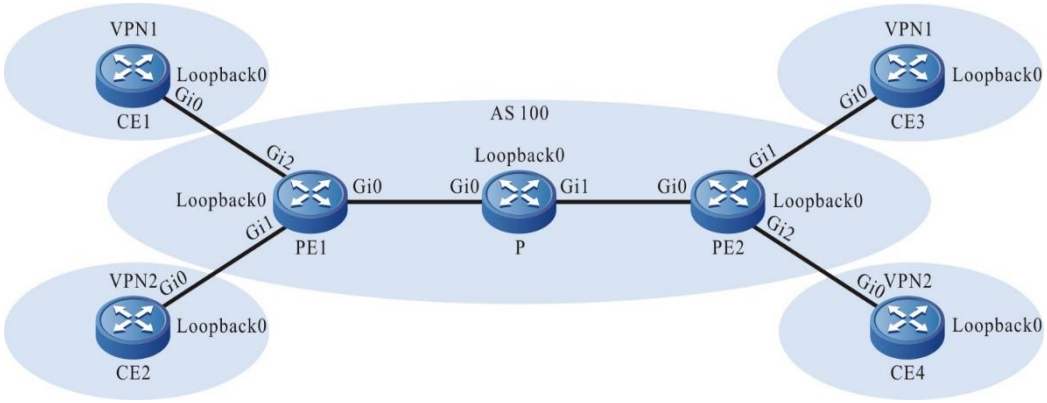

Figure 3-7Networking of configuring the intra-domain MPLS L3VPN

Device	Interface	IP Address	Device	Interface	IP Address
CE1	Gi0	95.1.1.2/16	P	Loopback0	11.11.11.11/32
	Loopback0	5.5.5.5/32	PE2	Gi0	92.1.1.1/16
PE1	Gi0	93.1.1.2/16		Gi1	90.1.1.1/16
	Gi1	94.1.1.1/16		Gi2	91.1.1.1/16
	Gi2	95.1.1.1/16		Loopback0	75.75.75.75/32
	Loopback0	90.90.90.90/32	CE3	Gi0	90.1.1.2/16
CE2	Gi0	94.1.1.2/16		Loopback0	8.8.8.8/32
	Loopback0	2.2.2.2/32	CE4	Gi0	91.1.1.2/16
P	Gi0	93.1.1.1/16		Loopback0	3.3.3.3/32
	Gi1	92.1.1.2/16			

Configuration Steps

Step 1: Configure the IP address of the interface (omitted).

Step 2: Configure the global OSPF and advertise the global route.

#Configure the global OSPF on PE1.

```
PE1#configure terminal
PE1(config)#router ospf 100
PE1(config-ospf)#network 90.90.90.90 0.0.0.0 area 0
PE1(config-ospf)#network 93.1.0.0 0.0.255.255 area 0
PE1(config-ospf)#exit
```

#Configure the global OSPF on P.

```
P#configure terminal
P(config)#router ospf 100
P(config-ospf)#network 11.11.11.11 0.0.0.0 area 0
P(config-ospf)#network 92.1.0.0 0.0.255.255 area 0
P(config-ospf)#network 93.1.0.0 0.0.255.255 area 0
P(config-ospf)#exit
```

#Configure the global OSPF on PE2.

```
PE2#configure terminal
PE2(config)#router ospf 100
PE2(config-ospf)#network 75.75.75.75 0.0.0.0 area 0
PE2(config-ospf)#network 92.1.0.0 0.0.255.255 area 0
PE2(config-ospf)#exit
```

#After the configuration is complete, view the global route table on the device.

Take PE1 as an example:

```
PE1#show ip route
Codes: C - Connected, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external




C   93.1.0.0/16 is directly connected, 00:34:54, gigabitethernet0
O   92.1.0.0/16 [110/2] via 93.1.1.1, 00:08:12, gigabitethernet0
C   90.90.90.90/32 is directly connected, 154:02:28, loopback0
O   11.11.11.11/32 [110/2] via 93.1.1.1, 00:05:12, gigabitethernet0
O   75.75.75.75/32 [110/3] via 93.1.1.1, 00:06:03, gigabitethernet0
```

You can see that there is the route information of P and PE2 loopback ports in the global route table of PE1.

Note:

- For the checking method of P and PE2, refer to PE1.

Step 3: Enable MPLS IP and MPLS LDP.

#On PE1, enable the global MPLS IP and MPLS LDP. Meanwhile, enable MPLS IP and MPLS LDP on the interface.

```
PE1(config)#mpls ip
PE1(config)#mpls ldp
PE1(config-ldp)#router-id 90.90.90.90
PE1(config-ldp)#address-family ipv4
PE1(config-ldp-af4)#transport-address 90.90.90.90
PE1(config-ldp-af4)#exit
PE1(config-ldp)#exit
PE1(config)#interface gigabitethernet0
PE1(config-if-gigabitethernet0)#mpls ip
PE1(config-if-gigabitethernet0)#mpls ldp
PE1(config-if-gigabitethernet0)#exit
```

#On P, enable the global MPLS IP and MPLS LDP. Meanwhile, enable MPLS IP and MPLS LDP on the interface.

```
P(config)#mpls ip
P(config)#mpls ldp
P(config-ldp)#router-id 11.11.11.11
P(config-ldp)#address-family ipv4
P(config-ldp-af4)#transport-address 11.11.11.11
P(config-ldp-af4)#exit
P(config-ldp)#exit
P(config)#interface gigabitethernet0
P(config-if-gigabitethernet0)#mpls ip
P(config-if-gigabitethernet0)#mpls ldp
P(config-if-gigabitethernet0)#exit
P(config)#interface gigabitethernet1
P(config-if-gigabitethernet1)#mpls ip
P(config-if-gigabitethernet1)#mpls ldp
P(config-if-gigabitethernet1)#exit
```

#On PE2, enable the global MPLS IP and MPLS LDP. Meanwhile, enable MPLS IP and MPLS LDP on the interface.

```
PE2(config)#mpls ip
```

```
PE2(config)#mpls ldp
PE2(config-ldp)#router-id 75.75.75.75
PE2(config-ldp)#address-family ipv4
PE2(config-ldp-af4)#transport-address 75.75.75.75
PE2(config-ldp-af4)#exit
PE2(config-ldp)#exit
PE2(config)#interface gigabitethernet0
PE2(config-if-gigabitethernet0)#mpls ip
PE2(config-if-gigabitethernet0)#mpls ldp
PE2(config-if-gigabitethernet0)#exit
```

Note:

- router-id and transport-address can be configured manually and also can be generated automatically. Usually, they are configured the same. If not configuring router-id and transport-address manually, the device will select automatically. From the up interfaces, first select the Loopback interface with the maximum IP address. If the device does not configure the Loopback interface address, select the common interface with the maximum IP address.

#After the configuration is complete, view the LDP session information on the device.

Take the PE1 as an example:

```
PE1#show mpls ldp session
Peer IP Address   Peer Type    My Role  State        DS Cap   DeadTime
11.11.11.11       Multicast    Active   OPERATIONAL  Disabled 00:02:20
Statistics for ldp sessions:
    Multicast sessions: 1
    Targeted sessions: 0
```

You can see that PE1 and P set up the LDP session successfully.

#View the route label information on the device.

Take the PE1 as an example:

```
PE1#show ip route 11.11.11.11 detail
Codes: C - Connected, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
    U - Per-user Static route
    O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external



O   11.11.11.11/32 [110/2] via 93.1.1.1, label 3, 00:05:12, gigabitethernet0
                           93.1.1.1 [0], gigabitethernet0
```

```
PE1#show ip route 75.75.75.75 detail
Codes: C - Connected, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external



O   75.75.75.75/32 [110/2] via 93.1.1.1, label 24016, 00:06:03, gigabitethernet0
                           93.1.1.1 [0], gigabitethernet0
```

You can see that the loopback port route from PE1 to P and PE2 has the label information.

Note:

For the checking method of P and PE2, refer to PE1.

Step 3: Configure the VPN instance and advertise the CE route to PE via OSPF.

#On PE1, configure the VPN instance and the OSPF in VPN1 and VPN2.

```
PE1(config)#ip vrf 1
PE1(config-vrf)#rd 100:1
PE1(config-vrf)#route-target export 100:1
PE1(config-vrf)#route-target import 100:1
PE1(config-vrf)#exit
PE1(config)#ip vrf 2
PE1(config-vrf)#rd 200:1
PE1(config-vrf)#route-target export 200:1
PE1(config-vrf)#route-target import 200:1
PE1(config-vrf)#exit
PE1(config)#interface gigabitethernet2
PE1(config-if-gigabitethernet2)#ip vrf forwarding 1
PE1(config-if-gigabitethernet2)#ip address 95.1.1.1 255.255.0.0
PE1(config-if-gigabitethernet2)#exit
PE1(config)#interface gigabitethernet1
PE1(config-if-gigabitethernet1)#ip vrf forwarding 2
PE1(config-if-gigabitethernet1)#ip address 94.1.1.1 255.255.0.0
PE1(config-if-gigabitethernet1)#exit
PE1(config)#router ospf 200 vrf 1
PE1(config-ospf)#network 95.1.0.0 0.0.255.255 area 0
PE1(config-ospf)#exit
```

```
PE1(config)#router ospf 300 vrf 2
PE1(config-ospf)#network 94.1.0.0 0.0.255.255 area 0
PE1(config-ospf)#exit
```

#Configure OSPF on CE1.

```
CE1#configure terminal
CE1(config)#router ospf 100
CE1(config-ospf)#network 5.5.5.5 0.0.0.0 area 0
CE1(config-ospf)#network 95.1.0.0 0.0.255.255 area 0
CE1(config-ospf)#exit
```

#Configure OSPF on CE2.

```
CE2#configure terminal
CE2(config)#router ospf 100
CE2(config-ospf)#network 2.2.2.2 0.0.0.0 area 0
CE2(config-ospf)#network 94.1.0.0 0.0.255.255 area 0
CE2(config-ospf)#exit
```

#Configure the VPN instance on PE2 and configure the OSPF in VPN1 and VPN2.

```
PE2(config)#ip vrf 1
PE2(config-vrf)#rd 100:1
PE2(config-vrf)#route-target export 100:1
PE2(config-vrf)#route-target import 100:1
PE2(config-vrf)#exit
PE2(config)#ip vrf 2
PE2(config-vrf)#rd 200:1
PE2(config-vrf)#route-target export 200:1
PE2(config-vrf)#route-target import 200:1
PE2(config-vrf)#exit
PE2(config)#interface gigabitethernet1
PE2(config-if-gigabitethernet1)#ip vrf forwarding 1
PE2(config-if-gigabitethernet1)#ip address 90.1.1.1 255.255.0.0
PE2(config-if-gigabitethernet1)#exit
PE2(config)#interface gigabitethernet2
PE2(config-if-gigabitethernet2)#ip vrf forwarding 2
PE2(config-if-gigabitethernet2)#ip address 91.1.1.1 255.255.0.0
PE2(config-if-gigabitethernet2)#exit
PE2(config)#router ospf 200 vrf 1
PE2(config-ospf)#network 90.1.0.0 0.0.255.255 area 0
PE2(config-ospf)#exit
```

```
PE2(config)#router ospf 300 vrf 2
PE2(config-ospf)#network 91.1.0.0 0.0.255.255 area 0
PE2(config-ospf)#exit
```

#Configure OSPF on CE3.

```
CE3#configure terminal
CE3(config)#router ospf 100
CE3(config-ospf)#network 8.8.8.8 0.0.0.0 area 0
CE3(config-ospf)#network 90.1.0.0 0.0.255.255 area 0
CE3(config-ospf)#exit
```

Configure OSPF on CE4.

```
CE4#configure terminal
CE4(config)#router ospf 100
CE4(config-ospf)#network 3.3.3.3 0.0.0.0 area 0
CE4(config-ospf)#network 91.1.0.0 0.0.255.255 area 0
CE4(config-ospf)#exit
```

#View the VPN route table on PE.

Take PE1 as an example.

```
PE1#show ip route vrf 1
Codes: C - Connected, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external



C   95.1.0.0/16 is directly connected, 00:11:45, gigabitethernet2
O   5.5.5.5/32 [110/2] via 95.1.1.2, 00:11:11, gigabitethernet2

PE1#show ip route vrf 2
Codes: C - Connected, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external



C   94.1.0.0/16 is directly connected, 00:23:25, gigabitethernet1
O   2.2.2.2/32 [110/2] via 94.1.1.2, 00:22:53, gigabitethernet1
```

You can see that there is the route information of CE1 and CE2 in the VPN1 and VPN2 route tables of PE1.

Note:

- For the checking method of PE2, refer to PE1.

Step 5: Configure MP-IBGP, and use the loopback interface as the peer address; re-distribute the route with the IGP protocol in the VPN instance.

#On PE1, configure MP-IBGP, enable the VPNv4 address family, and re-distribute the route with the IGP protocol in the VPN instance.

```
PE1(config)#router bgp 100
PE1(config-bgp)#neighbor 75.75.75.75 remote-as 100
PE1(config-bgp)#neighbor 75.75.75.75 update-source loopback0
PE1(config-bgp)#address-family vpnv4
PE1(config-bgp-af)#neighbor 75.75.75.75 activate
PE1(config-bgp-af)#neighbor 75.75.75.75 send-community extended
PE1(config-bgp-af)#exit-address-family
PE1(config-bgp)#address-family ipv4 vrf 1
PE1(config-bgp-af)#redistribute ospf 200
PE1(config-bgp-af)#exit-address-family
PE1(config-bgp)#address-family ipv4 vrf 2
PE1(config-bgp-af)#redistribute ospf 300
PE1(config-bgp-af)#exit-address-family
PE1(config-bgp)#exit
PE1(config)#router ospf 200 vrf 1
PE1(config-ospf)#redistribute bgp 100
PE1(config-ospf)#exit
PE1(config)#router ospf 300 vrf 2
PE1(config-ospf)#redistribute bgp 100
PE1(config-ospf)#exit
```

#On PE2, configure MP-IBGP, enable the VPNv4 address family, and re-distribute the route with the IGP protocol in the VPN instance.

```
PE2(config)#router bgp 100
PE2(config-bgp)#neighbor 90.90.90.90 remote-as 100
PE2(config-bgp)#neighbor 90.90.90.90 update-source loopback0
PE2(config-bgp)#address-family vpnv4
PE2(config-bgp-af)#neighbor 90.90.90.90 activate
PE2(config-bgp-af)#neighbor 90.90.90.90 send-community extended
PE2(config-bgp-af)#exit-address-family
PE2(config-bgp)#address-family ipv4 vrf 1
```

```
PE2(config-bgp-af)#redistribute ospf 200
PE2(config-bgp-af)#exit-address-family
PE2(config-bgp)#address-family ipv4 vrf 2
PE2(config-bgp-af)#redistribute ospf 300
PE2(config-bgp-af)#exit-address-family
PE2(config-bgp)#exit
PE2(config)#router ospf 200 vrf 1
PE2(config-ospf)#redistribute bgp 100
PE2(config-ospf)#exit
PE2(config)#router ospf 300 vrf 2
PE2(config-ospf)#redistribute bgp 100
PE2(config-ospf)#exit
```

Caution:

- In the actual application, if one site has two or more PE devices, it is suggested not to re-distribute the route between different route protocols directly. If it is necessary to configure, you need to configure the route policy to prevent the route loop.

Step 6: Check the result.

#After the configuration is complete, view the BGP neighbor information on the PE.

Take PE1 as an example:

```
PE1#show ip bgp vpnv4 all summary
BGP router identifier 90.90.90.90, local AS number 100
BGP table version is 6
1 BGP AS-PATH entries
0 BGP community entries

Neighbor        V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
75.75.75.75     4   100      40      41        5    0    0 00:32:01        4

Total number of neighbors 1
```

The content of the State/PfxRcd list is displayed as number (the number of the route prefixes received from the neighbor), and you can see that PE1 and PE2 set up the BGP neighbor successfully.

#View the BGP VPNv4 route table and VPN route table on the PE.

Take PE1 as an example:

```
PE1#show ip bgp vpnv4 vrf 1
BGP table version is 43, local router ID is 90.90.90.90
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              S Stale
```

```
Origin codes: i - IGP, e - EGP, ? - incomplete
    Network          Next Hop         Metric LocPrf Weight Path
Route Distinguisher: 100:1 (Default for VRF 1)
[0]*> 5.5.5.5/32        95.1.1.2              2        32768 ?
[B]*>i8.8.8.8/32        75.75.75.75           2    100      0 ?
[B]*>i90.1.0.0/16       75.75.75.75           1    100      0 ?
[0]*> 95.1.0.0/16       0.0.0.0               1        32768 ?

PE1#show ip bgp vpnv4 vrf 2
BGP table version is 43, local router ID is 90.90.90.90
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
    Network          Next Hop         Metric LocPrf Weight Path
Route Distinguisher: 200:1 (Default for VRF 2)
[0]*> 2.2.2.2/32        94.1.1.2              2        32768 ?
[B]*>i3.3.3.3/32        75.75.75.75           2    100      0 ?
[B]*>i91.1.0.0/16       75.75.75.75           1    100      0 ?
[0]*> 94.1.0.0/16       0.0.0.0               1        32768 ?

PE1#show ip route vrf 1
Codes: C - Connected, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external



B   90.1.0.0/16 [200/1] via 75.75.75.75, 00:01:06, gigabitethernet0
C   95.1.0.0/16 is directly connected, 00:23:25, gigabitethernet2
O   5.5.5.5/32 [110/2] via 95.1.1.2, 00:22:51, gigabitethernet2
B   8.8.8.8/32 [200/2] via 75.75.75.75, 00:01:06, gigabitethernet0

PE1#show ip route vrf 2
Codes: C - Connected, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external
```

```
B   91.1.0.0/16 [200/1] via 75.75.75.75, 00:01:15, gigabitethernet0
C   94.1.0.0/16 is directly connected, 00:23:25, gigabitethernet1
O   2.2.2.2/32 [110/2] via 94.1.1.2, 00:22:53, gigabitethernet1
B   3.3.3.3/32 [200/2] via 75.75.75.75, 00:01:15, gigabitethernet0
```

You can see that there is the route information to the peer CE3 and CE4 in the BGP VPNv4 route table, VPN1 and VPN2 route table of PE1.

#View the MPLS forwarding table on the PE.

Take PE1 as an example:

```
PE1#show mpls forwarding-table
Pro: L - LDP, O - OSPF, B - MP-BGP, R - RSVP, M - Mapped-Route, S - Static Label,ML - mLDP (ML FEC: Root address/OT/OV), RM - RSVP P2MP (RM FEC: P2MP ID/TID)

Pro Ident      FEC          Inlabel Outlabel Outgoing          Next hop
B   1          0.0.0.0/0    24240   /        /                /
B   2          0.0.0.0/0    24241   /        /                /
```

You can see that there is the route label information of VPN1 and VPN2 in the MPLS forwarding table of PE1.

Note:

- For the checking method of PE2, refer to PE1.

#Ping the loopback port of CE3 at CE1 and view whether the ping can be connected.

```
CE1#ping 8.8.8.8

Press key (ctrl + shift + 6) interrupt it.
Sending 5, 76-byte ICMP Echos to 8.8.8.8 , timeout is 2 seconds:
!!!!!
Success rate is 100% (5/5). Round-trip min/avg/max = 0/0/0 ms.
```

#Ping the loopback port of CE4 at CE1 and view whether the ping can be connected.

```
CE1#ping 3.3.3.3

Press key (ctrl + shift + 6) interrupt it.
Sending 5, 76-byte ICMP Echos to 3.3.3.3 , timeout is 2 seconds:
.....
```

```
Success rate is 0% (0/5).
```

You can see that the devices in one VPN can communicate normally, the devices of different VPNs cannot communicate, and the routes are separated.

3.3.2. Configure M-VRF

Network Requirements

- MCE is the device used by the user for the VPN multi-instance exchange.
- Separate the routes of the user networks VPN1 and VPN2, the sites of the same VPN can communicate with each other, and the sites of different VPNs cannot communicate.
- CE1, CE3 are the sites of VPN1; CE2, Ce4 are the sites of VPN2.
- PE1 and CE1 use EBGP; PE1 and CE2 use RIP.
- MCE and PE2 use OSPF; MCE and CE3, CE4 use the static route.

Network Topology

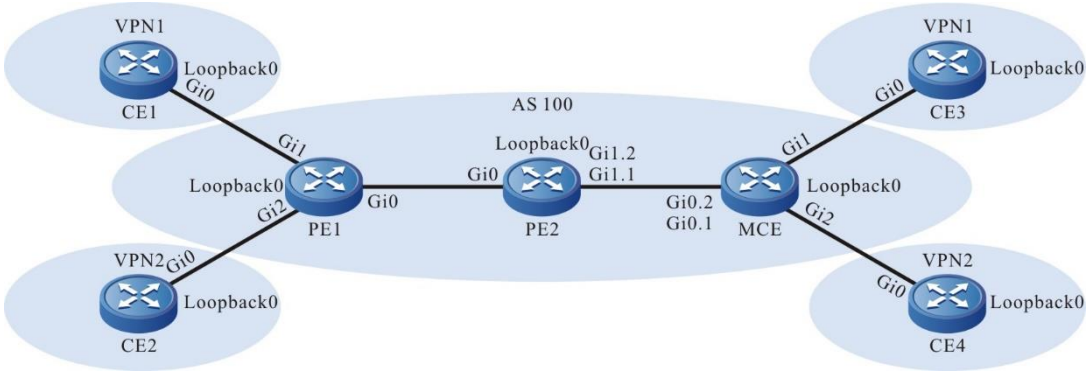

Figure 3-8 Networking of configuring M-VRF

Device	Interface	IP Address	Device	Interface	IP Address
CE1	Gi0	95.1.1.2/16	PE2	Gi1.2	92.1.1.2/16
	Loopback0	5.5.5.5/32		Loopback0	11.11.11.11/32
PE1	Gi0	93.1.1.2/16	MCE	Gi0.1	97.1.1.2/16
	Gi1	95.1.1.1/16		Gi0.2	92.1.1.1/16
	Gi2	94.1.1.1/16		Gi1	90.1.1.1/16
	Loopback0	90.90.90.90/32		Gi2	91.1.1.1/16
CE2	Gi0	94.1.1.2/16	CE3	Gi0	90.1.1.2/16
	Loopback0	2.2.2.2/32		Loopback0	8.8.8.8/32

Device	Interface	IP Address	Device	Interface	IP Address
PE2	Gi0	93.1.1.1/16	CE4	Gi0	91.1.1.2/16
	Gi1.1	97.1.1.1/16		Loopback0	3.3.3.3/32

Configuration Steps

Step 1: Configure the IP address of the interface (omitted).

Step 2: Configure the global OSPF and advertise the global route.

#Configure the global OSPF on PE1.

```
PE1#configure terminal
PE1(config)#router ospf 100
PE1(config-ospf)#network 90.90.90.90 0.0.0.0 area 0
PE1(config-ospf)#network 93.1.0.0 0.0.255.255 area 0
PE1(config-ospf)#exit
```

#Configure the global OSPF on PE2.

```
PE2#configure terminal
PE2(config)#router ospf 100
PE2(config-ospf)#network 11.11.11.11 0.0.0.0 area 0
PE2(config-ospf)#network 93.1.0.0 0.0.255.255 area 0
PE2(config-ospf)#exit
```

#After the configuration is complete, view the global route table on the device.

Take PE1 as an example:

```
PE1#show ip route
Codes: C - Connected, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external



O   11.11.11.11/32 [110/2] via 93.1.1.1, 03:19:45, gigabitethernet0
C   93.1.0.0/16 is directly connected, 03:20:31, gigabitethernet0
C   90.90.90.90/32 is directly connected, 03:22:09, loopback0
```

You can see that there is the route information of the PE2 loopback port in the global route table of PE1.

Note:

- For the checking method of PE2, refer to PE1.

Step 3: Enable MPLS IP and MPLS LDP.

#On PE1, enable the global MPLS IP and MPLS LDP. Meanwhile, enable MPLS IP and MPLS LDP on the interface.

```
PE1(config)#mpls ip
PE1(config)#mpls ldp
PE1(config-ldp)#router-id 90.90.90.90
PE1(config-ldp)#address-family ipv4
PE1(config-ldp-af4)#transport-address 90.90.90.90
PE1(config-ldp-af4)#exit
PE1(config-ldp)#exit
PE1(config)#interface gigabitethernet0
PE1(config-if-gigabitethernet0)#mpls ip
PE1(config-if-gigabitethernet0)#mpls ldp
PE1(config-if-gigabitethernet0)#exit
```

#On PE2, enable the global MPLS IP and MPLS LDP. Meanwhile, enable MPLS IP and MPLS LDP on the interface.

```
PE2(config)#mpls ip
PE2(config)#mpls ldp
PE2(config-ldp)#router-id 11.11.11.11
PE2(config-ldp)#address-family ipv4
PE2(config-ldp-af4)#transport-address 11.11.11.11
PE2(config-ldp-af4)#exit
PE2(config-ldp)#exit
PE2(config)#interface gigabitethernet0
PE2(config-if-gigabitethernet0)#mpls ip
PE2(config-if-gigabitethernet0)#mpls ldp
PE2(config-if-gigabitethernet0)#exit
```

#After the configuration is complete, view the LDP session information on the device.

Take PE1 as an example:

```
PE1#show mpls ldp session
Peer IP Address   Peer Type    My Role  State        DS Cap   DeadTime
11.11.11.11       Multicast    Active   OPERATIONAL  Disabled 00:02:19
Statistics for ldp sessions:
    Multicast sessions: 1
    Targeted sessions: 0
```

You can see that PE1 and PE2 set up the LDP session successfully.

#View the route label information on the device.

Take PE1 as an example:

```
PE1#show ip route 11.11.11.11 detail
Codes: C - Connected, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
    U - Per-user Static route
    O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external



O   11.11.11.11/32 [110/2] via 93.1.1.1, label 3, 03:19:45, gigabitethernet0
                           93.1.1.1 [0], gigabitethernet0
```

You can see that the loopback port route from PE1 to PE2 has the label information.

Note:

- For the checking method of PE2, refer to PE1.

Step 4: Configure the VPN instance, and advertise the CE1, CE2 route to PE1 via OSPF.

#On PE1, configure the VPN instance, configure EBGP in VPN1, and configure RIP in VPN2.

```
PE1(config)#ip vrf 1
PE1(config-vrf)#rd 100:1
PE1(config-vrf)#route-target export 100:1
PE1(config-vrf)#route-target import 100:1
PE1(config-vrf)#exit
PE1(config)#ip vrf 2
PE1(config-vrf)#rd 200:1
PE1(config-vrf)#route-target export 200:1
PE1(config-vrf)#route-target import 200:1
PE1(config-vrf)#exit
PE1(config)#interface gigabitethernet1
PE1(config-if-gigabitethernet1)#ip vrf forwarding 1
PE1(config-if-gigabitethernet1)#ip address 95.1.1.1 255.255.0.0
PE1(config-if-gigabitethernet1)#exit
PE1(config)#interface gigabitethernet2
PE1(config-if-gigabitethernet2)#ip vrf forwarding 2
PE1(config-if-gigabitethernet2)#ip address 94.1.1.1 255.255.0.0
PE1(config-if-gigabitethernet2)#exit
PE1(config)#router bgp 100
```

```
PE1(config-bgp)#address-family ipv4 vrf 1
PE1(config-bgp-af)#neighbor 95.1.1.2 remote-as 200
PE1(config-bgp-af)#exit-address-family
PE1(config-bgp)#exit
PE1(config)#router rip
PE1(config-rip)#address-family ipv4 vrf 2
PE1(config-rip-af)#version 2
PE1(config-rip-af)#network 94.1.0.0
PE1(config-rip-af)#exit-address-family
PE1(config-rip)#exit
```

#On CE1, configure EBGP, and advertise the CE route to PE.

```
CE1#configure terminal
CE1(config)#router bgp 200
CE1(config-bgp)#neighbor 95.1.1.1 remote-as 100
CE1(config-bgp)#network 5.5.5.5 255.255.255.255
CE1(config-bgp)#network 95.1.0.0 255.255.0.0
CE1(config-bgp)#exit
```

#On CE2, configure RIP, and advertise the CE route to PE.

```
CE2#configure terminal
CE2(config)#router rip
CE2(config-rip)#version 2
CE2(config-rip)#network 2.2.2.2
CE2(config-rip)#network 94.1.0.0
CE2(config-rip)#exit
```

#After the configuration is complete, view the route tables of VPN1 and VPN2 on PE1.

```
PE1#show ip route vrf 1
Codes: C - Connected, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external



C   95.1.0.0/16 is directly connected, 03:48:37, gigabitethernet1
B   5.5.5.5/32 [20/0] via 95.1.1.2, 03:22:26, gigabitethernet1

PE1#show ip route vrf 2
Codes: C - Connected, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
```

U - Per-user Static route

O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external

C 94.1.0.0/16 is directly connected, 03:58:11, gigabitethernet2

R 2.2.2.2/32 [120/1] via 94.1.1.2, 03:46:36, gigabitethernet2

You can see that there is the route information of CE1 and CE2 in the VPN1 and VPN2 route tables of PE1.

Step 5: On PE2 and MCE, configure the VPN instance; on CE3, CE4, configure the default route to MCE.

#On PE2, configure the VPN instance, and configure OSPF in VPN1 and VPN2.

```
PE2(config)#ip vrf 1
PE2(config-vrf)#rd 100:1
PE2(config-vrf)#route-target export 100:1
PE2(config-vrf)#route-target import 100:1
PE2(config-vrf)#exit
PE2(config)#ip vrf 2
PE2(config-vrf)#rd 200:1
PE2(config-vrf)#route-target export 200:1
PE2(config-vrf)#route-target import 200:1
PE2(config-vrf)#exit
PE2(config)#interface gigabitethernet1.2
PE2(config-if-gigabitethernet1.2)#ip vrf forwarding 1
PE2(config-if-gigabitethernet1.2)#encapsulation dot1q 2
PE2(config-if-gigabitethernet1.2)#ip address 92.1.1.1 255.255.0.0
PE2(config-if-gigabitethernet1.2)#exit
PE2(config)#interface gigabitethernet1.1
PE2(config-if-gigabitethernet1.1)#ip vrf forwarding 2
PE2(config-if-gigabitethernet1.1)#encapsulation dot1q 1
PE2(config-if-gigabitethernet1.1)#ip address 97.1.1.2 255.255.0.0
PE2(config-if-gigabitethernet1.1)#exit
PE2(config)#router ospf 200 vrf 1
PE2(config-ospf)#network 92.1.0.0 0.0.255.255 area 0
PE2(config-ospf)#exit
PE2(config)#router ospf 300 vrf 2
PE2(config-ospf)#network 97.1.0.0 0.0.255.255 area 0
```

```
PE2(config-ospf)#exit
```

#On MCE, configure the VPN instance; configure OSPF in VPN1 and VPN2, configure the static route to the CE loopback port, and re-distribute to OSPF.

```
MCE#configure terminal
MCE(config)#ip vrf 1
MCE(config-vrf)#rd 100:1
MCE(config-vrf)#exit
MCE(config)#ip vrf 2
MCE(config-vrf)#rd 200:1
MCE(config-vrf)#exit
MCE(config)#interface gigabitethernet0.2
MCE(config-if-gigabitethernet0.2)#ip vrf forwarding 1
MCE(config-if-gigabitethernet0.2)#encapsulation dot1q 2
MCE(config-if-gigabitethernet0.2)#ip address 92.1.1.2 255.255.0.0
MCE(config-if-gigabitethernet0.2)#exit
MCE(config)#interface gigabitethernet0.1
MCE(config-if-gigabitethernet0.1)#ip vrf forwarding 2
MCE(config-if-gigabitethernet0.1)# encapsulation dot1q 1
MCE(config-if-gigabitethernet0.1)#ip address 97.1.1.1 255.255.0.0
MCE(config-if-gigabitethernet0.1)#exit
MCE(config)#interface gigabitethernet1
MCE(config-if-gigabitethernet1)#ip vrf forwarding 1
MCE(config-if-gigabitethernet1)#ip address 90.1.1.1 255.255.0.0
MCE(config-if-gigabitethernet1)#exit
MCE(config)#interface gigabitethernet2
MCE(config-if-gigabitethernet2)#ip vrf forwarding 2
MCE(config-if-gigabitethernet2)#ip address 91.1.1.1 255.255.0.0
MCE(config-if-gigabitethernet2)#exit
MCE(config)#ip route vrf 1 8.8.8.8 255.255.255.255 90.1.1.2
MCE(config)#ip route vrf 2 3.3.3.3 255.255.255.255 91.1.1.2
MCE(config)#router ospf 100 vrf 1
MCE(config-ospf)#network 90.1.0.0 0.0.255.255 area 0
MCE(config-ospf)#network 92.1.0.0 0.0.255.255 area 0
MCE(config-ospf)#redistribute static
MCE(config-ospf)#exit
MCE(config)#router ospf 200 vrf 2
MCE(config-ospf)#network 91.1.0.0 0.0.255.255 area 0
```

```
MCE(config-ospf)#network 97.1.0.0 0.0.255.255 area 0
MCE(config-ospf)#redistribute static
MCE(config-ospf)#exit
```

#On CE3, configure the default route, and the egress interface points to MCE.

```
CE3#configure terminal
CE3(config)#ip route 0.0.0.0 0.0.0.0 90.1.1.1
```

#On CE4, configure the default route, and the egress interface points to MCE.

```
CE4#configure terminal
CE4(config)#ip route 0.0.0.0 0.0.0.0 91.1.1.1
```

Note:

- On CE3 and CE4, you just need to configure one default route and the egress interface points to MCE.

#After the configuration is complete, view the route tables of VPN1 and VPN2 on the MCE.

```
MCE#show ip route vrf 1
Codes: C - Connected, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
    U - Per-user Static route
    O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external



S   8.8.8.8/32 [1/10] via 90.1.1.2, 20:18:48, gigabitethernet1
C   90.1.0.0/16 is directly connected, 22:59:50, gigabitethernet1
C   92.1.0.0/16 is directly connected, 01:02:01, gigabitethernet0.2

MCE#show ip route vrf 2
Codes: C - Connected, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
    U - Per-user Static route
    O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external



C   91.1.0.0/16 is directly connected, 23:00:53, gigabitethernet2
C   97.1.0.0/16 is directly connected, 01:02:04, gigabitethernet0.1
S   3.3.3.3/32 [1/10] via 91.1.1.2, 20:18:33, gigabitethernet2
```

You can see that there is the static route information of CE3 and CE4 on the route tables of VPN1 and VPN2 of the MCE.

#View the route tables of VPN1 and VPN2 on PE2.

```
PE2#show ip route vrf 1
Codes: C - Connected, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external



OE  8.8.8.8/32 [150/20] via 92.1.1.1, 00:27:44, gigabitethernet1.2
O   90.1.0.0/16 [110/2] via 92.1.1.1, 00:27:45, gigabitethernet1.2
C   92.1.0.0/16 is directly connected, 00:27:57, gigabitethernet1.2

PE2#show ip route vrf 2
Codes: C - Connected, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external



O   91.1.0.0/16 [110/2] via 97.1.1.2, 00:27:49, gigabitethernet1.1
C   97.1.0.0/16 is directly connected, 00:28:00, gigabitethernet1.1
OE  3.3.3.3/32 [150/20] via 97.1.1.2, 00:27:48, gigabitethernet1.1
```

You can see that there is the route information of CE3 and CE4 on the route tables of VPN1 and VPN2 of PE2.

Step 6: Configure MP-IBGP, use the loopback interface as the peer address, and re-distribute the route with the IGP protocol in the VPN instance.

#On PE1, configure MP-IBGP, enable VPNv4 address family, and re-distribute the route with the IGP protocol in the VPN instance.

```
PE1(config)#router bgp 100
PE1(config-bgp)#neighbor 11.11.11.11 remote-as 100
PE1(config-bgp)#neighbor 11.11.11.11 update-source loopback0
PE1(config-bgp)#address-family vpnv4
PE1(config-bgp-af)#neighbor 11.11.11.11 activate
PE1(config-bgp-af)#neighbor 11.11.11.11 send-community extended
PE1(config-bgp-af)#exit-address-family
PE1(config-bgp)#address-family ipv4 vrf 2
PE1(config-bgp-af)#redistribute rip
PE1(config-bgp-af)#exit-address-family
```

```
PE1(config-bgp)#exit
PE1(config)#router rip
PE1(config-rip)#address-family ipv4 vrf 2
PE1(config-rip-af)#redistribute bgp 100
PE1(config-rip-af)#exit-address-family
PE1(config-rip)#exit
```

#On PE2, configure MP-IBGP, enable VPNv4 address family, and re-distribute the route with the IGP protocol in the VPN instance.

```
PE2(config)#router bgp 100
PE2(config-bgp)#neighbor 90.90.90.90 remote-as 100
PE2(config-bgp)#neighbor 90.90.90.90 update-source loopback0
PE2(config-bgp)#address-family vpnv4
PE2(config-bgp-af)#neighbor 90.90.90.90 activate
PE2(config-bgp-af)#neighbor 90.90.90.90 send-community extended
PE2(config-bgp-af)#exit-address-family
PE2(config-bgp)#address-family ipv4 vrf 1
PE2(config-bgp-af)#redistribute ospf 200
PE2(config-bgp-af)#exit-address-family
PE2(config-bgp)#address-family ipv4 vrf 2
PE2(config-bgp-af)#redistribute ospf 300
PE2(config-bgp-af)#exit-address-family
PE2(config-bgp)#exit
PE2(config)#router ospf 200 vrf 1
PE2(config-ospf)#redistribute bgp 100
PE2(config-ospf)#exit
PE2(config)#router ospf 300 vrf 2
PE2(config-ospf)#redistribute bgp 100
PE2(config-ospf)#exit
```

Step7: Check the result.

#After the configuration is complete, view the BGP neighbor information on the PE.

Take PE1 as an example:

```
PE1#show ip bgp vpnv4 all summary
BGP router identifier 90.90.90.90, local AS number 100
BGP table version is 4
2 BGP AS-PATH entries
0 BGP community entries
```

```
Neighbor        V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
11.11.11.11     4   100      11      12        4    0    0 00:07:25        6

Total number of neighbors 1
BGP VRF 1 Route Distinguisher:
100:1
BGP table version is 1
2 BGP AS-PATH entries
0 BGP community entries

Neighbor        V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
95.1.1.2        4   200       8       7        1    0    0 00:04:20        2

Total number of neighbors 1
```

The content of the State/PfxRcd list is displayed as number (the number of the route prefixes received from the neighbor), and you can see that PE1 and PE2, CE1 set up the BGP neighbor successfully.

#View the BGP VPNv4 route table and VPN route table on the PE.

Take PE1 as an example:

```
PE1#show ip bgp vpnv4 vrf 1
BGP table version is 33, local router ID is 90.90.90.90
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network          Next Hop            Metric LocPrf Weight Path
Route Distinguisher: 100:1 (Default for VRF 1)
[B]*> 5.5.5.5/32         95.1.1.2                 0             0 200 i
[B]*>i8.8.8.8/32         11.11.11.11             20    100      0 ?
[B]*>i90.1.0.0/16        11.11.11.11              2    100      0 ?
[B]*>i92.1.0.0/16        11.11.11.11              1    100      0 ?
[B]*> 95.1.0.0/16        95.1.1.2                 0             0 200 i

PE1#show ip bgp vpnv4 vrf 2
BGP table version is 33, local router ID is 90.90.90.90
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network          Next Hop            Metric LocPrf Weight Path
```

```
Route Distinguisher: 200:1 (Default for VRF 2)
[R]*> 2.2.2.2/32        94.1.1.2          1        32768 ?
[B]*>i3.3.3.3/32        11.11.11.11       20   100      0 ?
[B]*>i91.1.0.0/16       11.11.11.11       2    100      0 ?
[R]*> 94.1.0.0/16       0.0.0.0             1        32768 ?
[B]*>i97.1.0.0/16       11.11.11.11       1    100      0 ?

PE1#show ip route vrf 1
Codes: C - Connected, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external



B   8.8.8.8/32 [200/20] via 11.11.11.11, 00:07:03, gigabitethernet0
B   90.1.0.0/16 [200/2] via 11.11.11.11, 00:07:03, gigabitethernet0
B   92.1.0.0/16 [200/1] via 11.11.11.11, 00:07:03, gigabitethernet0
C   95.1.0.0/16 is directly connected, 23:13:25, gigabitethernet1
B   5.5.5.5/32 [20/0] via 95.1.1.2, 22:47:14, gigabitethernet1

PE1#show ip route vrf 2
Codes: C - Connected, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external



B   91.1.0.0/16 [200/2] via 11.11.11.11, 00:07:05, gigabitethernet0
C   94.1.0.0/16 is directly connected, 23:10:58, gigabitethernet2
B   97.1.0.0/16 [200/1] via 11.11.11.11, 00:07:05, gigabitethernet0
R   2.2.2.2/32 [120/1] via 94.1.1.2, 22:59:23, s gigabitethernet2
B   3.3.3.3/32 [200/20] via 11.11.11.11, 00:07:05, gigabitethernet0
```

You can see that there is the route information to the peer CE3 and CE4 in the BGP VPNv4 route table, VPN1 and VPN2 route table of PE1.

#View the MPLS forwarding table on the PE.

Take PE1 as an example:

```
PE1#show mpls forwarding-table
```

```
Pro: L - LDP, O - OSPF, B - MP-BGP, R - RSVP, M - Mapped-Route, S - Static
Label,ML - mLDP (ML FEC: Root address/OT/OV), RM - RSVP P2MP (RM FEC: P2MP
ID/TID)


Pro Ident       FEC             Inlabel Outlabel Outgoing       Next hop
B   1           0.0.0.0/0       24120   /       /               /
B   2           0.0.0.0/0       24121   /       /               /
```

You can see that there is the route label information of VPN1 and VPN2 in the MPLS forwarding table of PE1.

Note:

- For the checking method of PE2, refer to PE1.

#Ping the loopback port of CE3 at CE1 and view whether the ping can be connected.

```
CE1#ping 8.8.8.8


Press key (ctrl + shift + 6) interrupt it.
Sending 5, 76-byte ICMP Echos to 8.8.8.8 , timeout is 2 seconds:
!!!!!
Success rate is 100% (5/5). Round-trip min/avg/max = 0/0/0 ms.
```

#Ping the loopback port of CE4 at CE1 and view whether the ping can be connected.

```
CE1#ping 3.3.3.3


Press key (ctrl + shift + 6) interrupt it.
Sending 5, 76-byte ICMP Echos to 3.3.3.3 , timeout is 2 seconds:
.....
Success rate is 0% (0/5).
```

You can see that the devices in one VPN can communicate normally, the devices of different VPNs cannot communicate, and the routes are separated.

3.3.3. Configure Cross-Domain OptionA

- Network Requirements
- The whole MPLS network includes two AS domains. CE1 in AS100 needs to communicate with CE2 in AS200.
- CE1 and CE2 belong to VPN1 at the same time; use OSPF to connect PE.
- Use the VRF-to-VRF mode to exchange the VPN route between ASBR.
- Route-Targets of the VPN instances of different AS do not need to match.
- ASBR and PE use MP-IBGP to exchange the route.

Network Topology

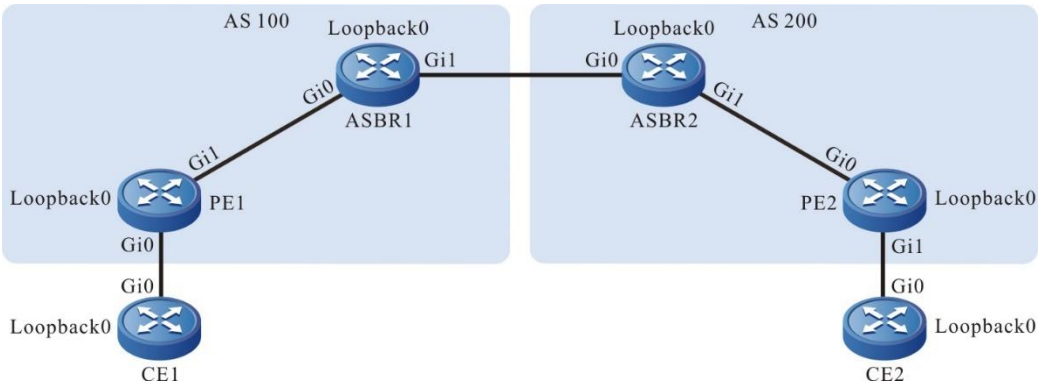

Figure 3-9 Networking of configuring the cross-domain OptionA

Device	Interface	IP Address	Device	Interface	IP Address
CE1	Gi0	10.1.1.1/24	ASBR2	Gi0	10.1.3.2/24
	Loopback0	1.1.1.1/32		Gi1	10.1.4.1/24
PE1	Gi0	10.1.1.2/24		Loopback0	33.33.33.33/32
	Gi1	10.1.2.1/24	PE2	Gi0	10.1.4.2/24
	Loopback0	11.11.11.11/32		Gi1	10.1.5.1/24
ASBR1	Gi0	10.1.2.2/24		Loopback0	44.44.44.44/32
	Gi1	10.1.3.1/24	CE2	Gi0	10.1.5.2/24
	Loopback0	22.22.22.22/32		Loopback0	2.2.2.2/32

Configuration Steps

Step 1: Configure the IP address of the interface (omitted).

Step 2: In one AS domain, configure the global OSPF to advertise the global route.

#Configure the global OSPF on PE1.

```
PE1#configure terminal
PE1(config)#router ospf 100
PE1(config-ospf)#network 10.1.2.0 0.0.0.255 area 0
```

```
PE1(config-ospf)#network 11.11.11.11 0.0.0.0 area 0
PE1(config-ospf)#exit
```

#Configure the global OSPF on ASBR1.

```
ASBR1#configure terminal
ASBR1(config)#router ospf 100
ASBR1(config-ospf)#network 10.1.2.0 0.0.0.255 area 0
ASBR1(config-ospf)#network 22.22.22.22 0.0.0.0 area 0
ASBR1(config-ospf)#exit
```

#Configure the global OSPF on ASBR2.

```
ASBR2#configure terminal
ASBR2(config)#router ospf 100
ASBR2(config-ospf)#network 10.1.4.0 0.0.0.255 area 0
ASBR2(config-ospf)#network 33.33.33.33 0.0.0.0 area 0
ASBR2(config-ospf)#exit
```

#Configure the global OSPF on PE2.

```
PE2#configure terminal
PE2(config)#router ospf 100
PE2(config-ospf)#network 10.1.4.0 0.0.0.255 area 0
PE2(config-ospf)#network 44.44.44.44 0.0.0.0 area 0
PE2(config-ospf)#exit
```

#After the configuration is complete, view the global route table on the device.

Take PE1 as an example:

```
PE1#show ip route
Codes: C - Connected, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
       U - Per-user Static route
         O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external
```

```
C   10.1.2.0/24 is directly connected, 69:53:53, gigabitethernet1
C   127.0.0.0/8 is directly connected, 1183:09:57, lo0
C   11.11.11.11/32 is directly connected, 69:53:37, loopback0
O   22.22.22.22/32 [110/2] via 10.1.2.2, 48:14:20, gigabitethernet1
```

You can see that there is the route information of ASBR1 loopback port in the global route table of PE1.

Note:

- For the checking method of PE2 and ASBR, refer to PE1.

Step 3: Enable MPLS IP and MPLS LDP.

#On PE1, enable the global MPLS IP and MPLS LDP. Meanwhile, enable MPLS IP and MPLS LDP on the interface.

```
PE1(config)#mpls ip
PE1(config)#mpls ldp
PE1(config-ldp)#router-id 11.11.11.11
PE1(config-ldp)#address-family ipv4
PE1(config-ldp-af4)#transport-address 11.11.11.11
PE1(config-ldp-af4)#exit
PE1(config-ldp)#exit
PE1(config)#interface gigabitethernet1
PE1(config-if-gigabitethernet1)#mpls ip
PE1(config-if-gigabitethernet1)#mpls ldp
PE1(config-if-gigabitethernet1)#exit
```

#On ASBR1, enable the global MPLS IP and MPLS LDP. Meanwhile, enable MPLS IP and MPLS LDP on the interface.

```
ASBR1(config)#mpls ip
ASBR1(config)#mpls ldp
ASBR1(config-ldp)#router-id 22.22.22.22
ASBR1(config-ldp)#address-family ipv4
ASBR1(config-ldp-af4)#transport-address 22.22.22.22
ASBR1(config-ldp-af4)#exit
ASBR1(config-ldp)#exit
ASBR1(config)#interface gigabitethernet0
ASBR1(config-if-gigabitethernet0)#mpls ip
ASBR1(config-if-gigabitethernet0)#mpls ldp
ASBR1(config-if-gigabitethernet0)#exit
```

#On ASBR2, enable the global MPLS IP and MPLS LDP. Meanwhile, enable MPLS IP and MPLS LDP on the interface.

```
ASBR2(config)#mpls ip
ASBR2(config)#mpls ldp
ASBR2(config-ldp)#router-id 33.33.33.33
ASBR2(config-ldp)#address-family ipv4
ASBR2(config-ldp-af4)#transport-address 33.33.33.33
ASBR2(config-ldp-af4)#exit
```

```
ASBR2(config-ldp)#exit
ASBR2(config)#interface gigabitethernet1
ASBR2(config-if-gigabitethernet1)#mpls ldp
ASBR2(config-if-gigabitethernet1)#mpls ip
ASBR2(config-if-gigabitethernet1)#exit
```

#On PE2, enable the global MPLS IP and MPLS LDP. Meanwhile, enable MPLS IP and MPLS LDP on the interface.

```
PE2(config)#mpls ip
PE2(config)#mpls ldp
PE2(config-ldp)#router-id 44.44.44.44
PE2(config-ldp)#address-family ipv4
PE2(config-ldp-af4)#transport-address 44.44.44.44
PE2(config-ldp-af4)#exit
PE2(config-ldp)#exit
PE2(config)#interface gigabitethernet0
PE2(config-if-gigabitethernet0)#mpls ip
PE2(config-if-gigabitethernet0)#mpls ldp
PE2(config-if-gigabitethernet0)#exit
```

#After the configuration is complete, view the LDP session information on the device.

Take PE1 as an example:

```
PE1#show mpls ldp session
Peer IP Address    Peer Type    My Role   State        DS Cap   DeadTime
22.22.22.22        Multicast    Active    OPERATIONAL  Disabled 00:02:34
Statistics for ldp sessions:
    Multicast sessions: 1
    Targeted sessions: 0
```

You can see that PE1 and ASBR1 set up the LDP session successfully.

#View the route label on the device.

Take PE1 as an example:

```
PE1#show ip route 22.22.22.22 detail
Codes: C - Connected, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
    U - Per-user Static route
    O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external



O   22.22.22.22/32 [110/2] via 10.1.2.2, label 3, 48:14:20, gigabitethernet1
```

```
10.1.2.2 [0], gigabitethernet1
```

You can see that the loopback port route from PE1 to ASBR1 has the label information.

Note:

- For the checking method of PE2 and ASBR2, refer to PE1.

Step 4: Configure the VPN instance and advertise the CE route to PE via OSPF.

#Configure OSPF on CE1.

```
CE1#configure terminal
CE1(config)#router ospf 100
CE1(config-ospf)#network 1.1.1.1 0.0.0.0 area 0
CE1(config-ospf)#network 10.1.1.0 0.0.0.255 area 0
CE1(config-ospf)#exit
```

#On PE1, configure the VPN instance and OSPF in VPN.

```
PE1(config)#ip vrf 1
PE1(config-vrf)#rd 100:1
PE1(config-vrf)#route-target export 100:1
PE1(config-vrf)#route-target import 100:1
PE1(config-vrf)#exit
PE1(config)#interface gigabitethernet0
PE1(config-if-gigabitethernet0)#ip vrf forwarding 1
PE1(config-if-gigabitethernet0)#ip address 10.1.1.2 255.255.255.0
PE1(config-if-gigabitethernet0)#exit
PE1(config)#router ospf 200 vrf 1
PE1(config-ospf)#network 10.1.1.0 0.0.0.255 area 0
PE1(config-ospf)#exit
```

#On ASBR1, configure the VPN instance.

```
ASBR1(config)#ip vrf 1
ASBR1(config-vrf)#rd 100:1
ASBR1(config-vrf)#route-target export 100:1
ASBR1(config-vrf)#route-target import 100:1
ASBR1(config-vrf)#exit
ASBR1(config)#interface gigabitethernet1
ASBR1(config-if-gigabitethernet1)#ip vrf forwarding 1
ASBR1(config-if-gigabitethernet1)#ip address 10.1.3.1 255.255.255.0
ASBR1(config-if-gigabitethernet1)#exit
```

#On ASBR2, configure the VPN instance.

```
ASBR2(config)#ip vrf 1
```

```
ASBR2(config-vrf)#rd 200:1
ASBR2(config-vrf)#route-target export 200:1
ASBR2(config-vrf)#route-target import 200:1
ASBR2(config-vrf)#exit
ASBR2(config)#interface gigabitethernet0
ASBR2(config-if-gigabitethernet0)#ip vrf forwarding 1
ASBR2(config-if-gigabitethernet0)#ip address 10.1.3.2 255.255.255.0
ASBR2(config-if-gigabitethernet0)#exit
```

#On PE2, configure the VPN instance and OSPF in VPN.

```
PE2(config)#ip vrf 1
PE2(config-vrf)#rd 200:1
PE2(config-vrf)#route-target export 200:1
PE2(config-vrf)#route-target import 200:1
PE2(config-vrf)#exit
PE2(config)#interface gigabitethernet1
PE2(config-if-gigabitethernet1)#ip vrf forwarding 1
PE2(config-if-gigabitethernet1)#ip address 10.1.5.1 255.255.255.0
PE2(config-if-gigabitethernet1)#exit
PE2(config)#router ospf 200 vrf 1
PE2(config-ospf)#network 10.1.5.0 0.0.0.255 area 0
PE2(config-ospf)#exit
```

#Configure OSPF on CE2.

```
CE2#configure terminal
CE2(config)#router ospf 100
CE2(config-ospf)#network 2.2.2.2 0.0.0.0 area 0
CE2(config-ospf)#network 10.1.5.0 0.0.0.255 area 0
CE2(config-ospf)#exit
```

#After the configuration is complete, view the VPN route table on the PE.

Take PE1 as an example:

```
PE1#show ip route vrf 1
Codes: C - Connected, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external



C   10.1.1.0/24 is directly connected, 70:09:30, gigabitethernet0
```

```
O   1.1.1.1/32 [110/2] via 10.1.1.1, 70:07:57, gigabitethernet0
```

You can see that there is the route information to CE1 in the VPN1 route table of PE1.

Note:

- For the checking method of PE2, refer to PE1.

Step 5: Configure MP-IBGP between PE and ASBR, and use the loopback interface as the peer address; configure EBGP between ASBR, and re-distribute the route with the IGP protocol in the VPN instance.

#On PE1, configure MP-IBGP, enable the VPNv4 address family, and re-distribute the route with the IGP protocol in the VPN instance.

```
PE1(config)#router bgp 100
PE1(config-bgp)#neighbor 22.22.22.22 remote-as 100
PE1(config-bgp)#neighbor 22.22.22.22 update-source loopback0
PE1(config-bgp)#address-family vpnv4
PE1(config-bgp-af)#neighbor 22.22.22.22 activate
PE1(config-bgp-af)#neighbor 22.22.22.22 send-community extended
PE1(config-bgp-af)#exit-address-family
PE1(config-bgp)#address-family ipv4 vrf 1
PE1(config-bgp-af)#redistribute ospf 200
PE1(config-bgp-af)#exit-address-family
PE1(config-bgp)#exit
PE1(config)#router ospf 200 vrf 1
PE1(config-ospf)#redistribute bgp 100
PE1(config-ospf)#exit
```

#On ASBR1, configure MP-IBGP with PE1, enable the VPNv4 address family, and configure EBGP with ASBR2 in the VRF address family.

```
ASBR1(config)#router bgp 100
ASBR1(config-bgp)#neighbor 11.11.11.11 remote-as 100
ASBR1(config-bgp)#neighbor 11.11.11.11 update-source loopback0
ASBR1(config-bgp)#address-family vpnv4
ASBR1(config-bgp-af)#neighbor 11.11.11.11 activate
ASBR1(config-bgp-af)#neighbor 11.11.11.11 send-community extended
ASBR1(config-bgp-af)#exit-address-family
ASBR1(config-bgp)#address-family ipv4 vrf 1
ASBR1(config-bgp-af)#redistribute connected
ASBR1(config-bgp-af)#neighbor 10.1.3.2 remote-as 200
ASBR1(config-bgp-af)#exit-address-family
ASBR1(config-bgp)#exit
```

#On ASBR2, configure MP-IBGP with PE2, enable the VPNv4 address family, and configure EBGP with ASBR1 in the VRF address family.

```
ASBR2(config)#router bgp 200
ASBR2(config-bgp)#neighbor 44.44.44.44 remote-as 200
ASBR2(config-bgp)#neighbor 44.44.44.44 update-source loopback0
ASBR2(config-bgp)#address-family vpnv4
ASBR2(config-bgp-af)#neighbor 44.44.44.44 activate
ASBR2(config-bgp-af)#neighbor 44.44.44.44 send-community extended
ASBR2(config-bgp-af)#exit-address-family
ASBR2(config-bgp)#address-family ipv4 vrf 1
ASBR2(config-bgp-af)#redistribute connected
ASBR2(config-bgp-af)#neighbor 10.1.3.1 remote-as 100
ASBR2(config-bgp-af)#exit-address-family
ASBR2(config-bgp)#exit
```

#On PE2, configure MP-IBGP, and enable the VPNv4 address family; re-distribute the route with the IGP protocol in the VPN instance.

```
PE2(config)#router bgp 200
PE2(config-bgp)#neighbor 33.33.33.33 remote-as 200
PE2(config-bgp)#neighbor 33.33.33.33 update-source loopback0
PE2(config-bgp)#address-family vpnv4
PE2(config-bgp-af)#neighbor 33.33.33.33 activate
PE2(config-bgp-af)#neighbor 33.33.33.33 send-community extended
PE2(config-bgp-af)#exit-address-family
PE2(config-bgp)#address-family ipv4 vrf 1
PE2(config-bgp-af)#redistribute ospf 200
PE2(config-bgp-af)#exit-address-family
PE2(config-bgp)#exit
PE2(config)#router ospf 200 vrf 1
PE2(config-ospf)#redistribute bgp 200
PE2(config-ospf)#exit
```

Step 6: Check the result.

#After the configuration is complete, view the BGP neighbor information on the PE and ASBR.

Take PE1, ASBR1 as an example:

```
PE1#show ip bgp vpnv4 all summary
BGP router identifier 11.11.11.11, local AS number 100
BGP table version is 6
1 BGP AS-PATH entries
```

```
0 BGP community entries

Neighbor        V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
22.22.22.22     4   100      44      43        6    0    0 00:34:07        3
Total number of neighbors 1
```

The content of the State/PfxRcd list is displayed as number (the number of the route prefixes received from the neighbor), and you can see that PE1 and ASBR1 set up the BGP neighbor successfully.

```
ASBR1#show ip bgp vpnv4 all summary
BGP router identifier 22.22.22.22, local AS number 100
BGP table version is 5
2 BGP AS-PATH entries
0 BGP community entries

Neighbor        V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
11.11.11.11     4   100      20      21        4    0    0 00:14:56        2

Total number of neighbors 1
BGP VRF 1 Route Distinguisher:
100:1
BGP table version is 1
2 BGP AS-PATH entries
0 BGP community entries

Neighbor        V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
10.1.3.2        4   200       3       3        1    0    0 00:00:03        3

Total number of neighbors 1
```

The content of the State/PfxRcd list is displayed as number (the number of the route prefixes received from the neighbor), and you can see that ASBR1 and PE1, ASBR2 set up the BGP neighbor successfully.

#View the BGP VPNv4 route table on the PE and ASBR.

Take PE1, ASBR1 as an example:

```
PE1#show ip bgp vpnv4 vrf 1
BGP table version is 28, local router ID is 11.11.11.11
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
```

```
    Network          Next Hop        Metric LocPrf Weight Path
Route Distinguisher: 100:1 (Default for VRF 1)
[0]*> 1.1.1.1/32        10.1.1.1             2        32768 ?
[B]*>i2.2.2.2/32         22.22.22.22             0    100      0 200 ?
[0]*> 10.1.1.0/24       0.0.0.0                  1        32768 ?
[B]*>i10.1.3.0/24        22.22.22.22             0    100      0 ?
[B]*>i10.1.5.0/24        22.22.22.22             0    100      0 200 ?

ASBR1#show ip bgp vpnv4 vrf 1
BGP table version is 386, local router ID is 22.22.22.22
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
    Network          Next Hop        Metric LocPrf Weight Path
Route Distinguisher: 100:1 (Default for VRF 1)
[B]*>i1.1.1.1/32        11.11.11.11             2    100      0 ?
[B]*> 2.2.2.2/32         10.1.3.2                 0           0 200 ?
[B]*>i10.1.1.0/24        11.11.11.11              1    100      0 ?
[B]*  10.1.3.0/24        10.1.3.2                 0           0 200 ?
[C]*>                 0.0.0.0                  0        32768 ?
[B]*> 10.1.5.0/24        10.1.3.2                 0           0 200 ?
```

You can see that there is the BGP route information to the peer CE2 in the BGP VPNv4 route table of PE1 and ASBR1.

#View the MPLS forwarding table on the PE and ASBR.

Take PE1, ASBR1 as an example:

```
PE1#show mpls forwarding-table
Pro: L - LDP, O - OSPF, B - MP-BGP, R - RSVP, M - Mapped-Route, S - Static
Label,ML - mLDP (ML FEC: Root address/OT/OV), RM - RSVP P2MP (RM FEC: P2MP
ID/TID)

Pro Ident        FEC              Inlabel Outlabel Outgoing              Next hop
B   1          0.0.0.0/0         24120   /       /                    /

ASBR1#show mpls forwarding-table
Pro: L - LDP, O - OSPF, B - MP-BGP, R - RSVP, M - Mapped-Route, S - Static
Label,ML - mLDP (ML FEC: Root address/OT/OV), RM - RSVP P2MP (RM FEC: P2MP
ID/TID)
```

```
Pro Ident       FEC             Inlabel Outlabel Outgoing          Next hop
B  1            0.0.0.0/0       24480   /       /                  /
```

You can see that there is the route label information of VPN1 in the MPLS forwarding table of PE1 and ASBR1.

Note:

- For the checking method of PE2, ASBR2 , refer to PE1, ASBR1.

#View the route table on the PE and CE.

Take PE1, CE1 as an example:

```
PE1#show ip route vrf 1
Codes: C - Connected, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external



C   10.1.1.0/24 is directly connected, 72:01:01, gigabitethernet0
B   10.1.3.0/24 [200/0] via 22.22.22.22, 01:13:44, gigabitethernet1
B   10.1.5.0/24 [200/0] via 22.22.22.22, 01:12:06, gigabitethernet1
O   1.1.1.1/32 [110/2] via 10.1.1.1, 71:59:28, gigabitethernet0
B   2.2.2.2/32 [200/0] via 22.22.22.22, 01:12:06, gigabitethernet1

CE1#show ip route
Codes: C - Connected, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external



C   10.1.1.0/24 is directly connected, 72:07:55, gigabitethernet0
OE  10.1.3.0/24 [150/1] via 10.1.1.2, 01:14:28, gigabitethernet0
OE  10.1.5.0/24 [150/1] via 10.1.1.2, 01:12:50, gigabitethernet0
C   127.0.0.0/8 is directly connected, 210:21:32, lo0
C   1.1.1.1/32 is directly connected, 72:03:40, loopback0
OE  2.2.2.2/32 [150/1] via 10.1.1.2, 01:12:50, gigabitethernet0
```

You can see that there is the route information to the peer CE2 in the route table of PE1 and CE1.

#On CE1, ping the loopback port of CE2 and view whether the ping can be connected.

```
CE1#ping 2.2.2.2


Press key (ctrl + shift + 6) interrupt it.
Sending 5, 76-byte ICMP Echos to 2.2.2.2 , timeout is 2 seconds:
!!!!!
Success rate is 100% (5/5). Round-trip min/avg/max = 0/0/0 ms.
```

You can see that CE1 can ping CE2.

3.3.4. Configure Cross-Domain OptionB

Network Requirements

- The whole MPLS network includes two AS domains. CE1 in AS100 needs to communicate with CE2 in AS200.
- CE1 and CE2 belong to VPN1 at the same time; use OSPF to exchange the route with PE.
- Use the MP-EBGP to exchange the route between ASBR.
- ASBR and PE use MP-IBGP to exchange the route.

Network Topology

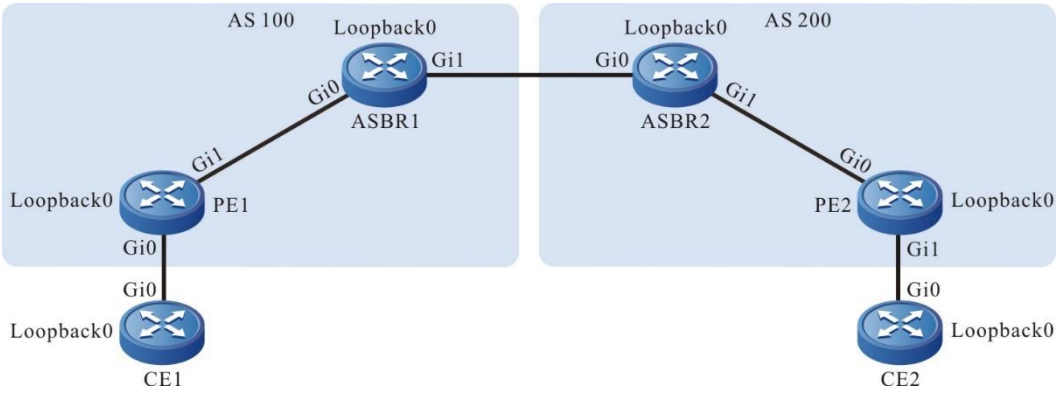

Figure 3-10 Networking of configuring cross-domain OptionB

Device	Interface	IP Address	Device	Interface	IP Address
CE1	Gi0	10.1.1.1/24	ASBR2	Gi0	10.1.3.2/24
	Loopback0	1.1.1.1/32		Gi1	10.1.4.1/24
PE1	Gi0	10.1.1.2/24		Loopback0	33.33.33.33/32
	Gi1	10.1.2.1/24	PE2	Gi0	10.1.4.2/24

Device	Interface	IP Address	Device	Interface	IP Address
	Loopback0	11.11.11.11/32		Gi1	10.1.5.1/24
ASBR1	Gi0	10.1.2.2/24		Loopback0	44.44.44.44/32
	Gi1	10.1.3.1/24	CE2	Gi0	10.1.5.2/24
	Loopback0	22.22.22.22/32		Loopback0	2.2.2.2/32

Configuration Steps

Step 1: Configure the IP address of the interface (omitted).

Step 2: In one AS domain, configure the global OSPF to advertise the global route.

#Configure the global OSPF on PE1.

```
PE1#configure terminal
PE1(config)#router ospf 100
PE1(config-ospf)#network 10.1.2.0 0.0.0.255 area 0
PE1(config-ospf)#network 11.11.11.11 0.0.0.0 area 0
PE1(config-ospf)#exit
```

#Configure the global OSPF on ASBR1.

```
ASBR1#configure terminal
ASBR1(config)#router ospf 100
ASBR1(config-ospf)#network 10.1.2.0 0.0.0.255 area 0
ASBR1(config-ospf)#network 22.22.22.22 0.0.0.0 area 0
ASBR1(config-ospf)#exit
```

#Configure the global OSPF on ASBR2.

```
ASBR2#configure terminal
ASBR2(config)#router ospf 100
ASBR2(config-ospf)#network 10.1.4.0 0.0.0.255 area 0
ASBR2(config-ospf)#network 33.33.33.33 0.0.0.0 area 0
ASBR2(config-ospf)#exit
```

#Configure the global OSPF on PE2.

```
PE2#configure terminal
PE2(config)#router ospf 100
PE2(config-ospf)#network 10.1.4.0 0.0.0.255 area 0
PE2(config-ospf)#network 44.44.44.44 0.0.0.0 area 0
```

```
PE2(config-ospf)#exit
```

#After the configuration is complete, view the global route table on the device.

Take PE1 as an example:

```
PE1#show ip route
Codes: C - Connected, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
    U - Per-user Static route
    O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external
```

```
C   10.1.2.0/24 is directly connected, 04:52:00, gigabitethernet0
C   127.0.0.0/8 is directly connected, 1118:08:05, lo0
C   11.11.11.11/32 is directly connected, 04:51:45, loopback0
O   22.22.22.22/32 [110/2] via 10.1.2.2, 01:45:41, gigabitethernet0
```

You can see that there is the route information of ASBR1 loopback port in the global route table of PE1.

Note:

- For the checking method of PE2 and ASBR, refer to PE1.

Step 3: Enable MPLS IP and MPLS LDP.

#On PE1, enable the global MPLS IP and MPLS LDP. Meanwhile, enable MPLS IP and MPLS LDP on the interface.

```
PE1(config)#mpls ip
PE1(config)#mpls ldp
PE1(config-ldp)#router-id 11.11.11.11
PE1(config-ldp)#address-family ipv4
PE1(config-ldp-af4)#transport-address 11.11.11.11
PE1(config-ldp-af4)#exit
PE1(config-ldp)#exit
PE1(config)#interface gigabitethernet1
PE1(config-if-gigabitethernet1)#mpls ip
PE1(config-if-gigabitethernet1)#mpls ldp
PE1(config-if-gigabitethernet1)#exit
```

#On ASBR1, enable the global MPLS IP and MPLS LDP; meanwhile, enable MPLS IP and MPLS LDP on the interface with PE1. The interfaces between ASBR only need to enable MPLS IP, but do not need to configure MPLS LDP.

```
ASBR1(config)#mpls ip
ASBR1(config)#mpls ldp
```

```
ASBR1(config-ldp)#router-id 22.22.22.22
ASBR1(config-ldp)#address-family ipv4
ASBR1(config-ldp-af4)#transport-address 22.22.22.22
ASBR1(config-ldp-af4)#exit
ASBR1(config-ldp)#exit
ASBR1(config)#interface gigabitethernet0
ASBR1(config-if-gigabitethernet0)#mpls ip
ASBR1(config-if-gigabitethernet0)#mpls ldp
ASBR1(config-if-gigabitethernet0)#exit
ASBR1(config)#interface gigabitethernet1
ASBR1(config-if-gigabitethernet1)#mpls ip
ASBR1(config-if-gigabitethernet1)#exit
```

#On ASBR2, enable the global MPLS IP and MPLS LDP; meanwhile, enable MPLS IP and MPLS LDP on the interface with PE2. The interfaces between ASBR only need to enable MPLS IP, but do not need to configure MPLS LDP.

```
ASBR2(config)#mpls ip
ASBR2(config)#mpls ldp
ASBR2(config-ldp)#router-id 33.33.33.33
ASBR2(config-ldp)#address-family ipv4
ASBR2(config-ldp-af4)#transport-address 33.33.33.33
ASBR2(config-ldp-af4)#exit
ASBR2(config-ldp)#exit
ASBR2(config)#interface gigabitethernet0
ASBR2(config-if-gigabitethernet0)#mpls ip
ASBR2(config-if-gigabitethernet0)#mpls ldp
ASBR2(config-if-gigabitethernet0)#exit
ASBR2(config)#interface gigabitethernet1
ASBR2(config-if-gigabitethernet1)#mpls ip
ASBR2(config-if-gigabitethernet1)#mpls ldp
ASBR2(config-if-gigabitethernet1)#exit
```

#On PE2, enable the global MPLS IP and MPLS LDP. Meanwhile, enable MPLS IP and MPLS LDP on the interface.

```
PE2(config)#mpls ip
PE2(config)#mpls ldp
PE2(config-ldp)#router-id 44.44.44.44
PE2(config-ldp)#address-family ipv4
PE2(config-ldp-af4)#transport-address 44.44.44.44
PE2(config-ldp-af4)#exit
```

```
PE2(config-ldp)#exit
PE2(config)#interface gigabitethernet0
PE2(config-if-gigabitethernet0)#mpls ip
PE2(config-if-gigabitethernet0)#mpls ldp
PE2(config-if-gigabitethernet0)#exit
```

#After the configuration is complete, view the LDP session information on the device.

Take PE1 as an example:

```
PE1#show mpls ldp session
Peer IP Address    Peer Type    My Role   State        DS Cap   DeadTime
22.22.22.22        Multicast    Active    OPERATIONAL  Disabled 00:02:34
Statistics for ldp sessions:
    Multicast sessions: 1
    Targeted sessions: 0
```

You can see that PE1 and ASBR1 set up the LDP session successfully.

#View the route label information on the device.

Take PE1 as an example:

```
PE1#show ip route 22.22.22.22 detail
Codes: C - Connected, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
    U - Per-user Static route
    O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external



O   22.22.22.22/32 [110/2] via 10.1.2.2, label 3, 01:45:41, gigabitethernet0
                           10.1.2.2 [0], gigabitethernet0
```

You can see that the loopback port route from PE1 to ASBR1 has the label information.

Note:

- For the checking method of PE2 and ASBR, refer to PE1.

Step 4: Configure the VPN instance and advertise the CE route to the PE via OSPF.

#On PE1, configure the VPN instance and OSPF in the VPN instance.

```
PE1(config)#ip vrf 1
PE1(config-vrf)#rd 100:1
PE1(config-vrf)#route-target export 100:1
PE1(config-vrf)#route-target import 100:1
PE1(config-vrf)#exit
PE1(config)#interface gigabitethernet0
```

```
PE1(config-if-gigabitethernet0)#ip vrf forwarding 1
PE1(config-if-gigabitethernet0)#ip address 10.1.1.2 255.255.255.0
PE1(config-if-gigabitethernet0)#exit
PE1(config)#router ospf 200 vrf 1
PE1(config-ospf)#network 10.1.1.0 0.0.0.255 area 0
PE1(config-ospf)#exit
```

#Configure OSPF on CE1.

```
CE1#configure terminal
CE1(config)#router ospf 100
CE1(config-ospf)#network 1.1.1.1 0.0.0.0 area 0
CE1(config-ospf)#network 10.1.1.0 0.0.0.255 area 0
CE1(config-ospf)#exit
```

#On PE2, configure the VPN instance and OSPF in the VPN instance.

```
PE2(config)#ip vrf 1
PE2(config-vrf)#rd 100:1
PE2(config-vrf)#route-target export 100:1
PE2(config-vrf)#route-target import 100:1
PE2(config-vrf)#exit
PE2(config)#interface gigabitethernet1
PE2(config-if-gigabitethernet1)#ip vrf forwarding 1
PE2(config-if-gigabitethernet1)#ip address 10.1.5.1 255.255.255.0
PE2(config-if-gigabitethernet1)#exit
PE2(config)#router ospf 200 vrf 1
PE2(config-ospf)#network 10.1.5.0 0.0.0.255 area 0
PE2(config-ospf)#exit
```

#Configure OSPF on CE2.

```
CE2#configure terminal
CE2(config)#router ospf 100
CE2(config-ospf)#network 2.2.2.2 0.0.0.0 area 0
CE2(config-ospf)#network 10.1.5.0 0.0.0.255 area 0
CE2(config-ospf)#exit
```

#After the configuration is complete, view the VPN route table on the PE.

Take PE1 as an example:

```
PE1#show ip route vrf 1
Codes: C - Connected, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external
```

C 10.1.1.0/24 is directly connected, 05:59:50, gigabitethernet0

O 1.1.1.1/32 [110/2] via 10.1.1.1, 05:58:17, gigabitethernet0

You can see that there is the route information to the CE1 in the VPN1 route table of PE1.

Note:

- For the checking method of PE2, refer to PE1.

Step 5: Configure MP-IBGP between PE and ASBR, and use the loopback interface as the peer address; configure EBGP between ASBR, and re-distribute the route with the IGP protocol in the VPN instance.

#On PE1, configure MP-IBGP, enable the VPNv4 address family, and re-distribute the route with the IGP protocol in the VPN instance.

```
PE1(config)#router bgp 100
PE1(config-bgp)#neighbor 22.22.22.22 remote-as 100
PE1(config-bgp)#neighbor 22.22.22.22 update-source loopback0
PE1(config-bgp)#address-family vpnv4
PE1(config-bgp-af)#neighbor 22.22.22.22 activate
PE1(config-bgp-af)#neighbor 22.22.22.22 send-community extended
PE1(config-bgp-af)#exit-address-family
PE1(config-bgp)#address-family ipv4 vrf 1
PE1(config-bgp-af)#redistribute ospf 200
PE1(config-bgp-af)#exit-address-family
PE1(config-bgp)#exit
PE1(config)#router ospf 200 vrf 1
PE1(config-ospf)#redistribute bgp 100
PE1(config-ospf)#exit
```

#On ASBR1, configure MP-IBGP with PE1, configure MP-EBGP between ASBR1 and ASBR2, and enable the VPNv4 address family.

```
ASBR1(config)#router bgp 100
ASBR1(config-bgp)#neighbor 10.1.3.2 remote-as 200
ASBR1(config-bgp)#neighbor 11.11.11.11 remote-as 100
ASBR1(config-bgp)#neighbor 11.11.11.11 update-source loopback0
ASBR1(config-bgp)#address-family vpnv4
ASBR1(config-bgp-af)#neighbor 10.1.3.2 activate
ASBR1(config-bgp-af)#neighbor 10.1.3.2 send-community extended
ASBR1(config-bgp-af)#neighbor 11.11.11.11 activate
ASBR1(config-bgp-af)#neighbor 11.11.11.11 next-hop-self
```

```
ASBR1(config-bgp-af)#neighbor 11.11.11.11 send-community extended
ASBR1(config-bgp-af)#exit-address-family
ASBR1(config-bgp)#exit
```

#On ASBR2, configure MP-IBGP with PE2, configure MP-EBGP between ASBR1 and ASBR2, and enable the VPNv4 address family.

```
ASBR2(config)#router bgp 200
ASBR2(config-bgp)#neighbor 10.1.3.1 remote-as 100
ASBR2(config-bgp)#neighbor 44.44.44.44 remote-as 200
ASBR2(config-bgp)#neighbor 44.44.44.44 update-source loopback0
ASBR2(config-bgp)#address-family vpnv4
ASBR2(config-bgp-af)#neighbor 10.1.3.1 activate
ASBR2(config-bgp-af)#neighbor 10.1.3.1 send-community extended
ASBR2(config-bgp-af)#neighbor 44.44.44.44 activate
ASBR2(config-bgp-af)#neighbor 44.44.44.44 next-hop-self
ASBR2(config-bgp-af)#neighbor 44.44.44.44 send-community extended
ASBR2(config-bgp-af)#exit-address-family
ASBR2(config-bgp)#exit
```

#On PE2, configure MP-IBGP, enable the VPNv4 address family, and re-distribute the route with the IGP protocol in the VPN instance.

```
PE2(config)#router bgp 200
PE2(config-bgp)#neighbor 33.33.33.33 remote-as 200
PE2(config-bgp)#neighbor 33.33.33.33 update-source loopback0
PE2(config-bgp)#address-family vpnv4
PE2(config-bgp-af)#neighbor 33.33.33.33 activate
PE2(config-bgp-af)#neighbor 33.33.33.33 send-community extended
PE2(config-bgp-af)#exit-address-family
PE2(config-bgp)#address-family ipv4 vrf 1
PE2(config-bgp-af)#redistribute ospf 200
PE2(config-bgp-af)#exit-address-family
PE2(config-bgp)#exit
PE2(config)#router ospf 200 vrf 1
PE2(config-ospf)#redistribute bgp 200
PE2(config-ospf)#exit
```

Step 6: Check the result.

#After the configuration is complete, view the BGP neighbor information on the PE and ASBR.

Take PE1, ASBR1 as an example:

```
PE1#show ip bgp vpnv4 all summary
```

```
BGP router identifier 11.11.11.11, local AS number 100
BGP table version is 1
2 BGP AS-PATH entries
0 BGP community entries

Neighbor        V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
22.22.22.22     4   100       4       4        1    0    0 00:02:08        2

Total number of neighbors 1
```

The content of the State/PfxRcd list is displayed as number (the number of the route prefixes received from the neighbor), and you can see that PE1 and ASBR1 set up the BGP neighbor successfully.

```
ASBR1#show ip bgp vpnv4 all summary
BGP router identifier 22.22.22.22, local AS number 100
BGP table version is 1
1 BGP AS-PATH entries
0 BGP community entries

Neighbor        V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
11.11.11.11     4   100       2       2        1    0    0 00:00:14        2
10.1.3.2        4   200       7       8        1    0    0 00:05:28        2

Total number of neighbors 2
```

The content of the State/PfxRcd list is displayed as number (the number of the route prefixes received from the neighbor), and you can see that ASBR1 and PE1, ASBR2 set up the BGP neighbor successfully.

#View the BGP VPNv4 route table on the PE and ASBR.

Take PE1, ASBR1 as an example:

```
PE1#show ip bgp vpnv4 vrf 1
BGP table version is 8, local router ID is 11.11.11.11
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network          Next Hop            Metric LocPrf Weight Path
Route Distinguisher: 100:1 (Default for VRF 1)
[0]*> 1.1.1.1/32         10.1.1.1                 2         32768 ?
[B]*>i2.2.2.2/32         22.22.22.22              0    100      0 200 ?
[0]*> 10.1.1.0/24        0.0.0.0                  1         32768 ?
```

```
[B]*>i10.1.5.0/24        22.22.22.22             0    100      0 200 ?
```

```
ASBR1#show ip bgp vpnv4 all
BGP table version is 364, local router ID is 22.22.22.22
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network          Next Hop          Metric LocPrf Weight Path
Route Distinguisher: 100:1
[B]*>i1.1.1.1/32         11.11.11.11              2    100      0 ?
[B]*> 2.2.2.2/32         10.1.3.2                 0             0 200 ?
[B]*>i10.1.1.0/24        11.11.11.11              1    100      0 ?
[B]*> 10.1.5.0/24        10.1.3.2                 0             0 200 ?
```

You can see that there is the BGP route information to the peer CE2 in the BGP VPNv4 route table of PE1 and ASBR1.

#View the MPLS forwarding table on the PE and ASBR.

Take PE1, ASBR1 as an example:

```
PE1#show mpls forwarding-table
Pro: L - LDP, O - OSPF, B - MP-BGP, R - RSVP, M - Mapped-Route, S - Static
Label,ML - mLDP (ML FEC: Root address/OT/OV), RM - RSVP P2MP (RM FEC: P2MP
ID/TID)
```

```
Pro Ident        FEC              Inlabel Outlabel Outgoing              Next hop
B   1            0.0.0.0/0        24120   /        /                     /
```

```
ASBR1#show mpls forwarding-table
Pro: L - LDP, O - OSPF, B - MP-BGP, R - RSVP, M - Mapped-Route, S - Static
Label,ML - mLDP (ML FEC: Root address/OT/OV), RM - RSVP P2MP (RM FEC: P2MP
ID/TID)
```

```
Pro Ident        FEC              Inlabel Outlabel Outgoing          Next hop
B   global       2.2.2.2/32       24480   24016    gigabitethernet1  10.1.3.2
B   global       10.1.5.0/24      24481   24017    gigabitethernet1  10.1.3.2
B   global       1.1.1.1/32       24482   24120    gigabitethernet0  11.11.11.11
```

You can see that there is the route label information of VPN1 in the MPLS forwarding table of PE1 and ASBR1.

Note:

- For the checking method of PE2, ASBR2 , refer to PE1, ASBR1.

#View the route table on the device.

Take PE1, CE1 as an example:

```
PE1#show ip route vrf 1
Codes: C - Connected, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
    U - Per-user Static route
    O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external



C   10.1.1.0/24 is directly connected, 22:15:35, gigabitethernet0
B   10.1.5.0/24 [200/0] via 22.22.22.22, 00:35:06, gigabitethernet1
O   1.1.1.1/32 [110/2] via 10.1.1.1, 22:14:02, gigabitethernet0
B   2.2.2.2/32 [200/0] via 22.22.22.22, 00:35:06, gigabitethernet1

CE1#show ip route
Codes: C - Connected, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
    U - Per-user Static route
    O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external



C   10.1.1.0/24 is directly connected, 22:22:30, gigabitethernet0
O   10.1.5.0/24 [110/2] via 10.1.1.2, 00:35:47, gigabitethernet0
C   127.0.0.0/8 is directly connected, 160:36:07, lo0
C   1.1.1.1/32 is directly connected, 22:18:15, loopback0
O   2.2.2.2/32 [110/2] via 10.1.1.2, 00:35:47, gigabitethernet0
```

You can see that there is the route information to the peer CE2 in the route table of PE1 and CE1.

#On CE1, ping the loopback port of CE2 and view whether the ping can be connected.

```
CE1#ping 2.2.2.2



Press key (ctrl + shift + 6) interrupt it.
Sending 5, 76-byte ICMP Echos to 2.2.2.2 , timeout is 2 seconds:
!!!!!
```

```
Success rate is 100% (5/5). Round-trip min/avg/max = 0/0/0 ms.
```

You can see that CE1 can ping CE2.

3.3.5. Configure Cross-Domain OptionC

Network Requirements

- The whole MPLS network includes two AS domains. CE1 in AS100 needs to communicate with CE2 in AS200.
- CE1 and CE2 belong to VPN1 at the same time; use OSPF to exchange the route with PE.
- Use EBGP to exchange the route between ASBR.
- ASBR and PE use MP-IBGP to exchange the route.
- Use multi-hop MP-EBGP to exchange the route between PEs.

Network Topology

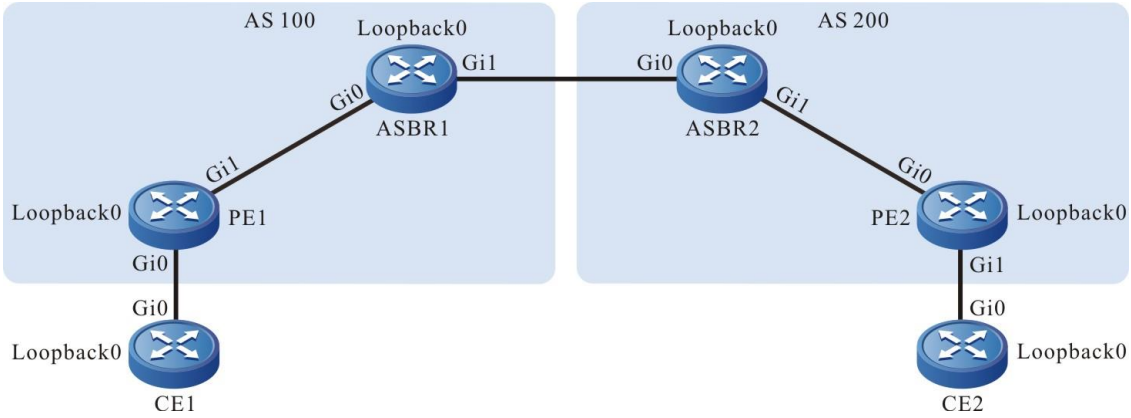

Figure 3-11 Networking of configuring cross-domain OptionC

Device	Interface	IP Address	Device	Interface	IP Address
CE1	Gi0	10.1.1.1/24	ASBR2	Gi0	10.1.3.2/24
	Loopback0	1.1.1.1/32		Gi1	10.1.4.1/24
PE1	Gi0	10.1.1.2/24		Loopback0	33.33.33.33/32
	Gi1	10.1.2.1/24	PE2	Gi0	10.1.4.2/24
	Loopback0	11.11.11.11/32		Gi1	10.1.5.1/24
ASBR1	Gi0	10.1.2.2/24		Loopback0	44.44.44.44/32
	Gi1	10.1.3.1/24	CE2	Gi0	10.1.5.2/24
	Loopback0	22.22.22.22/32и		Loopback0	2.2.2.2/32

Configuration Steps

Step 1: Configure the IP address of the interface (omitted).

Step 2: In one AS domain, configure the global OSPF to advertise the global route.

#Configure the global OSPF on PE1.

```
PE1#configure terminal
PE1(config)#router ospf 100
PE1(config-ospf)#network 10.1.2.0 0.0.0.255 area 0
PE1(config-ospf)#network 11.11.11.11 0.0.0.0 area 0
PE1(config-ospf)#exit
```

#Configure the global OSPF on ASBR1.

```
ASBR1#configure terminal
ASBR1(config)#router ospf 100
ASBR1(config-ospf)#network 10.1.2.0 0.0.0.255 area 0
ASBR1(config-ospf)#network 22.22.22.22 0.0.0.0 area 0
ASBR1(config-ospf)#exit
```

#Configure the global OSPF on ASBR2.

```
ASBR2#configure terminal
ASBR2(config)#router ospf 100
ASBR2(config-ospf)#network 10.1.4.0 0.0.0.255 area 0
ASBR2(config-ospf)#network 33.33.33.33 0.0.0.0 area 0
ASBR2(config-ospf)#exit
```

#Configure the global OSPF on PE2.

```
PE2#configure terminal
PE2(config)#router ospf 100
PE2(config-ospf)#network 10.1.4.0 0.0.0.255 area 0
PE2(config-ospf)#network 44.44.44.44 0.0.0.0 area 0
PE2(config-ospf)#exit
```

#After the configuration is complete, view the global route table on the device.

Take PE1 as an example:

```
PE1#show ip route
Codes: C - Connected, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external
```

```
C   10.1.2.0/24 is directly connected, 04:52:00, gigabitethernet1
L   10.1.2.1/32 is directly connected, 04:52:00, gigabitethernet1
C   127.0.0.0/8 is directly connected, 05:50:00, lo0
L   127.0.0.1/32 is directly connected, 05:50:00, lo0
LC  11.11.11.11/32 is directly connected, 04:51:45, loopback0
O   22.22.22.22/32 [110/2] via 10.1.2.2, 01:45:41, gigabitethernet1
```

You can see that there is the route information of ASBR1 loopback port in the global route table of PE1.

Note:

- For the checking method of PE2 and ASBR, refer to PE1.

Step 3: Enable MPLS IP and MPLS LDP.

#On PE1, enable the global MPLS IP and MPLS LDP. Meanwhile, enable MPLS IP and MPLS LDP on the interface.

```
PE1(config)#mpls ip
PE1(config)#mpls ldp
PE1(config-ldp)#router-id 11.11.11.11
PE1(config-ldp)#transport-address 11.11.11.11
PE1(config-ldp)#exit
PE1(config)#interface gigabitethernet1
PE1(config-if-gigabitethernet1)#mpls ip
PE1(config-if-gigabitethernet1)#mpls ldp
PE1(config-if-gigabitethernet1)#exit
```

#On ASBR1, enable the global MPLS IP and MPLS LDP; meanwhile, enable MPLS IP and MPLS LDP on the interface with PE1. The interfaces between ASBR only need to enable MPLS IP, but do not need to configure MPLS LDP.

```
ASBR1(config)#mpls ip
ASBR1(config)#mpls ldp
ASBR1(config-ldp)#router-id 22.22.22.22
ASBR1(config-ldp)#transport-address 22.22.22.22
ASBR1(config-ldp)#exit
ASBR1(config)#interface gigabitethernet0
ASBR1(config-if-gigabitethernet0)#mpls ip
ASBR1(config-if-gigabitethernet0)#mpls ldp
ASBR1(config-if-gigabitethernet0)#exit
ASBR1(config)#interface gigabitethernet1
ASBR1(config-if-gigabitethernet1)#mpls ip
ASBR1(config-if-gigabitethernet1)#exit
```

#On ASBR2, enable the global MPLS IP and MPLS LDP; meanwhile, enable MPLS IP and MPLS LDP on the interface with PE2. The interfaces between ASBR only need to enable MPLS IP, but do not need to configure MPLS LDP.

```
ASBR2(config)#mpls ip
ASBR2(config)#mpls ldp
ASBR2(config-ldp)#router-id 33.33.33.33
ASBR2(config-ldp)#transport-address 33.33.33.33
ASBR2(config-ldp)#exit
ASBR2(config)#interface gigabitethernet0
ASBR2(config-if-gigabitethernet0)#mpls ip
ASBR2(config-if-gigabitethernet0)#exit
ASBR2(config)#interface gigabitethernet1
ASBR2(config-if-gigabitethernet1)#mpls ip
ASBR2(config-if-gigabitethernet1)#mpls ldp
ASBR2(config-if-gigabitethernet1)#exit
```

#On PE2, enable the global MPLS IP and MPLS LDP. Meanwhile, enable MPLS IP and MPLS LDP on the interface.

```
PE2(config)#mpls ip
PE2(config)#mpls ldp
PE2(config-ldp)#router-id 44.44.44.44
PE2(config-ldp)#transport-address 44.44.44.44
PE2(config-ldp)#exit
PE2(config)#interface gigabitethernet0
PE2(config-if-gigabitethernet0)#mpls ip
PE2(config-if-gigabitethernet0)#mpls ldp
PE2(config-if-gigabitethernet0)#exit
```

#After the configuration is complete, view the LDP session information on the device.

Take PE1 as an example:

```
PE1#show mpls ldp session
Peer IP Address    Peer Type    My Role   State        DeadTime
22.22.22.22        Multicast    Passive   OPERATIONAL  00:02:34
Statistics for ldp sessions:
    Multicast sessions: 1
    Targeted sessions: 0
```

You can see that PE1 and ASBR1 set up the LDP session successfully.

#View the route label information on the device.

Take PE1 as an example:

```
PE1#show ip route 22.22.22.22 detail
```

```
Codes: C - Connected, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external
```

```
O   22.22.22.22/32 [110/2] via 10.1.2.2, label 3, 02:45:41, gigabitethernet1
                           10.1.2.2 [0], gigabitethernet1
```

You can see that the loopback port route from PE1 to ASBR1 has the label information.

Note:

For the checking method of PE2 and ASBR, refer to PE1.

Step 4: Configure the VPN instance and advertise the CE route to the PE via OSPF.

#On PE1, configure the VPN instance and OSPF in the VPN instance.

```
PE1(config)#ip vrf 1
PE1(config-vrf)#rd 100:1
PE1(config-vrf)#route-target export 100:1
PE1(config-vrf)#route-target import 100:1
PE1(config-vrf)#exit
PE1(config)#interface gigabitethernet0
PE1(config-if-gigabitethernet0)#ip vrf forwarding 1
PE1(config-if-gigabitethernet0)#ip address 10.1.1.2 255.255.255.0
PE1(config-if-gigabitethernet0)#exit
PE1(config)#router ospf 200 vrf 1
PE1(config-ospf)#network 10.1.1.0 0.0.0.255 area 0
PE1(config-ospf)#exit
```

#On CE1, configure OSPF.

```
CE1#configure terminal
CE1(config)#router ospf 100
CE1(config-ospf)#network 1.1.1.1 0.0.0.0 area 0
CE1(config-ospf)#network 10.1.1.0 0.0.0.255 area 0
CE1(config-ospf)#exit
```

#On PE2, configure the VPN instance and OSPF in the VPN instance.

```
PE2(config)#ip vrf 1
PE2(config-vrf)#rd 100:1
PE2(config-vrf)#route-target export 100:1
PE2(config-vrf)#route-target import 100:1
```

```
PE2(config-vrf)#exit
PE2(config)#interface gigabitethernet1
PE2(config-if-gigabitethernet1)#ip vrf forwarding 1
PE2(config-if-gigabitethernet1)#ip address 10.1.5.1 255.255.255.0
PE2(config-if-gigabitethernet1)#exit
PE2(config)#router ospf 200 vrf 1
PE2(config-ospf)#network 10.1.5.0 0.0.0.255 area 0
PE2(config-ospf)#exit
```

#On CE1, configure OSPF.

```
CE2#configure terminal
CE2(config)#router ospf 100
CE2(config-ospf)#network 2.2.2.2 0.0.0.0 area 0
CE2(config-ospf)#network 10.1.5.0 0.0.0.255 area 0
CE2(config-ospf)#exit
```

#After configuration, view the VPN route table on PE.

Take PE1 as an example:

```
PE1#show ip route vrf 1
Codes: C - Connected, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external



C   10.1.1.0/24 is directly connected, 05:59:50, gigabitethernet0
L   10.1.1.2/32 is directly connected, 05:59:50, gigabitethernet0
O   1.1.1.1/32 [110/2] via 10.1.1.1, 05:58:17, gigabitethernet0
```

You can see that there is the route to the CE1 in the VPN1 route table of PE1.

Note:

- For the checking method of PE2, refer to PE1.

Step 5: Configure IBGP between PE and ASBR, use the loopback interface as the peer address, advertise the loopback port route, and enable the label advertising capability; configure EBGP between ASBR, and enable the label advertising capability.

#On PE1, configure IBGP with ASBR1, advertise the loopback route, and enable the label advertising capability.

```
PE1(config)#router bgp 100
PE1(config-bgp)#network 11.11.11.11 255.255.255.255
```

```
PE1(config-bgp)#neighbor 22.22.22.22 remote-as 100
PE1(config-bgp)#neighbor 22.22.22.22 update-source loopback0
PE1(config-bgp)#neighbor 22.22.22.22 send-label
PE1(config-bgp)#exit
```

#On ASBR1, configure IBGP with PE1, configure EBGP between ASBR1 and ASBR2, and enable the label advertising capability.

```
ASBR1(config)#router bgp 100
ASBR1(config-bgp)#neighbor 10.1.3.2 remote-as 200
ASBR1(config-bgp)#neighbor 10.1.3.2 send-label
ASBR1(config-bgp)#neighbor 11.11.11.11 remote-as 100
ASBR1(config-bgp)#neighbor 11.11.11.11 update-source loopback0
ASBR1(config-bgp)#neighbor 11.11.11.11 send-label
ASBR1(config-bgp)#neighbor 11.11.11.11 next-hop-self
ASBR1(config-bgp)#exit
```

#On ASBR1, configure IBGP with PE1, configure EBGP between ASBR1 and ASBR2, and enable the label advertising capability.

```
ASBR2(config)#router bgp 200
ASBR2(config-bgp)#neighbor 10.1.3.1 remote-as 100
ASBR2(config-bgp)#neighbor 10.1.3.1 send-label
ASBR2(config-bgp)#neighbor 44.44.44.44 remote-as 200
ASBR2(config-bgp)#neighbor 44.44.44.44 update-source loopback0
ASBR2(config-bgp)#neighbor 44.44.44.44 send-label
ASBR2(config-bgp)#neighbor 44.44.44.44 next-hop-self
ASBR2(config-bgp)#exit
```

#On PE2, configure IBGP with ASBR2, advertise the loopback route, and enable the label advertising capability.

```
PE2(config)#router bgp 200
PE2(config-bgp)#network 44.44.44.44 255.255.255.255
PE2(config-bgp)#neighbor 33.33.33.33 remote-as 200
PE2(config-bgp)#neighbor 33.33.33.33 update-source loopback0
PE2(config-bgp)#neighbor 33.33.33.33 send-label
PE2(config-bgp)#exit
```

#View the route label information on the device.

Take PE1 as an example:

```
PE1#show ip route 44.44.44.44 detail
Codes: C - Connected, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external
```

```
B   44.44.44.44/32 [200/0] via 22.22.22.22, label 24002, 02:39:00, gigabitethernet1
                   10.1.2.2 [2], label 3, gigabitethernet1
```

You can see the route label information of the loopback port from PE1 to PE2. Label 24002 on the gateway is assigned to BGP and label 3 on the next hop is assigned to LDP.

#View MPLS forwarding table entries on the device.

Take ASBR1 as an example:

```
ASBR1#show mpls forwarding-table
Pro: L - LDP, O - OSPF, B - MP-BGP, R - RSVP, M - Mapped-Route, S - Static
Label,ML - mLDP (ML FEC: Root address/OT/OV), RM - RSVP P2MP (RM FEC: P2MP
ID/TID)

Pro Ident       FEC              Inlabel Outlabel Outgoing          Next hop
B   global      44.44.44.44/32   24002   24046    gigabitethernet1  10.1.3.2
B   global      11.11.11.11/32   24100   3        gigabitethernet0  10.1.2.1
```

You can see that the MPLS forwarding table of ASBR1 contains the forwarding table entries to PE1 and PE2 loopback ports.

Note:

- For the checking method of PE2 and ASBR2, refer to PE1 and ASBR1.

Step 6: Configure multi-hop MP-EBGP between PE1 and PE2, use the loopback interface as the peer address, and complete the route redistribution with the IGP protocol under the VPN instance.

#On PE1, configure MP-EBGP and enable the VPNv4 address family; and redistribute the route with the IGP protocol under the VPN instance.

```
PE1(config)#router bgp 100
PE1(config-bgp)#neighbor 44.44.44.44 remote-as 200
PE1(config-bgp)#neighbor 44.44.44.44 update-source loopback0
PE1(config-bgp)#no neighbor 44.44.44.44 activate
PE1(config-bgp)#neighbor 44.44.44.44 ebgp-multihop 255
PE1(config-bgp)#address-family vpnv4
PE1(config-bgp-af)#neighbor 44.44.44.44 activate
PE1(config-bgp-af)#neighbor 44.44.44.44 send-community extended
PE1(config-bgp-af)#exit-address-family
PE1(config-bgp)#address-family ipv4 vrf 1
PE1(config-bgp-af)#redistribute ospf 200
```

```
PE1(config-bgp-af)#exit-address-family
PE1(config-bgp)#exit
PE1(config)#router ospf 200 vrf 1
PE1(config-ospf)#redistribute bgp 100
PE1(config-ospf)#exit
```

#On PE2, configure MP-EBGP and enable the VPNv4 address family; and redistribute the route with the IGP protocol under the VPN instance.

```
PE2(config)#router bgp 200
PE2(config-bgp)#neighbor 11.11.11.11 remote-as 100
PE2(config-bgp)#neighbor 11.11.11.11 update-source loopback0
PE2(config-bgp)#no neighbor 11.11.11.11 activate
PE2(config-bgp)#neighbor 11.11.11.11 ebgp-multihop 255
PE2(config-bgp)#address-family vpnv4
PE2(config-bgp-af)#neighbor 11.11.11.11 activate
PE2(config-bgp-af)#neighbor 11.11.11.11 send-community extended
PE2(config-bgp-af)#exit-address-family
PE2(config-bgp)#address-family ipv4 vrf 1
PE2(config-bgp-af)#redistribute ospf 200
PE2(config-bgp-af)#exit-address-family
PE2(config-bgp)#exit
PE2(config)#router ospf 200 vrf 1
PE2(config-ospf)#redistribute bgp 200
PE2(config-ospf)#exit
```

Step 7: Check the result.

#On PE1, view the BGP VPNv4 route table.

Take PE1 as an example:

```
PE1#show ip bgp vpnv4 vrf 1
BGP table version is 8, local router ID is 11.11.11.11
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network          Next Hop            Metric LocPrf Weight Path
Route Distinguisher: 100:1 (Default for VRF 1)
[0]*> 1.1.1.1/32         10.1.1.1                 2         32768 ?
[B]*>i2.2.2.2/32         44.44.44.44              0    100      0 200 ?
[0]*> 10.1.1.0/24        0.0.0.0                  1         32768 ?
[B]*>i10.1.5.0/24        44.44.44.44              0    100      0 200 ?
```

#On the device, view the route table.

Take PE1 and CE1 as an example:

```
PE1#show ip route vrf 1
Codes: C - Connected, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external



C   10.1.1.0/24 is directly connected, 22:15:35, gigabitethernet0
L   10.1.1.0/24 is directly connected, 22:15:35, gigabitethernet0
B   10.1.5.0/24 [20/0] via 44.44.44.44, 00:35:06, gigabitethernet1
O   1.1.1.1/32 [110/2] via 10.1.1.1, 22:14:02, gigabitethernet0
B   2.2.2.2/32 [20/0] via 44.44.44.44, 00:35:06, gigabitethernet1

CE1#show ip route
Codes: C - Connected, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external



C   10.1.1.0/24 is directly connected, 22:22:30, gigabitethernet0
L   10.1.1.0/24 is directly connected, 22:22:30, gigabitethernet0
O   10.1.5.0/24 [110/2] via 10.1.1.2, 00:35:47, gigabitethernet0
C   127.0.0.0/8 is directly connected, 2d:22:50:57, lo0
L   127.0.0.1/32 is directly connected, 2d:22:50:57, lo0
LC  1.1.1.1/32 is directly connected, 22:18:15, loopback0
O   2.2.2.2/32 [110/2] via 10.1.1.2, 00:35:47, gigabitethernet0
```

You can see that the route information to the peer CE2 exists in the PE1 and CE1 route tables.

View the route label information of the route to the peer CE2 on PE1

```
PE1#show ip route vrf 1 2.2.2.2 detail
Codes: C - Connected, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external
```

```
B   2.2.2.2/32 [20/0] via 44.44.44.44, label 24019, 00:38:06
                10.1.2.2 [2], label 3, extlabel 24002, gigabitethernet1
```

It can be seen that the route has three layers of outgoing labels. The outgoing label 24019 on the gateway is the private label assigned by BGP, which is located at the bottom layer. There are two layers of labels on the next hop. Among them, label 24002 is the global label assigned by BGP, which is located at the middle layer, and label 3 is the global label assigned by LDP, which is located at the top layer.

#Ping the loopback port of CE2 on CE1 and view whether it can be pinged normally.

```
CE1#ping 2.2.2.2


Press key (ctrl + shift + 6) interrupt it.
Sending 5, 76-byte ICMP Echos to 2.2.2.2 , timeout is 2 seconds:
!!!!!
Success rate is 100% (5/5). Round-trip min/avg/max = 0/0/0 ms.
```

You can see that CE1 can ping CE2.

3.3.6. Configure BGP AS Replacing

Network Requirements

- Configure the intra-domain MPLS L3VPN
- CE1 and CE2 are both the devices of VPN1.
- CE1 and CE2 both belong to AS100, use EBGP to advertise the route to PE, and configure AS coverage to ensure that the two CEs can receive the peer route normally.

Network Topology

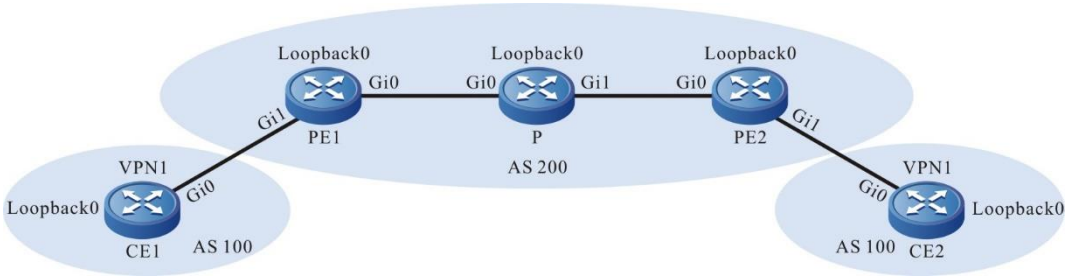

Figure 3-12 Networking of configuring BGP AS replacing

Device	Interface	IP Address	Device	Interface	IP Address
CE1	Gi0	95.1.1.2/16	P	Loopback0	11.11.11.11/32
	Loopback0	5.5.5.5/32	PE2	Gi0	92.1.1.1/16
PE1	Gi0	93.1.1.2/16		Gi1	90.1.1.1/16

Device	Interface	IP Address	Device	Interface	IP Address
	Gi1	95.1.1.1/16		Loopback0	75.75.75.75/32
	Loopback0	90.90.90.90/32	CE2	Gi0	90.1.1.2/16
P	Gi0	93.1.1.1/16		Loopback0	8.8.8.8/32
	Gi1	92.1.1.2/16			

Configuration Steps

Step 1: Configure the IP address of the interface (omitted).

Step 2: Configure the global OSPF and advertise the global route.

#Configure the global OSPF on PE1.

```
PE1#configure terminal
PE1(config)#router ospf 100
PE1(config-ospf)#network 90.90.90.90 0.0.0.0 area 0
PE1(config-ospf)#network 93.1.0.0 0.0.255.255 area 0
PE1(config-ospf)#exit
```

Configure the global OSPF on P.

```
P#configure terminal
P(config)#router ospf 100
P(config-ospf)#network 11.11.11.11 0.0.0.0 area 0
P(config-ospf)#network 92.1.0.0 0.0.255.255 area 0
P(config-ospf)#network 93.1.0.0 0.0.255.255 area 0
P(config-ospf)#exit
```

#Configure the global OSPF on PE2.

```
PE2#configure terminal
PE2(config)#router ospf 100
PE2(config-ospf)#network 75.75.75.75 0.0.0.0 area 0
PE2(config-ospf)#network 92.1.0.0 0.0.255.255 area 0
PE2(config-ospf)#exit
```

#After the configuration is complete, view the global route table on the device.

Take PE1 as an example:

```
PE1#show ip route
Codes: C - connected, S - static, R - RIP,  O - OSPF, OE-OSPF External, M - Management
```

```
D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-ISIS

Gateway of last resort is not set
C   93.1.0.0/16 is directly connected, 00:34:54, gigabitethernet0
O   92.1.0.0/16 [110/2] via 93.1.1.1, 00:08:12, gigabitethernet0
C   90.90.90.90/32 is directly connected, 154:02:28, loopback0
O   11.11.11.11/32 [110/2] via 93.1.1.1, 00:05:03, gigabitethernet0
O   75.75.75.75/32 [110/3] via 93.1.1.1, 00:06:03, gigabitethernet0
```

You can see that there is the route information of P and PE2 loopback ports in the global route table of PE1.

Note:

- For the checking method of PE2, P, refer to PE1.

Step 3: Enable MPLS IP and MPLS LDP.

#On PE1, enable the global MPLS IP and MPLS LDP. Meanwhile, enable MPLS IP and MPLS LDP on the interface.

```
PE1(config)#mpls ip
PE1(config)#mpls ldp
PE1(config-ldp)#router-id 90.90.90.90
PE1(config-ldp)#address-family ipv4
PE1(config-ldp-af4)#transport-address 90.90.90.90
PE1(config-ldp-af4)#exit
PE1(config-ldp)#exit
PE1(config)#interface gigabitethernet0
PE1(config-if-gigabitethernet0)#mpls ip
PE1(config-if-gigabitethernet0)#mpls ldp
PE1(config-if-gigabitethernet0)#exit
```

#On P, enable the global MPLS IP and MPLS LDP. Meanwhile, enable MPLS IP and MPLS LDP on the interface.

```
P(config)#mpls ip
P(config)#mpls ldp
P(config-ldp)#router-id 11.11.11.11
P(config-ldp)#address-family ipv4
P(config-ldp-af4)#transport-address 11.11.11.11
P(config-ldp-af4)#exit
P(config-ldp)#exit
P(config)#interface gigabitethernet0
P(config-if-gigabitethernet0)#mpls ip
```

```
P(config-if-gigabitethernet0)#mpls ldp
P(config-if-gigabitethernet0)#exit
P(config)#interface gigabitethernet1
P(config-if-gigabitethernet1)#mpls ip
P(config-if-gigabitethernet1)#mpls ldp
P(config-if-gigabitethernet1)#exit
```

#On PE2, enable the global MPLS IP and MPLS LDP. Meanwhile, enable MPLS IP and MPLS LDP on the interface.

```
PE2(config)#mpls ip
PE2(config)#mpls ldp
PE2(config-ldp)#router-id 75.75.75.75
PE2(config-ldp)#address-family ipv4
PE2(config-ldp-af4)#transport-address 75.75.75.75
PE2(config-ldp-af4)#exit
PE2(config-ldp)#exit
PE2(config)#interface gigabitethernet0
PE2(config-if-gigabitethernet0)#mpls ip
PE2(config-if-gigabitethernet0)#mpls ldp
PE2(config-if-gigabitethernet0)#exit
```

#After the configuration is complete, view the LDP session information on the device.

Take PE1 as an example:

```
PE1#show mpls ldp session
Peer IP Address    Peer Type    My Role   State        DS Cap    DeadTime
11.11.11.11        Multicast    Active    OPERATIONAL  Disabled  00:02:20
Statistics for ldp sessions:
    Multicast sessions: 1
    Targeted sessions: 0
```

You can see that PE1 and P set up the LDP session successfully.

#View the MPLS forwarding table on the device.

Take PE1 as an example:

```
PE1#show ip route 11.11.11.11 detail
Codes: C - Connected, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
    U - Per-user Static route
    O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external
```

```
O   11.11.11.11/32 [110/2] via 93.1.1.1, label 3, 00:05:03, gigabitethernet0
                           93.1.1.1 [0], gigabitethernet0

PE1#show ip route 75.75.75.75 detail
Codes: C - Connected, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
    U - Per-user Static route
    O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external

O   75.75.75.75/32 [110/2] via 93.1.1.1, label 24016, 00:06:03, gigabitethernet0
                           93.1.1.1 [0], gigabitethernet0
```

You can see that the loopback port route from PE1 to P and PE2 has the label information.

Note:

- For the checking method of PE2, P, refer to PE1.

Step 4: On the PE, configure the VPN instance, and configure BGP between PE and CE.

#On PE1, configure the VPN instance and set up the EBGP neighbor with CE.

```
PE1(config)#ip vrf 1
PE1(config-vrf)#rd 100:1
PE1(config-vrf)#route-target export 100:1
PE1(config-vrf)#route-target import 100:1
PE1(config-vrf)#exit
PE1(config)#interface gigabitethernet1
PE1(config-if-gigabitethernet1)#ip vrf forwarding 1
PE1(config-if-gigabitethernet1)#ip address 95.1.1.1 255.255.0.0
PE1(config-if-gigabitethernet1)#exit
PE1(config)#router bgp 200
PE1(config-bgp)#address-family ipv4 vrf 1
PE1(config-bgp-af)#neighbor 95.1.1.2 remote-as 100
PE1(config-bgp-af)#exit-address-family
PE1(config-bgp)#exit
```

#On CE1, configure the EBGP with PE.

```
CE1#configure terminal
CE1(config)#router bgp 100
CE1(config-bgp)#network 5.5.5.5 255.255.255.255
CE1(config-bgp)#network 95.1.0.0 255.255.0.0
```

```
CE1(config-bgp)#neighbor 95.1.1.1 remote-as 200
CE1(config-bgp)#exit
```

#On PE2, configure the VPN instance and set up the EBGP neighbor with the CE.

```
PE2(config)#ip vrf 1
PE2(config-vrf)#rd 100:1
PE2(config-vrf)#route-target export 100:1
PE2(config-vrf)#route-target import 100:1
PE2(config-vrf)#exit
PE2(config)#interface gigabitethernet1
PE2(config-if-gigabitethernet1)#ip vrf forwarding 1
PE2(config-if-gigabitethernet1)#ip address 90.1.1.1 255.255.0.0
PE2(config-if-gigabitethernet1)#exit
PE2(config)#router bgp 200
PE2(config-bgp)#address-family ipv4 vrf 1
PE2(config-bgp-af)#neighbor 90.1.1.2 remote-as 100
PE2(config-bgp-af)#exit-address-family
PE2(config-bgp)#exit
```

#On CE2, configure EBGP with the PE.

```
CE2#configure terminal
CE2(config)#router bgp 100
CE2(config-bgp)#network 8.8.8.8 255.255.255.255
CE2(config-bgp)#network 90.1.0.0 255.255.0.0
CE2(config-bgp)#neighbor 90.1.1.1 remote-as 200
CE2(config-bgp)#exit
```

#After the configuration is complete, view the EBGP neighbor information on the PE.

Take PE1 as an example:

```
PE1#show ip bgp vpnv4 all summary
BGP router identifier 90.90.90.90, local AS number 200BGP VRF 1 Route Distinguisher:
100:1
BGP table version is 1
1 BGP AS-PATH entries
0 BGP community entries

Neighbor        V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
95.1.1.2        4   100       2       2        1    0    0 00:00:08        2
```

```
Total number of neighbors 1
```

The content of the State/PfxRcd list is displayed as number (the number of the route prefixes received from the neighbor), and you can see that PE1 and CE1 set up the BGP neighbor successfully.

#View the BGP VPNv4 route table and VPN route table on the PE.

```
PE1#show ip bgp vpnv4 vrf 1
BGP table version is 18, local router ID is 90.90.90.90
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network          Next Hop            Metric LocPrf Weight Path
Route Distinguisher: 100:1 (Default for VRF 1)
[B]*> 5.5.5.5/32    95.1.1.2                 0             0 100 i
[B]*> 95.1.0.0/16   95.1.1.2                 0             0 100 i

PE1#show ip route vrf 1
Codes: C - Connected, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external



C   95.1.0.0/16 is directly connected, 15:40:01, gigabitethernet1
B   5.5.5.5/32 [20/0] via 95.1.1.2, 01:13:15, gigabitethernet1
```

You can see that there is the route information to CE1 in the BGP route table and VPN route table of PE1.

Note:

- For the checking method of PE2, refer to PE1.

Step 5: Configure MP-IBGP, and use the loopback interface as the peer address.

#On PE1, configure MP-IBGP and enable the VPNv4 address family.

```
PE1(config)#router bgp 200
PE1(config-bgp)#neighbor 75.75.75.75 remote-as 200
PE1(config-bgp)#neighbor 75.75.75.75 update-source loopback0
PE1(config-bgp)#address-family vpnv4
PE1(config-bgp-af)#neighbor 75.75.75.75 activate
PE1(config-bgp-af)#neighbor 75.75.75.75 send-community extended
PE1(config-bgp-af)#exit-address-family
```

```
PE1(config-bgp)#exit
```

#On PE2, configure MP-IBGP and enable the VPNv4 address family.

```
PE2(config)#router bgp 200
PE2(config-bgp)#neighbor 90.90.90.90 remote-as 200
PE2(config-bgp)#neighbor 90.90.90.90 update-source loopback0
PE2(config-bgp)#address-family vpnv4
PE2(config-bgp-af)#neighbor 90.90.90.90 activate
PE2(config-bgp-af)#neighbor 90.90.90.90 send-community extended
PE2(config-bgp-af)#exit-address-family
PE2(config-bgp)#exit
```

#After the configuration is complete, view the BGP neighbor information.

Take PE1 as an example:

```
PE1#show ip bgp vpnv4 all summary
BGP router identifier 90.90.90.90, local AS number 200
BGP table version is 2
1 BGP AS-PATH entries
0 BGP community entries

Neighbor        V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
75.75.75.75     4   200       3       3        1    0    0 00:00:06        4

Total number of neighbors 1
BGP VRF 1 Route Distinguisher:
100:1
BGP table version is 1
2 BGP AS-PATH entries
0 BGP community entries

Neighbor        V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
95.1.1.2        4   100      18      18        1    0    0 00:14:25        2

Total number of neighbors 1
```

The content of the State/PfxRcd list is displayed as number (the number of the route prefixes received from the neighbor), and you can see that PE1 and PE2, CE1 set up the BGP neighbor successfully.

#View the BGP VPNv4 route table and VPN route table on the PE.

Take PE1 as an example:

```
PE1#show ip bgp vpnv4 vrf 1
BGP table version is 27, local router ID is 90.90.90.90
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network          Next Hop            Metric LocPrf Weight Path
Route Distinguisher: 100:1 (Default for VRF 1)
[B]*> 5.5.5.5/32         95.1.1.2                 0             0 100 i
[B]*>i8.8.8.8/32         75.75.75.75              0    100      0 100 i
[B]*>i90.1.0.0/16        75.75.75.75              0    100      0 100 i
[B]*> 95.1.0.0/16        95.1.1.2                 0             0 100 i

PE1#show ip bgp vpnv4 vrf 1 8.8.8.8
Route Distinguisher: 100:1 (Default for VRF 1), Prefix: 8.8.8.8/32
 Not advertised to any peer
 100
  75.75.75.75 (metric 3) from 75.75.75.75 (75.75.75.75)

   Origin IGP, metric 0, localpref 100, valid, internal, best, vrf ftn installed, vrf
duplicated, vrf external
    Extended Community: RT:100:1
    Last update: 01:38:32 ago

PE1#show ip route vrf 1
Codes: C - Connected, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
     U - Per-user Static route
     O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external



B   90.1.0.0/16 [200/0] via 75.75.75.75, 00:04:05, gigabitethernet0
C   95.1.0.0/16 is directly connected, 18:33:25, gigabitethernet1
B   5.5.5.5/32 [20/0] via 95.1.1.2, 00:09:40, gigabitethernet1
B   8.8.8.8/32 [200/0] via 75.75.75.75, 01:46:03, gigabitethernet0
```

You can see that there is the route information to CE2 in the BGP VPNv4 route table of PE1. AS-PATH is displayed as 100 and there is also the route information to CE2 in the VPN1 route table of PE1.

Note:

- For the checking method of PE2, refer to PE1.

#View the BGP route table on the CE.

Take CE1 as an example:

```
CE1#show ip bgp
BGP table version is 1, local router ID is 5.5.5.5
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network          Next Hop            Metric LocPrf Weight Path
[B]*> 5.5.5.5/32    0.0.0.0                  0         32768 i
[B]*> 95.1.0.0/16   0.0.0.0                  0         32768 i
```

You can see that there is no route information to CE2 in the BGP route table of CE1.

Note:

- CE discovers that the AS PATH attribute of the received peer route contains the same AS number 100, so refuses the BGP route. After configuring the AS cover on the PE, CE can learn the peer route.

Step 6: On the PE, configure the AS coverage.

#In the BGP VRF address family of PE1, configure the AS cover for the EBGP neighbor, so as to cover the same AS number with its own local AS number and transmit to the CE.

```
PE1(config)#router bgp 200
PE1(config-bgp)#address-family ipv4 vrf 1
PE1(config-bgp-af)#neighbor 95.1.1.2 as-override
PE1(config-bgp-af)#exit-address-family
PE1(config-bgp)#exit
```

#In the BGP VRF address family of PE2, configure the AS cover for the EBGP neighbor, so as to cover the same AS number with its own local AS number and transmit to the CE.

```
PE2(config)#router bgp 200
PE2(config-bgp)#address-family ipv4 vrf 1
PE2(config-bgp-af)#neighbor 90.1.1.2 as-override
PE2(config-bgp-af)#exit-address-family
PE2(config-bgp)#exit
```

Step7: Check the result.

#After the configuration is complete, view the BGP VPNv4 route table and VPN route table on the PE.

Take PE1 as an example:

```
PE1#show ip bgp vpnv4 vrf 1
```

```
BGP table version is 27, local router ID is 90.90.90.90
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network          Next Hop            Metric LocPrf Weight Path
Route Distinguisher: 100:1 (Default for VRF 1)
[B]*> 5.5.5.5/32         95.1.1.2                 0             0 100 i
[B]*>i8.8.8.8/32         75.75.75.75              0    100      0 100 i
[B]*>i90.1.0.0/16        75.75.75.75              0    100      0 100 i
[B]*> 95.1.0.0/16        95.1.1.2                 0             0 100 i

PE1#show ip bgp vpnv4 vrf 1 8.8.8.8
Route Distinguisher: 100:1 (Default for VRF 1), Prefix: 8.8.8.8/32
 Not advertised to any peer
 100
  75.75.75.75 (metric 3) from 75.75.75.75 (75.75.75.75)

   Origin IGP, metric 0, localpref 100, valid, internal, best, vrf ftn installed, vrf
duplicated, vrf external
    Extended Community: RT:100:1
    Last update: 01:38:32 ago

PE1#show ip route vrf 1
Codes: C - Connected, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external



B   90.1.0.0/16 [200/0] via 75.75.75.75, 00:04:05, gigabitethernet0
C   95.1.0.0/16 is directly connected, 18:33:25, gigabitethernet1
B   5.5.5.5/32 [20/0] via 95.1.1.2, 00:09:40, gigabitethernet1
B   8.8.8.8/32 [200/0] via 75.75.75.75, 01:46:03, gigabitethernet0
```

You can see that there is the route information to CE2 in the BGP VPNv4 route table of PE1. AS-PATH is displayed as 100 and there is also the route information to CE2 in the VPN1 route table of PE1.

#View the MPLS forwarding table on the PE.

Take PE1 as an example:

```
PE1#show mpls forwarding-table
Pro: L - LDP, O - OSPF, B - MP-BGP, R - RSVP, M - Mapped-Route, S - Static
Label,ML - mLDP (ML FEC: Root address/OT/OV), RM - RSVP P2MP (RM FEC: P2MP
ID/TID)

Pro Ident      FEC          Inlabel Outlabel Outgoing          Next hop
B   1          0.0.0.0/0    25360   /        /                 /
B   2          0.0.0.0/0    25361   /        /                 /
```

Information of VPN1 and VPN2 in the MPLS forwarding table of PE1.

Note:

- For the checking method of PE2, refer to PE1.

#View the BGP route bale again on the CE.

```
CE1#show ip bgp
BGP table version is 4, local router ID is 5.5.5.5
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
    Network          Next Hop        Metric LocPrf Weight Path
[B]*> 5.5.5.5/32     0.0.0.0              0        32768 i
[B]*> 8.8.8.8/32     95.1.1.1             0          0 200 200 i
[B]*> 90.1.0.0/16    95.1.1.1             0          0 200 200 i
[B]*> 95.1.0.0/16    0.0.0.0              0        32768 i

CE1#show ip bgp 8.8.8.8
BGP routing table entry for 8.8.8.8/32
Paths: (1 available, best #1, table Default-IP-Routing-Table)
 Not advertised to any peer
 200 200
  95.1.1.1 (metric 100) from 95.1.1.1 (90.90.90.90)

   Origin IGP, metric 0, localpref 100, valid, external, best
    Last update: 00:06:06 ago

CE1#show ip route
Codes: C - Connected, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external
```

```
B   90.1.0.0/16 [20/0] via 95.1.1.1, 00:03:09, gigabitethernet0
C   95.1.0.0/16 is directly connected, 23:33:15, gigabitethernet0
C   5.5.5.5/32 is directly connected, 04:05:46, loopback0
B   8.8.8.8/32 [20/0] via 95.1.1.1, 00:08:51, gigabitethernet0
```

You can see that there is the route information to CE2 in the BGP route table of the CE1 and the global route table and the AS-PATH of CE2 route is modified to 200 200 in the BGP route table.

On CE1, ping the loopback port of CE2 and view whether the ping can be connected.

```
CE1#ping 8.8.8.8


Press key (ctrl + shift + 6) interrupt it.
Sending 5, 76-byte ICMP Echos to 8.8.8.8 , timeout is 2 seconds:
!!!!!
Success rate is 100% (5/5). Round-trip min/avg/max = 0/0/0 ms.
```

You can see that CE1 can ping CE2.

3.3.7. Configure OSPF Sham Link

Network Requirements

- CE1 and CE2 belong to VPN1; CE and PE use OSPF to advertise the route.
- There is one backdoor link between CE1 and CE2; configure the sham link between PEs to make the VPN traffic between CE1 and CE2 first be forwarded via the global MPLS and only use the backdoor link to back up.
- Configure OSPF between PEs to make PEs communicate with each other; configure MP-IBGP to exchange the VPN route information.

Network Topology

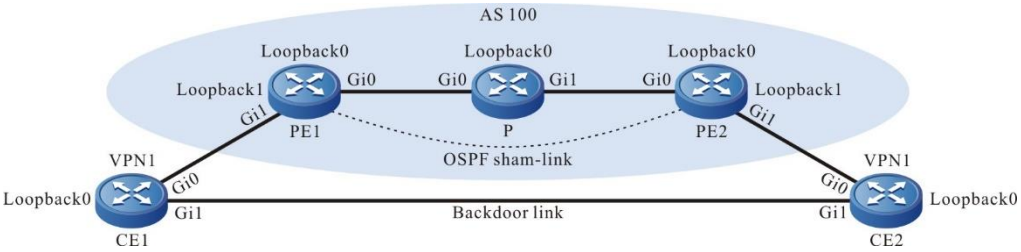

Figure 3-13 Networking of configuring the OSPF sham link

Device	Interface	IP Address	Device	Interface	IP Address
CE1	Gi0	95.1.1.2/16	P	Loopback0	11.11.11.11/32
	Gi1	98.1.1.1/16	PE2	Gi0	92.1.1.1/16
	Loopback0	5.5.5.5/32		Gi1	90.1.1.1/16
PE1	Gi0	93.1.1.2/16		Loopback0	75.75.75.75/32
	Gi1	95.1.1.1/16		Loopback1	6.6.6.6/32
	Loopback0	90.90.90.90/32	CE2	Gi0	90.1.1.2/16
	Loopback1	1.1.1.1/32		Gi1	98.1.1.2/16
P	Gi0	93.1.1.1/16		Loopback0	8.8.8.8/32
	Gi1	92.1.1.2/16			

Configuration Steps

Step 1: Configure the IP address of the interface (omitted).

Step 2: Configure the global OSPF and advertise the global route.

#Configure the global OSPF on PE1.

```
PE1#configure terminal
PE1(config)#router ospf 100
PE1(config-ospf)#network 90.90.90.90 0.0.0.0 area 0
PE1(config-ospf)#network 93.1.0.0 0.0.255.255 area 0
PE1(config-ospf)#exit
```

#Configure the global OSPF on P.

```
P#configure terminal
P(config)#router ospf 100
P(config-ospf)#network 11.11.11.11 0.0.0.0 area 0
P(config-ospf)#network 92.1.0.0 0.0.255.255 area 0
P(config-ospf)#network 93.1.0.0 0.0.255.255 area 0
P(config-ospf)#exit
```

#Configure the global OSPF on PE2.

```
PE2#configure terminal
PE2(config)#router ospf 100
PE2(config-ospf)#network 75.75.75.75 0.0.0.0 area 0
PE2(config-ospf)#network 92.1.0.0 0.0.255.255 area 0
PE2(config-ospf)#exit
```

#After the configuration is complete, view the global route table on the device.

Take PE1 as an example:

```
PE1#show ip route
Codes: C - Connected, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external



C   93.1.0.0/16 is directly connected, 00:34:54, gigabitethernet0
O   92.1.0.0/16 [110/2] via 93.1.1.1, 00:08:12, gigabitethernet0
C   90.90.90.90/32 is directly connected, 00:08:28, loopback0
O   11.11.11.11/32 [110/2] via 93.1.1.1, 00:05:03, gigabitethernet0
O   75.75.75.75/32 [110/3] via 93.1.1.1, 00:06:03, gigabitethernet0
```

You can see that there is the route information of the PE2 and P loopback ports in the global route table of PE1.

Note:

- For the checking method of P, PE2, refer to PE1.

Step 3: Enable MPLS IP and MPLS LDP.

#On PE1, enable the global MPLS IP and MPLS LDP. Meanwhile, enable MPLS IP and MPLS LDP on the interface.

```
PE1(config)#mpls ip
PE1(config)#mpls ldp
PE1(config-ldp)#router-id 90.90.90.90
PE1(config-ldp)#address-family ipv4
PE1(config-ldp-af4)#transport-address 90.90.90.90
PE1(config-ldp-af4)#exit
PE1(config-ldp)#exit
PE1(config)#interface gigabitethernet0
PE1(config-if-gigabitethernet0)#mpls ip
PE1(config-if-gigabitethernet0)#mpls ldp
PE1(config-if-gigabitethernet0)#exit
```

#On P, enable the global MPLS IP and MPLS LDP. Meanwhile, enable MPLS IP and MPLS LDP on the interface.

```
P(config)#mpls ip
P(config)#mpls ldp
P(config-ldp)#router-id 11.11.11.11
P(config-ldp)#address-family ipv4
P(config-ldp-af4)#transport-address 11.11.11.11
P(config-ldp-af4)#exit
P(config-ldp)#exit
P(config)#interface gigabitethernet0
P(config-if-gigabitethernet0)#mpls ip
P(config-if-gigabitethernet0)#mpls ldp
P(config-if-gigabitethernet0)#exit
P(config)#interface gigabitethernet1
P(config-if-gigabitethernet1)#mpls ip
P(config-if-gigabitethernet1)#mpls ldp
P(config-if-gigabitethernet1)#exit
```

#On PE2, enable the global MPLS IP and MPLS LDP. Meanwhile, enable MPLS IP and MPLS LDP on the interface.

```
PE2(config)#mpls ip
PE2(config)#mpls ldp
PE2(config-ldp)#router-id 75.75.75.75
PE2(config-ldp)#address-family ipv4
PE2(config-ldp-af4)#transport-address 75.75.75.75
PE2(config-ldp-af4)#exit
PE2(config-ldp)#exit
PE2(config)#interface gigabitethernet0
PE2(config-if-gigabitethernet0)#mpls ip
PE2(config-if-gigabitethernet0)#mpls ldp
PE2(config-if-gigabitethernet0)#exit
```

#After the configuration is complete, view the LDP session information on the device.

Take PE1 as an example:

```
PE1#show mpls ldp session
Peer IP Address    Peer Type     My Role   State        DS Cap    DeadTime
11.11.11.11        Multicast     Active    OPERATIONAL  Disabled  00:02:20
Statistics for ldp sessions:
    Multicast sessions: 1
    Targeted sessions: 0
```

You can see that PE1 and P set up the LDP session successfully.

#View the route label information on the device.

Take PE1 as an example:

```
PE1#show ip route 11.11.11.11 detail
Codes: C - Connected, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
    U - Per-user Static route
    O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external



O   11.11.11.11/32 [110/2] via 93.1.1.1, label 3, 00:05:03, gigabitethernet0
                   93.1.1.1 [0], gigabitethernet0

PE1#show ip route 75.75.75.75 detail
Codes: C - Connected, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
    U - Per-user Static route
    O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external



O   75.75.75.75/32 [110/2] via 93.1.1.1, label 24016, 00:05:03, gigabitethernet0
                   93.1.1.1 [0], gigabitethernet0
```

You can see that the loopback port route from PE1 to P and PE2 has the label information.

Note:

- For the checking method of P, PE2, refer to PE1.

Step 4: Configure the VPN instance and advertise the CE route to the PE via OSPF.

#On PE1, configure the VPN instance and OSPF in the VPN instance.

```
PE1(config)#ip vrf 1
PE1(config-vrf)#rd 100:1
PE1(config-vrf)#route-target export 100:1
PE1(config-vrf)#route-target import 100:1
PE1(config-vrf)#exit
PE1(config)#interface gigabitethernet1
PE1(config-if-gigabitethernet1)#ip vrf forwarding 1
PE1(config-if-gigabitethernet1)#ip address 95.1.1.1 255.255.0.0
```

```
PE1(config-if-gigabitethernet1)#exit
PE1(config)#router ospf 200 vrf 1
PE1(config-ospf)#network 95.1.0.0 0.0.255.255 area 0
PE1(config-ospf)#exit
```

#On CE1, configure OSPF with PE1, CE2.

```
CE1#configure terminal
CE1(config)#router ospf 100
CE1(config-ospf)#network 5.5.5.5 0.0.0.0 area 0
CE1(config-ospf)#network 95.1.0.0 0.0.255.255 area 0
CE1(config-ospf)#network 98.1.0.0 0.0.255.255 area 0
CE1(config-ospf)#exit
```

#On PE2, configure the VPN instance and OSPF in the VPN instance.

```
PE2(config)#ip vrf 1
PE2(config-vrf)#rd 100:1
PE2(config-vrf)#route-target export 100:1
PE2(config-vrf)#route-target import 100:1
PE2(config-vrf)#exit
PE2(config)#interface gigabitethernet1
PE2(config-if-gigabitethernet1)#ip vrf forwarding 1
PE2(config-if-gigabitethernet1)#ip address 90.1.1.1 255.255.0.0
PE2(config)#exit
PE2(config)#router ospf 200 vrf 1
PE2(config-ospf)#network 90.1.0.0 0.0.255.255 area 0
PE2(config-ospf)#exit
```

#On CE2, configure OSPF with PE2, CE1.

```
CE2#configure terminal
CE2(config)#router ospf 100
CE2(config-ospf)#network 8.8.8.8 0.0.0.0 area 0
CE2(config-ospf)#network 90.1.0.0 0.0.255.255 area 0
CE2(config-ospf)#network 98.1.0.0 0.0.255.255 area 0
CE2(config-ospf)#exit
```

#After the configuration is complete, view the VPN route table on the PE.

Take PE1 as an example:

```
PE1#show ip route vrf 1
Codes: C - Connected, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external
```

```
C   95.1.0.0/16 is directly connected, 00:11:45, gigabitethernet1
O   98.1.0.0/16 [110/2] via 95.1.1.2, 00:10:11, gigabitethernet1
O   5.5.5.5/32 [110/2] via 95.1.1.2, 00:11:11, gigabitethernet1
```

You can see that there is the route information to CE1 loopback port in the VPN route table of PE1.

Note:

- For the checking method of PE2, refer to PE1.

Step 5: Configure MP-IBGP, and use the loopback interface as the peer address; re-distribute the route with the IGP protocol in the VPN instance.

#On PE1, configure MP-IBGP, and enable the VPNv4 address family; re-distribute the route with the IGP protocol in the VPN instance.

```
PE1(config)#router bgp 100
PE1(config-bgp)#neighbor 75.75.75.75 remote-as 100
PE1(config-bgp)#neighbor 75.75.75.75 update-source loopback0
PE1(config-bgp)#address-family vpnv4
PE1(config-bgp-af)#neighbor 75.75.75.75 activate
PE1(config-bgp-af)#neighbor 75.75.75.75 send-community extended
PE1(config-bgp-af)#exit-address-family
PE1(config-bgp)#address-family ipv4 vrf 1
PE1(config-bgp-af)#redistribute ospf 200
PE1(config-bgp-af)#exit-address-family
PE1(config-bgp)#exit
PE1(config)#router ospf 200 vrf 1
PE1(config-ospf)#redistribute bgp 100
PE1(config-ospf)#exit
```

#On PE2, configure MP-IBGP, and enable the VPNv4 address family; re-distribute the route with the IGP protocol in the VPN instance.

```
PE2(config)#router bgp 100
PE2(config-bgp)#neighbor 90.90.90.90 remote-as 100
PE2(config-bgp)#neighbor 90.90.90.90 update-source loopback0
PE2(config-bgp)#address-family vpnv4
PE2(config-bgp-af)#neighbor 90.90.90.90 activate
PE2(config-bgp-af)#neighbor 90.90.90.90 send-community extended
PE2(config-bgp-af)#exit-address-family
PE2(config-bgp)#address-family ipv4 vrf 1
```

```
PE2(config-bgp-af)#redistribute ospf 200
PE2(config-bgp-af)#exit-address-family
PE2(config-bgp)#exit
PE2(config)#router ospf 200 vrf 1
PE2(config-ospf)#redistribute bgp 100
PE2(config-ospf)#exit
```

#After the configuration is complete, view the BGP neighbor information on PE1.

Take PE1 as an example:

```
PE1#show ip bgp vpnv4 all summary
BGP router identifier 90.90.90.90, local AS number 100
BGP table version is 6
1 BGP AS-PATH entries
0 BGP community entries

Neighbor        V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
75.75.75.75     4   100      40      41        5    0    0 00:32:01        2

Total number of neighbors 1
```

The content of the State/PfxRcd list is displayed as number (the number of the route prefixes received from the neighbor), and you can see that PE1 and PE2 set up the BGP neighbor successfully.

#View the BGP VPNv4 route table and VPN route table on the PE.

Take PE1 as an example:

```
PE1#show ip bgp vpnv4 vrf 1
BGP table version is 19, local router ID is 90.90.90.90
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network          Next Hop            Metric LocPrf Weight Path
Route Distinguisher: 100:1 (Default for VRF 1)
[B]* i5.5.5.5/32    75.75.75.75              5    100      0 ?
[0]*>               95.1.1.2                 2        32768 ?
[0]*> 8.8.8.8/32    95.1.1.2                 5        32768 ?
[B]* i              75.75.75.75              2    100      0 ?
[0]*> 90.1.0.0/16   95.1.1.2                 5        32768 ?
[B]* i              75.75.75.75              1    100      0 ?
[B]* i95.1.0.0/16   75.75.75.75              5    100      0 ?
[0]*>               0.0.0.0                  1        32768 ?
```

```
[B]* i98.1.0.0/16       75.75.75.75          4    100     0 ?
[O]*>                   95.1.1.2             4          32768 ?
```

```
PE1#show ip route vrf 1
Codes: C - Connected, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external
```

```
O   90.1.0.0/16 [110/5] via 95.1.1.2, 00:00:05, gigabitethernet1
C   95.1.0.0/16 is directly connected, 03:01:34, gigabitethernet1
O   98.1.0.0/16 [110/4] via 95.1.1.2, 02:58:04, gigabitethernet1
O   5.5.5.5/32 [110/2] via 95.1.1.2, 03:00:43, gigabitethernet1
O   8.8.8.8/32 [110/5] via 95.1.1.2, 00:00:05, gigabitethernet1
```

You can see that the route to CE2 in the BGP VPNv4 route table and VPN route table passes the CE1 backdoor link, but does not pass the global MPLS network.

Note:

- For the checking method of PE2, refer to PE1.

Step 6: On the PE, configure the OSPF sham link and configure the COST value of the interface on the CE1 backdoor link, making CEs communicate with each other via the global network.

#On PE1, configure the OSPF sham link and advertise the loopback port route of the OSPF sham link starting point in the BGP.

```
PE1(config)#interface loopback 1
PE1(config-if-loopback1)#ip vrf forwarding 1
PE1(config-if-loopback1)#ip address 1.1.1.1 255.255.255.255
PE1(config-if-loopback1)#exit
PE1(config)#router bgp 100
PE1(config-bgp)#address-family ipv4 vrf 1
PE1(config-bgp-af)#network 1.1.1.1 255.255.255.255
PE1(config-bgp-af)#exit-address-family
PE1(config-bgp)#exit
PE1(config)#router ospf 200 vrf 1
PE1(config-ospf)#area 0 sham-link 1.1.1.1 6.6.6.6
PE1(config-ospf)#exit
```

#On PE2, configure the OSPF sham link and advertise the loopback port route of the OSPF sham link starting point in the BGP.

```
PE2(config)#interface loopback 1
PE2(config-if-loopback1)#ip vrf forwarding 1
PE2(config-if-loopback1)#ip address 6.6.6.6 255.255.255.255
PE2(config-if-loopback1)#exit
PE2(config)#router bgp 100
PE2(config-bgp)#address-family ipv4 vrf 1
PE2(config-bgp-af)#network 6.6.6.6 255.255.255.255
PE2(config-bgp-af)#exit-address-family
PE2(config-bgp)#exit
PE2(config)#router ospf 200 vrf 1
PE2(config-ospf)#area 0 sham-link 6.6.6.6 1.1.1.1
PE2(config-ospf)#exit
```

#On CE1, modify the COST value of the backdoor route interface, making CEs communicate via the global network.

```
CE1(config)#interface gigabitethernet1
CE1(config-if-gigabitethernet1)#ip ospf cost 4
CE1(config-if-gigabitethernet1)#exit
```

#On CE2, modify the COST value of the backdoor route interface, making CEs communicate via the global network.

```
CE2(config)#interface gigabitethernet1
CE2(config-if-gigabitethernet1)#ip ospf cost 4
CE2(config-if-gigabitethernet1)#exit
```

Step7: Check the result.

#After the configuration is complete, view the OSPF sham link information on the PE.

```
PE1#show ip ospf sham-links
Sham Link SLINK0 to addr 6.6.6.6 is up
Area 0.0.0.0 source address 1.1.1.1
 Run as demand circuit
 DoNotAge LSA allowed. Cost of using 1 State Point-To-Point,
 Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
  Hello due in 00:00:07
  Adjacency state Full(Hello suppressed)

PE2#show ip ospf sham-links
Sham Link SLINK0 to addr 1.1.1.1 is up
Area 0.0.0.0 source address 6.6.6.6
```

```
    Run as demand circuit
    DoNotAge LSA allowed. Cost of using 1 State Point-To-Point,
    Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
      Hello due in 00:00:04
      Adjacency state Full(Hello suppressed)
```

#On the PE, view the BGP VPNv4 route table and VPN route table again.

Take PE1 as an example:

```
PE1#show ip route vrf 1
Codes: C - Connected, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external



O   90.1.0.0/16 [110/2] via 75.75.75.75, 00:11:32, gigabitethernet0
C   95.1.0.0/16 is directly connected, 03:22:25, gigabitethernet1
O   98.1.0.0/16 [110/4] via 95.1.1.2, 03:18:55, gigabitethernet1
C   1.1.1.1/32 is directly connected, 00:12:09, loopback1
O   5.5.5.5/32 [110/2] via 95.1.1.2, 03:21:34, gigabitethernet1
B   6.6.6.6/32 [200/0] via 75.75.75.75, 03:09:38, gigabitethernet0
O   8.8.8.8/32 [110/3] via 75.75.75.75, 00:11:32, gigabitethernet0

PE1#show ip bgp vpnv4 vrf 1
BGP table version is 17, local router ID is 90.90.90.90
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network          Next Hop          Metric LocPrf Weight Path
Route Distinguisher: 100:1 (Default for VRF 1)
[B]*> 1.1.1.1/32         0.0.0.0                0         32768 i
[O]*> 5.5.5.5/32         95.1.1.2               2         32768 ?
[B]*>i6.6.6.6/32         75.75.75.75            0    100      0 i
[B]*>i8.8.8.8/32         75.75.75.75            2    100      0 ?
[B]*>i90.1.0.0/16        75.75.75.75            1    100      0 ?
[O]*> 95.1.0.0/16        0.0.0.0                1         32768 ?
[B]* i98.1.0.0/16        75.75.75.75            4    100      0 ?
[O]*>                    95.1.1.2               4         32768 ?
```

You can see that the route to CE2 in the BGP VPNv4 route table and VPN route table of PE1 passes the global MPLS network, but does not pass the CE1 backdoor link.

#View the MPLS forwarding table on the PE.

Take PE1 as an example:

```
PE1#show mpls forwarding-table
Pro: L - LDP, O - OSPF, B - MP-BGP, R - RSVP, M - Mapped-Route, S - Static Label,ML - mLDP (ML FEC: Root address/OT/OV), RM - RSVP P2MP (RM FEC: P2MP ID/TID)

Pro Ident       FEC             Inlabel Outlabel Outgoing          Next hop
B  1           0.0.0.0/0        25120   /       /                  /
```

You can see that there is the route label information of VPN1 in the MPLS forwarding table of PE1.

Note:

- For the checking method of PE2, refer to PE1.

#On CE1, view the VPN route table and traceroute the loopback port of CE2.

```
CE1#show ip route
Codes: C - Connected, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external

O   90.1.0.0/16 [110/3] via 95.1.1.1, 00:00:02, gigabitethernet0
C   95.1.0.0/16 is directly connected, 04:22:46, gigabitethernet0
C   98.1.0.0/16 is directly connected, 05:05:23, gigabitethernet1
C   127.0.0.0/8 is directly connected, 241:57:31, lo0
C   5.5.5.5/32 is directly connected, 29:40:05, loopback0
O   8.8.8.8/32 [110/4] via 95.1.1.1, 00:00:02, gigabitethernet0

CE1#traceroute 8.8.8.8
Type escape sequence to abort.
Tracing the route to 8.8.8.8 , min ttl = 1, max ttl = 30 .

 1  95.1.1.1   0 ms    0 ms    0 ms
 2  93.1.1.1 [MPLS: Labels 24016/25120 Exp 0]     0 ms    0 ms    0 ms
 3  92.1.1.1 [MPLS: Labels 25120 Exp 0] 0 ms    0 ms    0 ms
```

```
4  8.8.8.8    16 ms    0 ms    0 ms
```

You can see that the path from CE1 to CE2 passes the global network.

3.3.8. Enterprise Intranet Accessing Internet

Network Requirements

- PE1, PE2 connect the CE of VPN1 respectively; CE1 and CE2 belong to one VPN.
- Internet gateway is the external route of the VPN, and all sites in the VPN are connected to Internet via the enterprise intranet.
- The VPN member forwards the data flow of the accessed Internet to the CE (CE1) of connecting Internet gateway by importing one default route of accessing Internet.
- Configure OSPF between PEs to make PEs communicate with each other; configure MP-IBGP to exchange the VPN route information.

Network Topology

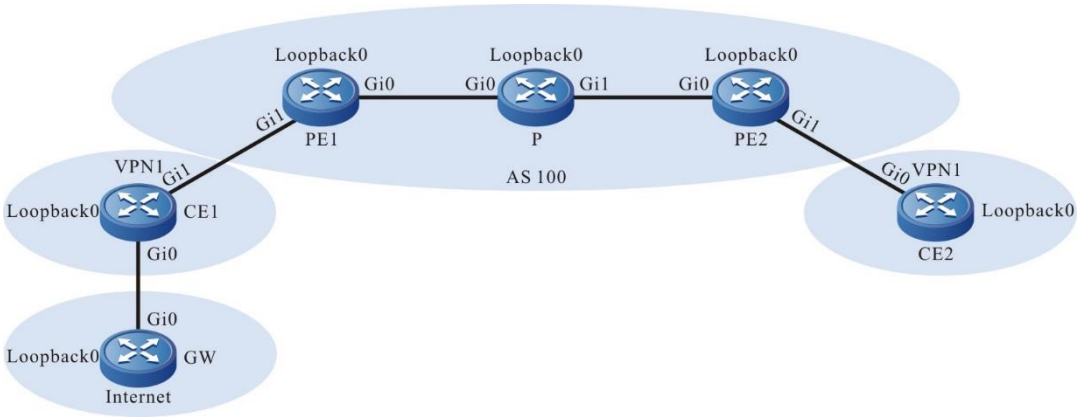

Figure 3-14 The access mode of the enterprise intranet

Device	Interface	IP Address	Device	Interface	IP Address
CE1	Gi0	95.1.1.2/16	P	Loopback0	11.11.11.11/32
	Gi1	98.1.1.1/16	PE2	Gi0	92.1.1.1/16
	Loopback0	5.5.5.5/32		Gi1	90.1.1.1/16
PE1	Gi0	93.1.1.2/16		Loopback0	75.75.75.75/32
	Gi1	95.1.1.1/16	CE2	Gi0	90.1.1.2/16
	Loopback0	90.90.90.90/32		Loopback0	8.8.8.8/32

Device	Interface	IP Address	Device	Interface	IP Address
P	Gi0	93.1.1.1/16	GW	Gi0	98.1.1.2/16
	Gi1	92.1.1.2/16		Loopback0	1.1.1.1/32

Configuration Steps

Step 1: Configure the IP address of the interface (omitted).

Step 2: Configure the global OSPF and advertise the global route.

#Configure the global OSPF on PE1.

```
PE1#configure terminal
PE1(config)#router ospf 100
PE1(config-ospf)#network 90.90.90.90 0.0.0.0 area 0
PE1(config-ospf)#network 93.1.0.0 0.0.255.255 area 0
PE1(config-ospf)#exit
```

#Configure the global OSPF on P.

```
P#configure terminal
P(config)#router ospf 100
P(config-ospf)#network 11.11.11.11 0.0.0.0 area 0
P(config-ospf)#network 92.1.0.0 0.0.255.255 area 0
P(config-ospf)#network 93.1.0.0 0.0.255.255 area 0
P(config-ospf)#exit
```

#Configure the global OSPF on PE2.

```
PE2#configure terminal
PE2(config)#router ospf 100
PE2(config-ospf)#network 75.75.75.75 0.0.0.0 area 0
PE2(config-ospf)#network 92.1.0.0 0.0.255.255 area 0
PE2(config-ospf)#exit
```

#After the configuration is complete, view the global route table on the device.

Take PE1 as an example:

```
PE1#show ip route
Codes: C - Connected, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external
```

```
C   93.1.0.0/16 is directly connected, 00:34:54, gigabitethernet0
O   92.1.0.0/16 [110/2] via 93.1.1.1, 00:08:12, gigabitethernet0
C   90.90.90.90/32 is directly connected, 154:02:28, loopback0
O   11.11.11.11/32 [110/2] via 93.1.1.1, 00:06:12, gigabitethernet0
O   75.75.75.75/32 [110/3] via 93.1.1.1, 00:06:03, gigabitethernet0
```

You can see that there is the route information of the PE2 and P loopback ports in the global route table of PE1.

Note:

- For the checking method of P and PE2, refer to PE1.

Step 3: Enable MPLS IP and MPLS LDP.

#On PE1, enable the global MPLS IP and MPLS LDP. Meanwhile, enable MPLS IP and MPLS LDP on the interface.

```
PE1(config)#mpls ip
PE1(config)#mpls ldp
PE1(config-ldp)#router-id 90.90.90.90
PE1(config-ldp)#address-family ipv4
PE1(config-ldp-af4)#transport-address 90.90.90.90
PE1(config-ldp-af4)#exit
PE1(config-ldp)#exit
PE1(config)#interface gigabitethernet0
PE1(config-if-gigabitethernet0)#mpls ip
PE1(config-if-gigabitethernet0)#mpls ldp
PE1(config-if-gigabitethernet0)#exit
```

#On P, enable the global MPLS IP and MPLS LDP. Meanwhile, enable MPLS IP and MPLS LDP on the interface.

```
P(config)#mpls ip
P(config)#mpls ldp
P(config-ldp)#router-id 11.11.11.11
P(config-ldp)#address-family ipv4
P(config-ldp-af4)#transport-address 11.11.11.11
P(config-ldp-af4)#exit
P(config-ldp)#exit
P(config)#interface gigabitethernet0
P(config-if-gigabitethernet0)#mpls ip
P(config-if-gigabitethernet0)#mpls ldp
```

```
P(config-if-gigabitethernet0)#exit
P(config)#interface gigabitethernet1
P(config-if-gigabitethernet1)#mpls ip
P(config-if-gigabitethernet1)#mpls ldp
P(config-if-gigabitethernet1)#exit
```

#On PE2, enable the global MPLS IP and MPLS LDP. Meanwhile, enable MPLS IP and MPLS LDP on the interface.

```
PE2(config)#mpls ip
PE2(config)#mpls ldp
PE2(config-ldp)#router-id 75.75.75.75
PE2(config-ldp)#address-family ipv4
PE2(config-ldp-af4)#transport-address 75.75.75.75
PE2(config-ldp-af4)#exit
PE2(config-ldp)#exit
PE2(config)#interface gigabitethernet0
PE2(config-if-gigabitethernet0)#mpls ip
PE2(config-if-gigabitethernet0)#mpls ldp
PE2(config-if-gigabitethernet0)#exit
```

#After the configuration is complete, view the LDP session information on the device.

Take PE1 as an example:

```
PE1#show mpls ldp session
Peer IP Address    Peer Type    My Role   State       DS Cap    DeadTime
11.11.11.11        Multicast    Active    OPERATIONAL   Disabled  00:02:20
Statistics for ldp sessions:
    Multicast sessions: 1
    Targeted sessions: 0
```

You can see that PE1 and P set up the LDP session successfully.

#View the route label information on the device.

Take PE1 as an example:

```
PE1#show ip route 11.11.11.11 detail
Codes: C - Connected, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
    U - Per-user Static route
    O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external



O   11.11.11.11/32 [110/2] via 93.1.1.1, label 3, 00:05:03, gigabitethernet0
```

```
                    93.1.1.1 [0], gigabitethernet0

        PE1#show ip route 75.75.75.75 detail
        Codes: C - Connected, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
            U - Per-user Static route
            O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external



        O   75.75.75.75/32 [110/2] via 93.1.1.1, label 24016, 00:05:03, gigabitethernet0
                    93.1.1.1 [0], gigabitethernet0
```

You can see that the loopback port route from PE1 to P and PE2 has the label information.

Note:

- For the checking method of P and PE2, refer to PE1.

Step 4: Configure the VPN instance and advertise the CE route to the PE via OSPF.

#On PE1, configure the VPN instance and OSPF in the VPN instance.

```
PE1(config)#ip vrf 1
PE1(config-vrf)#rd 100:1
PE1(config-vrf)#route-target export 100:1
PE1(config-vrf)#route-target import 100:1
PE1(config-vrf)#exit
PE1(config)#interface gigabitethernet1
PE1(config-if-gigabitethernet1)#ip vrf forwarding 1
PE1(config-if-gigabitethernet1)#ip address 95.1.1.1 255.255.0.0
PE1(config-if-gigabitethernet1)#exit
PE1(config)#router ospf 200 vrf 1
PE1(config-ospf)#network 95.1.0.0 0.0.255.255 area 0
PE1(config-ospf)#exit
```

#Configure OSPF on CE1.

```
CE1#configure terminal
CE1(config)#router ospf 100
CE1(config-ospf)#network 5.5.5.5 0.0.0.0 area 0
CE1(config-ospf)#network 95.1.0.0 0.0.255.255 area 0
CE1(config-ospf)#exit
```

#On PE2, configure the VPN instance and OSPF in the VPN instance.

```
PE2(config)#ip vrf 1
```

```
PE2(config-vrf)#rd 100:1
PE2(config-vrf)#route-target export 100:1
PE2(config-vrf)#route-target import 100:1
PE2(config-vrf)#exit
PE2(config)#interface gigabitethernet1
PE2(config-if-gigabitethernet1)#ip vrf forwarding 1
PE2(config-if-gigabitethernet1)#ip address 90.1.1.1 255.255.0.0
PE2(config)#exit
PE2(config)#router ospf 200 vrf 1
PE2(config-ospf)#network 90.1.0.0 0.0.255.255 area 0
PE2(config-ospf)#exit
```

#Configure OSPF on CE2.

```
CE2#configure terminal
CE2(config)#router ospf 100
CE2(config-ospf)#network 8.8.8.8 0.0.0.0 area 0
CE2(config-ospf)#network 90.1.0.0 0.0.255.255 area 0
CE2(config-ospf)#exit
```

#After the configuration is complete, view the VPN route table on the PE.

Take PE1 as an example:

```
PE1#show ip route vrf 1
Codes: C - Connected, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external

C   95.1.0.0/16 is directly connected, 00:11:45, gigabitethernet1
O   5.5.5.5/32 [110/2] via 95.1.1.2, 00:11:11, gigabitethernet1
```

You can see that there is the route information to CE1 loopback port in the VPN route table of PE1.

Note:

For the checking method of PE2, refer to PE1.

Step 5: Configure MP-IBGP, and use the loopback interface as the peer address; re-distribute the route with the IGP protocol in the VPN instance.

#On PE1, configure MP-IBGP, and enable the VPNv4 address family; re-distribute the route with the IGP protocol in the VPN instance.

```
PE1(config)#router bgp 100
```

```
PE1(config-bgp)#neighbor 75.75.75.75 remote-as 100
PE1(config-bgp)#neighbor 75.75.75.75 update-source loopback0
PE1(config-bgp)#address-family vpnv4
PE1(config-bgp-af)#neighbor 75.75.75.75 activate
PE1(config-bgp-af)#neighbor 75.75.75.75 send-community extended
PE1(config-bgp-af)#exit-address-family
PE1(config-bgp)#address-family ipv4 vrf 1
PE1(config-bgp-af)#redistribute ospf 200
PE1(config-bgp-af)#exit-address-family
PE1(config-bgp)#exit
PE1(config)#router ospf 200 vrf 1
PE1(config-ospf)#redistribute bgp 100
PE1(config-ospf)#exit
```

#On PE2, configure MP-IBGP, and enable the VPNv4 address family; re-distribute the route with the IGP protocol in the VPN instance.

```
PE2(config)#router bgp 100
PE2(config-bgp)#neighbor 90.90.90.90 remote-as 100
PE2(config-bgp)#neighbor 90.90.90.90 update-source loopback0
PE2(config-bgp)#address-family vpnv4
PE2(config-bgp-af)#neighbor 90.90.90.90 activate
PE2(config-bgp-af)#neighbor 90.90.90.90 send-community extended
PE2(config-bgp-af)#exit-address-family
PE2(config-bgp)#address-family ipv4 vrf 1
PE2(config-bgp-af)#redistribute ospf 200
PE2(config-bgp-af)#exit-address-family
PE2(config-bgp)#exit
PE2(config)#router ospf 200 vrf 1
PE2(config-ospf)#redistribute bgp 100
PE2(config-ospf)#exit
```

#After the configuration is complete, view the BGP neighbor information.

Take PE1 as an example:

```
PE1#show ip bgp vpnv4 all summary
BGP router identifier 90.90.90.90, local AS number 100
BGP table version is 6
1 BGP AS-PATH entries
0 BGP community entries
```

```
Neighbor        V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
75.75.75.75     4   100      40      41        5    0    0 00:32:01        4

Total number of neighbors 1
```

The content of the State/PfxRcd list is displayed as number (the number of the route prefixes received from the neighbor), and you can see that PE1 and PE2 set up the BGP neighbor successfully.

#View the BGP VPNv4 route table and VPN1 route table on the PE.

Take PE1 as an example:

```
PE1#show ip bgp vpnv4 vrf 1
BGP table version is 39, local router ID is 90.90.90.90
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network          Next Hop            Metric LocPrf Weight Path
Route Distinguisher: 100:1 (Default for VRF 1)
[0]*> 5.5.5.5/32         95.1.1.2                 2         32768 ?
[B]*>i8.8.8.8/32         75.75.75.75              2    100      0 ?
[B]*>i90.1.0.0/16        75.75.75.75              1    100      0 ?
[0]*> 95.1.0.0/16        0.0.0.0                  1         32768 ?

PE1#show ip route vrf 1
Codes: C - Connected, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external



B   90.1.0.0/16 [200/1] via 75.75.75.75, 00:20:04, gigabitethernet0
C   95.1.0.0/16 is directly connected, 00:51:28, gigabitethernet1
O   5.5.5.5/32 [110/2] via 95.1.1.2, 00:50:39, gigabitethernet1
B   8.8.8.8/32 [200/2] via 75.75.75.75, 00:20:04, gigabitethernet0
```

You can see that there is the route information to CE2 in the BGP VPNv4 route table and VPN1 route table of CE1..

#View the MPLS forwarding table on the PE.

Take PE1 as an example:

```
PE1#show mpls forwarding-table
```

```
Pro: L - LDP, O - OSPF, B - MP-BGP, R - RSVP, M - Mapped-Route, S - Static
Label,ML - mLDP (ML FEC: Root address/OT/OV), RM - RSVP P2MP (RM FEC: P2MP
ID/TID)


Pro Ident       FEC             Inlabel Outlabel Outgoing           Next hop
B   1           0.0.0.0/0       25120   /       /                   /
```

You can see that there is the route label information of VPN1 in the MPLS forwarding table of PE1.

Note:

- For the checking method of PE2, refer to PE1.

Step 6: Configure the static route to make the VPN member access Internet.

#On CE1, configure the default route to Internet.

```
CE1(config)#ip route 0.0.0.0 0.0.0.0 98.1.1.2
```

#On PE1, configure the default route to Internet and re-distribute the default route to BGP, so as to advertise the route to Internet to the peer PE and CE.

```
PE1(config)#ip route vrf 1 0.0.0.0 0.0.0.0 95.1.1.2
PE1(config)#router bgp 100
PE1(config-bgp)#address-family ipv4 vrf 1
PE1(config-bgp-af)#redistribute static
PE1(config-bgp-af)#default-information originate
PE1(config-bgp-af)#exit-address-family
PE1(config-bgp)#exit
```

#In OSPF of PE2, enable the function of importing the default route, receiving the re-distributed route.

```
PE2(config)#router ospf 200
PE2(config-ospf)#default-information originate
PE2(config-ospf)#exit
```

#On the Internet gateway, configure the default route.

```
GW#configure terminal
GW(config)#ip route 0.0.0.0 0.0.0.0 98.1.1.1
```

Caution:

- To configure the BGP to re-distribute the default route, use the **default-information originate** command.

Step7: Check the result.

#After the configuration is complete, view the BGP VPNv4 route table and VPN1 route table on the device.

Take PE1 as an example:

```
PE1#show ip bgp vpnv4 vrf 1
BGP table version is 39, local router ID is 90.90.90.90
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network          Next Hop          Metric LocPrf Weight Path
Route Distinguisher: 100:1 (Default for VRF 1)
[S]*> 0.0.0.0/0         95.1.1.2               0        32768 ?
[B]*>i8.8.8.8/32        75.75.75.75            2    100      0 ?
[O]*> 5.5.5.5/32        95.1.1.2               2        32768 ?
[B]*>i90.1.0.0/16       75.75.75.75            1    100      0 ?
[O]*> 95.1.0.0/16       0.0.0.0                1        32768 ?

PE1#show ip route vrf 1
Codes: C - Connected, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external



S   0.0.0.0/0 [1/10] via 95.1.1.2, 01:12:43, gigabitethernet1
B   90.1.0.0/16 [200/1] via 75.75.75.75, 00:41:19, gigabitethernet0
C   95.1.0.0/16 is directly connected, 01:12:43, gigabitethernet1
O   5.5.5.5/32 [110/2] via 95.1.1.2, 01:11:55, gigabitethernet1
B   8.8.8.8/32 [200/2] via 75.75.75.75, 00:41:19, gigabitethernet0
```

You can see that there is one default route to CE1 on the BGP VPNv4 route table and VPN route table of PE1.

#Check the reachability of the device to Internet.

```
PE1#ping vrf 1 1.1.1.1



Press key (ctrl + shift + 6) interrupt it.
Sending 5, 76-byte ICMP Echos to 98.1.1.2 , timeout is 2 seconds:
!!!!!
Success rate is 100% (5/5). Round-trip min/avg/max = 0/0/0 ms.

PE2#ping vrf 1 1.1.1.1
```

```
Press key (ctrl + shift + 6) interrupt it.
Sending 5, 76-byte ICMP Echos to 98.1.1.2 , timeout is 2 seconds:
!!!!!
Success rate is 100% (5/5). Round-trip min/avg/max = 0/0/0 ms.

CE2#ping 1.1.1.1

Press key (ctrl + shift + 6) interrupt it.
Sending 5, 76-byte ICMP Echos to 98.1.1.2 , timeout is 2 seconds:
!!!!!
Success rate is 100% (5/5). Round-trip min/avg/max = 0/3/16 ms.
```

You can see that PC1, PE2, CE2 can ping the loopback ports of the Internet gateway.

3.3.9. Service Provider Network Accessing Internet

Network Requirements

- PE1, PE2 connect the CE of VPN1 respectively; CE1 and CE2 belong to one VPN.
- Internet gateway is the external route of the VPN, and all sites in the VPN are connected to Internet via the service provider network.
- The VPN member forwards the data flow of the accessed Internet to the PE (PE1) of connecting Internet gateway by importing one default route of accessing Internet.
- Configure OSPF between PEs to make PEs communicate with each other; configure MP-IBGP to exchange the VPN route information.

Network Topology

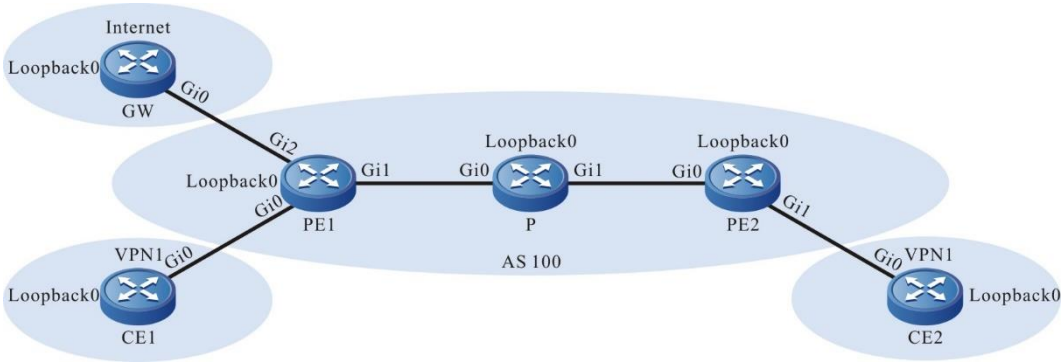

Figure 3-15 The access mode of the service provider network

Device	Interface	IP Address	Device	Interface	IP Address
CE1	Gi0	10.1.1.1/24	P	Loopback0	22.22.22.22/32
	Loopback0	1.1.1.1/32	PE2	Gi0	10.1.3.2/24
PE1	Gi0	10.1.1.2/24		Gi1	10.1.4.1/24
	Gi1	10.1.2.1/24		Loopback0	33.33.33.33/32
	Gi2	10.1.5.1/24	CE2	Gi0	10.1.4.2/24
	Loopback0	11.11.11.11/32		Loopback0	2.2.2.2/32
P	Gi0	10.1.2.2/24	GW	Gi0	10.1.5.2/24
	Gi1	10.1.3.1/24		Loopback0	3.3.3.3/32

Configuration Steps

Step 1: Configure the IP address of the interface (omitted).

Step 2: Configure the global OSPF and advertise the global route.

#Configure the global OSPF on PE1.

```
PE1#configure terminal
PE1(config)#router ospf 100
PE1(config-ospf)#network 10.1.2.0 0.0.0.255 area 0
PE1(config-ospf)#network 11.11.11.11 0.0.0.0 area 0
PE1(config-ospf)#exit
```

#Configure the global OSPF on P.

```
P#configure terminal
P(config)#router ospf 100
P(config-ospf)#network 10.1.2.0 0.0.0.255 area 0
P(config-ospf)#network 10.1.3.0 0.0.0.255 area 0
P(config-ospf)#network 22.22.22.22 0.0.0.0 area 0
P(config-ospf)#exit
```

#Configure the global OSPF on PE2.

```
PE2#configure terminal
PE2(config)#router ospf 100
PE2(config-ospf)#network 10.1.3.0 0.0.0.255 area 0
PE2(config-ospf)#network 33.33.33.33 0.0.0.0 area 0
PE2(config-ospf)#exit
```

#After the configuration is complete, view the global route table on the device.

Take PE1 as an example:

```
PE1#show ip route
Codes: C - Connected, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
    U - Per-user Static route
    O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external



C   10.1.2.0/24 is directly connected, 65:47:37, gigabitethernet1
O   10.1.3.0/24 [110/2] via 10.1.2.2, 01:18:39, gigabitethernet1
C   10.1.5.0/24 is directly connected, 00:22:25, gigabitethernet2
C   127.0.0.0/8 is directly connected, 65:47:57, lo0
C   11.11.11.11/32 is directly connected, 65:47:37, loopback0
O   22.22.22.22/32 [110/2] via 10.1.2.2, 65:11:53, gigabitethernet1
O   33.33.33.33/32 [110/3] via 10.1.2.2, 01:18:34, gigabitethernet1
```

You can see that there is the route information of the PE2 and P loopback ports in the global route table of PE1.

Note:

- For the checking method of P and PE2, refer to PE1.

Step 3: Enable MPLS IP and MPLS LDP.

#On PE1, enable the global MPLS IP and MPLS LDP. Meanwhile, enable MPLS IP and MPLS LDP on the interface.

```
PE1(config)#mpls ip
PE1(config)#mpls ldp
PE1(config-ldp)#router-id 11.11.11.11
PE1(config-ldp)#address-family ipv4
PE1(config-ldp-af4)#transport-address 11.11.11.11
PE1(config-ldp-af4)#exit
PE1(config-ldp)#exit
PE1(config)#interface gigabitethernet1
PE1(config-if-gigabitethernet1)#mpls ip
```

```
PE1(config-if-gigabitethernet1)#mpls ldp
PE1(config-if-gigabitethernet1)#exit
```

#On P, enable the global MPLS IP and MPLS LDP. Meanwhile, enable MPLS IP and MPLS LDP on the interface.

```
P(config)#mpls ip
P(config)#mpls ldp
P(config-ldp)#router-id 22.22.22.22
P(config-ldp)#address-family ipv4
P(config-ldp-af4)#transport-address 22.22.22.22
P(config-ldp-af4)#exit
P(config-ldp)#exit
P(config)#interface gigabitethernet0
P(config-if-gigabitethernet0)#mpls ip
P(config-if-gigabitethernet0)#mpls ldp
P(config-if-gigabitethernet0)#interface gigabitethernet1
P(config-if-gigabitethernet1)#mpls ip
P(config-if-gigabitethernet1)#mpls ldp
P(config-if-gigabitethernet1)#exit
```

#On PE2, enable the global MPLS IP and MPLS LDP. Meanwhile, enable MPLS IP and MPLS LDP on the interface.

```
PE2(config)#mpls ip
PE2(config)#mpls ldp
PE2(config-ldp)#router-id 33.33.33.33
PE2(config-ldp)#address-family ipv4
PE2(config-ldp-af4)#transport-address 33.33.33.33
PE2(config-ldp-af4)#exit
PE2(config-ldp)#exit
PE2(config)#interface gigabitethernet0
PE2(config-if-gigabitethernet0)#mpls ip
PE2(config-if-gigabitethernet0)#mpls ldp
PE2(config-if-gigabitethernet0)#exit
```

#After the configuration is complete, view the LDP session information on the device.

Take PE1 as an example:

```
PE1#show mpls ldp session
Peer IP Address   Peer Type    My Role  State        DS Cap   DeadTime
22.22.22.22       Multicast    Active   OPERATIONAL  Disabled 00:02:20
Statistics for ldp sessions:
```

```
Multicast sessions: 1
Targeted sessions: 0
```

You can see that PE1 and P set up the LDP session successfully.

#View the route label information on the device.

Take PE1 as an example:

```
PE1#show ip route 22.22.22.22 detail
Codes: C - Connected, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
    U - Per-user Static route
    O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external



O   22.22.22.22/32 [110/2] via 10.1.2.2, label 3, 00:05:03, gigabitethernet1
                   10.1.2.2 [0], gigabitethernet1

PE1#show ip route 33.33.33.33 detail
Codes: C - Connected, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
    U - Per-user Static route
    O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external



O   33.33.33.33/32 [110/2] via 10.1.2.2, label 24016, 00:05:03, gigabitethernet1
                   10.1.2.2 [0], gigabitethernet1
```

You can see that the loopback port route from PE1 to P and PE2 has the label information.

Note:

- For the checking method of P and PE2, refer to PE1.

Step 4: Configure the VPN instance and advertise the CE route to the PE via OSPF.

#On PE1, configure the VPN instance and OSPF in the VPN instance.

```
PE1(config)#ip vrf 1
PE1(config-vrf)#rd 100:1
PE1(config-vrf)#route-target export 100:1
PE1(config-vrf)#route-target import 100:1
PE1(config-vrf)#exit
PE1(config)#interface gigabitethernet1
PE1(config-if-gigabitethernet1)#ip vrf forwarding 1
```

```
PE1(config-if-gigabitethernet1)#ip address 10.1.1.2 255.255.255.0
PE1(config-if-gigabitethernet1)#exit
PE1(config)#router ospf 200 vrf 1
PE1(config-ospf)#network 10.1.1.0 0.255.255.255 area 0
PE1(config-ospf)#exit
```

#Configure OSPF on CE1.

```
CE1#configure terminal
CE1(config)#router ospf 100
CE1(config-ospf)#network 1.1.1.1 0.0.0.0 area 0
CE1(config-ospf)#network 10.1.1.0 0.0.0.255 area 0
CE1(config-ospf)#exit
```

#On PE2, configure the VPN instance and OSPF in the VPN instance.

```
PE2(config)#ip vrf 1
PE2(config-vrf)#rd 100:1
PE2(config-vrf)#route-target export 100:1
PE2(config-vrf)#route-target import 100:1
PE2(config-vrf)#exit
PE2(config)#interface gigabitethernet1
PE2(config-if-gigabitethernet1)#ip vrf forwarding 1
PE2(config-if-gigabitethernet1)#ip address 10.1.4.1 255.255.255.0
PE2(config)#exit
PE2(config)#router ospf 200 vrf 1
PE2(config-ospf)#network 10.1.4.0 0.0.0.255 area 0
PE2(config-ospf)#exit
```

#Configure OSPF on CE2.

```
CE2#configure terminal
CE2(config)#router ospf 100
CE2(config-ospf)#network 2.2.2.2 0.0.0.0 area 0
CE2(config-ospf)#network 10.1.4.0 0.0.0.255 area 0
CE2(config-ospf)#exit
```

#After the configuration is complete, view the VPN route table on the PE.

Take PE1 as an example:

```
PE1#show ip route vrf 1
Codes: C - Connected, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external
```

```
C   10.1.1.0/24 is directly connected, 00:00:23, gigabitethernet0
O   1.1.1.1/32 [110/2] via 10.1.1.1, 00:00:12, gigabitethernet0
```

You can see that there is the route information to CE1 loopback port in the VPN route table of PE1.

Note:

- For the checking method of PE2, refer to PE1.

Step 5: Configure MP-IBGP, and use the loopback interface as the peer address; re-distribute the route with the IGP protocol in the VPN instance.

#On PE1, configure MP-IBGP, and enable the VPNv4 address family; re-distribute the route with the IGP protocol in the VPN instance.

```
PE1(config)#router bgp 100
PE1(config-bgp)#neighbor 33.33.33.33 remote-as 100
PE1(config-bgp)#neighbor 33.33.33.33 update-source loopback0
PE1(config-bgp)#address-family vpnv4
PE1(config-bgp-af)#neighbor 33.33.33.33 activate
PE1(config-bgp-af)#neighbor 33.33.33.33 send-community extended
PE1(config-bgp-af)#exit-address-family
PE1(config-bgp)#address-family ipv4 vrf 1
PE1(config-bgp-af)#redistribute ospf 200
PE1(config-bgp-af)#exit-address-family
PE1(config-bgp)#exit
PE1(config)#router ospf 200 vrf 1
PE1(config-ospf)#redistribute bgp 100
PE1(config-ospf)#exit
```

#On PE2, configure MP-IBGP, and enable the VPNv4 address family; re-distribute the route with the IGP protocol in the VPN instance.

```
PE2(config)#router bgp 100
PE2(config-bgp)#neighbor 11.11.11.11 remote-as 100
PE2(config-bgp)#neighbor 11.11.11.11 update-source loopback0
PE2(config-bgp)#address-family vpnv4
PE2(config-bgp-af)#neighbor 11.11.11.11 activate
PE2(config-bgp-af)#neighbor 11.11.11.11 send-community extended
PE2(config-bgp-af)#exit-address-family
PE2(config-bgp)#address-family ipv4 vrf 1
PE2(config-bgp-af)#redistribute ospf 200
PE2(config-bgp-af)#exit-address-family
```

```
PE2(config-bgp)#exit
PE2(config)#router ospf 200 vrf 1
PE2(config-ospf)#redistribute bgp 100
PE2(config-ospf)#exit
```

#After the configuration is complete, view the BGP neighbor information.

Take PE1 as an example:

```
PE1#show ip bgp vpnv4 all summary
BGP router identifier 11.11.11.11, local AS number 100
BGP table version is 3
1 BGP AS-PATH entries
0 BGP community entries

Neighbor        V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
33.33.33.33     4   100       8       9        3    0    0 00:04:26        2

Total number of neighbors 1
```

The content of the State/PfxRcd list is displayed as number (the number of the route prefixes received from the neighbor), and you can see that PE1 and PE2 set up the BGP neighbor successfully.

#View the BGP VPNv4 route table and VPN1 route table on the PE.

Take PE1 as an example:

```
PE1#show ip bgp vpnv4 vrf 1
BGP table version is 3, local router ID is 11.11.11.11
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network          Next Hop            Metric LocPrf Weight Path
Route Distinguisher: 100:1 (Default for VRF 1)
[0]*> 1.1.1.1/32         10.1.1.1                 2         32768 ?
[B]*>i2.2.2.2/32         33.33.33.33              2    100      0 ?
[0]*> 10.1.1.0/24        0.0.0.0                  1         32768 ?
[B]*>i10.1.4.0/24        33.33.33.33              1    100      0 ?

PE1#show ip route vrf 1
Codes: C - Connected, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external
```

```
C   10.1.1.0/24 is directly connected, 00:20:42, gigabitethernet0
B   10.1.4.0/24 [200/1] via 33.33.33.33, 00:09:33, gigabitethernet1
O   1.1.1.1/32 [110/2] via 10.1.1.1, 00:20:31, gigabitethernet0
B   2.2.2.2/32 [200/2] via 33.33.33.33, 00:08:17, gigabitethernet1
```

You can see that there is the route information to CE2 in the BGP VPNv4 route table and VPN1 route table of PE1..

#View the MPLS forwarding table on the PE.

```
PE1#show mpls forwarding-table
Pro: L - LDP, O - OSPF, B - MP-BGP, R - RSVP, M - Mapped-Route, S - Static Label,ML - mLDP (ML FEC: Root address/OT/OV), RM - RSVP P2MP (RM FEC: P2MP ID/TID)

Pro Ident       FEC             Inlabel Outlabel Outgoing       Next hop
B  1            0.0.0.0/0       24016   /       /               /
```

You can see that there is the route label information of VPN1 in the MPLS forwarding table of the PE.

Note:

- For checking method of PE2, refer to PE1.

Step 6: On the PE and CE, configure the static route to make the VPN member access Internet.

#On CE1, configure the default route to Internet.

```
CE1(config)#ip route 0.0.0.0 0.0.0.0 10.1.1.2
```

#Configure the default route to Internet and the route to CE1 globally on PE1; in the VPN, configure the cross-VPN default route to Internet, and cancel distributing and receiving the label for the 32-bit mask in the MPLS LDP process.

```
PE1(config)#ip route 0.0.0.0 0.0.0.0 10.1.5.2
PE1(config)#ip route vrf global 1.1.1.1 255.255.255.255 10.1.1.1 vrf 1
PE1(config)#ip route vrf global 10.1.1.0 255.255.255.0 10.1.1.1 vrf 1
PE1(config)#ip route vrf 1 0.0.0.0 0.0.0.0 10.1.5.2 vrf global
PE1(config)#router bgp 100
PE1(config-bgp)#address-family ipv4 vrf 1
PE1(config-bgp-af)#redistribute connected
PE1(config-bgp-af)#exit-address-family
PE1(config-bgp)#exit
PE1(config)#mpls ldp
```

```
PE1(config-ldp)#address-family ipv4
PE1(config-ldp-af4)#no advertise-labels for 32bit-mask-fec-only
PE1(config-ldp-af4)#no accept-labels for 32bit-mask-fec-only
PE1(config-ldp-af4)#exit
```

#Configure the default route to Internet and the route to CE2 globally on PE2; in the VPN, configure the cross-VPN default route to Internet, the next hop is the BGP neighbor address of PE2, re-distribute the global static route in the global OSPF, re-distribute the route to the private network to PE1, and cancel distributing and receiving the label for the 32-bit mask in the MPLS LDP process.

```
PE2(config)#ip route vrf global 2.2.2.2 255.255.255.255 10.1.4.2 vrf 1
PE2(config)#ip route vrf global 10.1.4.0 255.255.255.0 10.1.4.2 vrf 1
PE2(config)#ip route vrf 1 0.0.0.0 0.0.0.0 11.11.11.11 vrf global
PE2(config)#router ospf 100
PE2(config-ospf)#redistribute static
PE2(config-ospf)#exit
PE2(config)#mpls ldp
PE2(config-ldp)#address-family ipv4
PE2(config-ldp-af4)#no advertise-labels for 32bit-mask-fec-only
PE2(config-ldp-af4)#no accept-labels for 32bit-mask-fec-only
PE2(config-ldp-af4)#exit
```

#On CE2, configure the default route to Internet.

```
CE2(config)#ip route 0.0.0.0 0.0.0.0 10.1.4.1
```

#On the Internet gateway, configure the default routte.

```
GW#configure terminal
GW(config)#ip route 0.0.0.0 0.0.0.0 10.1.5.1
```

Step7: Check the result.

#After the configuration is complete, view the global route table on the PE.

Take PE1 as an example:

```
PE1#show ip route
Codes: C - Connected, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external



S   0.0.0.0/0 [1/10] via 10.1.5.2, 00:11:42, gigigabitethernet2
S   10.1.1.0/24 [1/10] via 10.1.1.1, 95:27:49, gigigabitethernet0
```

C 10.1.2.0/24 is directly connected, 96:57:55, gigigabitethernet1

O 10.1.3.0/24 [110/2] via 10.1.2.2, 72:44:34, gigigabitethernet1

OE 10.1.4.0/24 [150/20] via 10.1.2.2, 00:13:22, gigigabitethernet1

C 10.1.5.0/24 is directly connected, 96:57:41, gigigabitethernet2

C 127.0.0.0/8 is directly connected, 458:41:50, lo0

S 1.1.1.1/32 [1/10] via 10.1.1.1, 95:27:42, gigigabitethernet0

OE 2.2.2.2/32 [150/20] via 10.1.2.2, 00:13:22, gigigabitethernet1

C 11.11.11.11/32 is directly connected, 96:47:46, loopback0

O 22.22.22.22/32 [110/2] via 10.1.2.2, 72:44:34, gigigabitethernet1

O 33.33.33.33/32 [110/3] via 10.1.2.2, 00:14:28, gigigabitethernet1

PE1#show ip route vrf 1

Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS

U - Per-user Static route

O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external

S 0.0.0.0/0 [1/10] via 10.1.5.2, 95:27:24, gigigabitethernet2

C 10.1.1.0/24 is directly connected, 95:57:28, gigigabitethernet0

B 10.1.4.0/24 [200/0] via 33.33.33.33, 00:14:12, gigigabitethernet1

O 1.1.1.1/32 [110/2] via 10.1.1.1, 95:57:17, gigigabitethernet0

B 2.2.2.2/32 [200/2] via 33.33.33.33, 00:13:44, gigigabitethernet1

You can see that there is one default route to Internet in the global route table and VPN route table of PE1.

Note:

- For the checking method of PE2, refer to PE1.

#On PE2, view the MPLS forwarding table.

PE2#show mpls forwarding-table

Pro: L - LDP, O - OSPF, B - MP-BGP, R - RSVP, M - Mapped-Route, S - Static Label,ML - mLDP (ML FEC: Root address/OT/OV), RM - RSVP P2MP (RM FEC: P2MP ID/TID)

Pro	Ident	FEC	Inlabel	Outlabel	Outgoing	Next hop
B	1	0.0.0.0/0	24016	/	/	/

You can see that PE2 generates one VPN1 MPLS label mapping.

#View the reachability of the device to Internet.

```
CE1#ping 3.3.3.3

Press key (ctrl + shift + 6) interrupt it.
Sending 5, 76-byte ICMP Echos to 3.3.3.3 , timeout is 2 seconds:
!!!!!
Success rate is 100% (5/5). Round-trip min/avg/max = 0/0/0 ms.

CE2#ping 3.3.3.3

Press key (ctrl + shift + 6) interrupt it.
Sending 5, 76-byte ICMP Echos to 3.3.3.3 , timeout is 2 seconds:
!!!!!
Success rate is 100% (5/5). Round-trip min/avg/max = 0/0/0 ms.
```

You can see that CE1 and C2 both can ping Internet route.

3.3.10. Configure Share VPN

Network Requirements

- The whole MPLS network includes three VPNs, VPN1, VPN2, and VPN-share.
- CE1 belongs to the user network of VPN1, CE2 belongs to the user network of VPN2, and the Import Target attribute of any PE connecting the non-share VPN is not the same as the Export Target attribute of the other PE connecting the non-share VPN so that the non-share VPNs cannot communicate with each other.
- CE3 belongs to the user network of the share VPN, the share VPN can accept the routes of all non-share VPN sites, and the routes released by the share-VPN sites also can be received by all non-share VPN sites.
- The share VPN site can communicate with any non-share VPN site; the non-share VPN sites cannot communicate with each other.

Network Topology

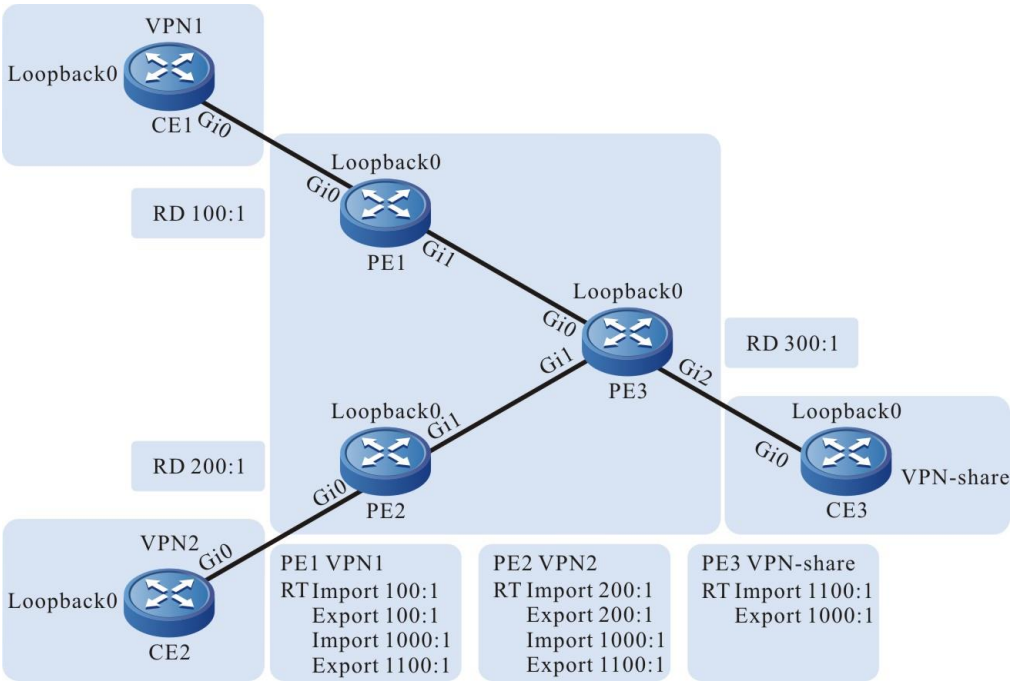

Figure 3-16 Configure the share VPN

Device	Interface	IP Address	Device	Interface	IP Address
CE1	Gi0	10.1.1.1/24	PE2	Gi1	10.1.4.1/24
	Loopback0	1.1.1.1/32		Loopback0	22.22.22.22/32
PE1	Gi0	10.1.1.2/24	PE3	Gi0	10.1.2.2/24
	Gi1	10.1.2.1/24		Gi1	10.1.4.2/24
	Loopback0	11.11.11.11/32		Gi2	10.1.3.1/24
CE2	Gi0	10.1.5.1/24		Loopback0	33.33.33.33/32
	Loopback0	2.2.2.2/32	CE3	Gi0	10.1.3.2/24
PE2	Gi0	10.1.5.2/24		Loopback0	3.3.3.3/32

Configuration Steps

Step 1: Configure the IP address of the interface (omitted).

Step 2: Configure the global OSPF and advertise the global route.

#Configure the global OSPF on PE1.

```
PE1#configure terminal
PE1(config)#router ospf 100
PE1(config-ospf)#network 10.1.2.0 0.0.0.255 area 0
PE1(config-ospf)#network 11.11.11.11 0.0.0.0 area 0
PE1(config-ospf)#exit
```

#Configure the global OSPF on PE2.

```
PE2#configure terminal
PE2(config)#router ospf 100
PE2(config-ospf)#network 10.1.4.0 0.0.0.255 area 0
PE2(config-ospf)#network 22.22.22.22 0.0.0.0 area 0
PE2(config-ospf)#exit
```

#Configure the global OSPF on PE3.

```
PE3#configure terminal
PE3(config)#router ospf 100
PE3(config-ospf)#network 10.1.2.0 0.0.0.255 area 0
PE3(config-ospf)#network 10.1.4.0 0.0.0.255 area 0
PE3(config-ospf)#network 33.33.33.33 0.0.0.0 area 0
PE3(config-ospf)#exit
```

#After the configuration is complete, view the global route table on the device.

Take PE1 as an example:

```
PE1#show ip route
Codes: C - Connected, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external



C   10.1.2.0/24 is directly connected, 04:39:17, gigabitethernet1
O   10.1.4.0/24 [110/2] via 10.1.2.2, 03:46:04, gigabitethernet1
C   127.0.0.0/8 is directly connected, 1579:41:11, lo0
C   11.11.11.11/32 is directly connected, 04:39:05, loopback0
O   22.22.22.22/32 [110/3] via 10.1.2.2, 03:46:04, gigabitethernet1
O   33.33.33.33/32 [110/2] via 10.1.2.2, 03:45:25, gigabitethernet1
```

You can see that there is the route information og PE2 and PE3 loopback ports in the global route table of PE1.

Note:

- For the checking method of PE2, PE3, refer to PE1.

Step 3: Enable MPLS IP and MPLS LDP.

#On PE1, enable the global MPLS IP and MPLS LDP. Meanwhile, enable MPLS IP and MPLS LDP on the interface.

```
PE1(config)#mpls ip
PE1(config)#mpls ldp
PE1(config-ldp)#router-id 11.11.11.11
PE1(config-ldp)#address-family ipv4
PE1(config-ldp-af4)#transport-address 11.11.11.11
PE1(config-ldp-af4)#exit
PE1(config-ldp)#exit
PE1(config)#interface gigabitethernet1
PE1(config-if-gigabitethernet1)#mpls ip
PE1(config-if-gigabitethernet1)#mpls ldp
PE1(config-if-gigabitethernet1)#exit
```

#On PE2, enable the global MPLS IP and MPLS LDP. Meanwhile, enable MPLS IP and MPLS LDP on the interface.

```
PE2(config)#mpls ip
PE2(config)#mpls ldp
PE2(config-ldp)#router-id 22.22.22.22
PE2(config-ldp)#address-family ipv4
PE2(config-ldp-af4)#transport-address 22.22.22.22
PE2(config-ldp-af4)#exit
PE2(config-ldp)#exit
PE2(config)#interface gigabitethernet1
PE2(config-if-gigabitethernet1)#mpls ip
PE2(config-if-gigabitethernet1)#mpls ldp
PE2(config-if-gigabitethernet1)#exit
```

#On PE3, enable the global MPLS IP and MPLS LDP. Meanwhile, enable MPLS IP and MPLS LDP on the interface.

```
PE3(config)#mpls ip
PE3(config)#mpls ldp
PE3(config-ldp)#router-id 33.33.33.33
PE3(config-ldp)#address-family ipv4
PE3(config-ldp-af4)#transport-address 33.33.33.33
PE3(config-ldp-af4)#exit
```

```
PE3(config-ldp)#exit
PE3(config)#interface gigabitethernet0
PE3(config-if-gigabitethernet0)#mpls ip
PE3(config-if-gigabitethernet0)#mpls ldp
PE3(config-if-gigabitethernet0)#exit
PE3(config)#interface gigabitethernet1
PE3(config-if-gigabitethernet1)#mpls ip
PE3(config-if-gigabitethernet1)#mpls ldp
PE3(config-if-gigabitethernet1)#exit
```

#After the configuration is complete, view the LDP session information on the device.

Take PE1 as an example:

```
PE1#show mpls ldp session
Peer IP Address    Peer Type    My Role   State        DS Cap    DeadTime
33.33.33.33        Multicast    Active    OPERATIONAL  Disabled  00:02:48
Statistics for ldp sessions:
    Multicast sessions: 1
    Targeted sessions: 0
```

You can see that PE1 and PE3 set up the LDP session successfully.

#View the route label information on the device.

Take PE1 as an example:

```
PE1#show ip route 22.22.22.22 detail
Codes: C - Connected, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
    U - Per-user Static route
    O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external



O   22.22.22.22/32 [110/2] via 10.1.2.2, label 24017, 00:05:03, gigabitethernet1
                           10.1.2.2 [0], gigabitethernet1

PE1#show ip route 33.33.33.33 detail
Codes: C - Connected, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
    U - Per-user Static route
    O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external
```

```
O   33.33.33.33/32 [110/2] via 10.1.2.2, label 3, 00:05:03, gigabitethernet1
                           10.1.2.2 [0], gigabitethernet1
```

You can see that the loopback port route from PE1 to PE2 and PE3 has the label information.

Note:

- For the checking method of PE2 and PE3, refer to PE1.

Step 4: Configure the VPN instance and advertise the CE route to the PE via OSPF.

#On PE1, configure the VPN instance and OSPF in the VPN instance.

```
PE1(config)#ip vrf 1
PE1(config-vrf)#rd 100:1
PE1(config-vrf)#route-target export 100:1
PE1(config-vrf)#route-target import 100:1
PE1(config-vrf)#route-target export 1100:1
PE1(config-vrf)#route-target import 1000:1
PE1(config-vrf)#exit
PE1(config)#interface gigabitethernet0
PE1(config-if-gigabitethernet0)#ip vrf forwarding 1
PE1(config-if-gigabitethernet0)#ip address 10.1.1.2 255.255.255.0
PE1(config-if-gigabitethernet0)#exit
PE1(config)#router ospf 200 vrf 1
PE1(config-ospf)#network 10.1.1.0 0.0.0.255 area 0
PE1(config-ospf)#exit
```

Note:

- import-target and export-target in the Rt attribute of PE1 is 100:1, which is used to import and export the VPN internal route. export-target is 1100:1, which is used to export the VPN internal route to the share VPN; import-target is 1000:1, which is used to import the route from the share-VPN.

#Configure OSPF on CE1.

```
CE1#configure terminal
CE1(config)#router ospf 100
CE1(config-ospf)#network 1.1.1.1 0.0.0.0 area 0
CE1(config-ospf)#network 10.1.1.0 0.0.0.255 area 0
CE1(config-ospf)#exit
```

#On PE2, configure the VPN instance and OSPF in the VPN instance.

```
PE2(config)#ip vrf 1
PE2(config-vrf)#rd 200:1
PE2(config-vrf)#route-target export 200:1
```

```
PE2(config-vrf)#route-target import 200:1
PE2(config-vrf)#route-target export 1100:1
PE2(config-vrf)#route-target import 1000:1
PE2(config-vrf)#exit
PE2(config)#interface gigabitethernet0
PE2(config-if-gigabitethernet0)#ip vrf forwarding 1
PE2(config-if-gigabitethernet0)#ip address 10.1.5.2 255.255.255.0
PE2(config)#exit
PE2(config)#router ospf 200 vrf 1
PE2(config-ospf)#network 10.1.5.0 0.0.0.255 area 0
PE2(config-ospf)#exit
```

Note:

- import-target and export-target in the Rt attribute of PE2 is 100:1, which is used to import and export the VPN internal route. export-target is 1100:1, which is used to export the VPN internal route to the share VPN; import-target is 1000:1, which is used to import the route from the share-VPN.

#Configure OSPF on CE2.

```
CE2#configure terminal
CE2(config)#router ospf 100
CE2(config-ospf)#network 2.2.2.2 0.0.0.0 area 0
CE2(config-ospf)#network 10.1.5.0 0.0.0.255 area 0
CE2(config-ospf)#exit
```

#On PE3, configure the VPN instance and OSPF in the VPN instance.

```
PE3(config)#ip vrf vpn-share
PE3(config-vrf)#rd 300:1
PE3(config-vrf)#route-target export 1000:1
PE3(config-vrf)#route-target import 1100:1
PE3(config-vrf)#exit
PE3(config)#interface gigabitethernet2
PE3(config-if-gigabitethernet2)#ip vrf forwarding vpn-share
PE3(config-if-gigabitethernet2)#ip address 10.1.3.1 255.255.255.0
PE3(config)#exit
PE3(config)#router ospf 200 vrf vpn-share
PE3(config-ospf)#network 10.1.3.0 0.0.0.255 area 0
PE3(config-ospf)#exit
```

Note:

- export-target in the Rt attribute of PE3 is 1000:1, which is used to export the local VPN route to the other VPN; import-target is 1100:1, which is used to import the route from the other VPN.

#On CE3, configure OSPF.

```
CE2#configure terminal
CE2(config)#router ospf 100
CE2(config-ospf)#network 3.3.3.3 0.0.0.0 area 0
CE2(config-ospf)#network 10.1.3.0 0.0.0.255 area 0
CE2(config-ospf)#exit
```

#After the configuration is complete, view the VPN route table on the PE.

Take PE1 as an example:

```
PE1#show ip route vrf 1
Codes: C - Connected, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
    U - Per-user Static route
    O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external
```

```
C   10.1.1.0/24 is directly connected, 04:19:47, gigabitethernet0
O   1.1.1.1/32 [110/2] via 10.1.1.1, 04:09:32, gigabitethernet0
```

You can see that there is the route information to CE1 loopback port in the VPN route table of PE1.

Note:

- For the checking method of PE2 and PE3, refer to PE1.

Step 5: Configure MP-IBGP, and use the loopback interface as the peer address; re-distribute the route with the IGP protocol in the VPN instance.

#On PE1, configure MP-IBGP, set up the BGP neighbor with PE3, and enable the VPNv4 address family; re-distribute the route with the IGP protocol in the VPN instance.

```
PE1(config)#router bgp 100
PE1(config-bgp)#neighbor 33.33.33.33 remote-as 100
PE1(config-bgp)#neighbor 33.33.33.33 update-source loopback0
PE1(config-bgp)#address-family vpnv4
PE1(config-bgp-af)#neighbor 33.33.33.33 activate
PE1(config-bgp-af)#neighbor 33.33.33.33 send-community extended
PE1(config-bgp-af)#exit-address-family
PE1(config-bgp)#address-family ipv4 vrf 1
PE1(config-bgp-af)#redistribute ospf 200
```

```
PE1(config-bgp-af)#exit-address-family
PE1(config-bgp)#exit
PE1(config)#router ospf 200 vrf 1
PE1(config-ospf)#redistribute bgp 100
PE1(config-ospf)#exit
```

#On PE2, configure MP-IBGP, set up the BGP neighbor with PE3, and enable the VPNv4 address family; re-distribute the route with the IGP protocol in the VPN instance.

```
PE2(config)#router bgp 100
PE2(config-bgp)#neighbor 33.33.33.33 remote-as 100
PE2(config-bgp)#address-family vpnv4
PE2(config-bgp-af)#neighbor 33.33.33.33 activate
PE2(config-bgp-af)#neighbor 33.33.33.33 send-community extended
PE2(config-bgp-af)#exit-address-family
PE2(config-bgp)#address-family ipv4 vrf 1
PE2(config-bgp-af)#redistribute ospf 200
PE2(config-bgp-af)#exit-address-family
PE2(config-bgp)#exit
PE2(config)#router ospf 200 vrf 1
PE2(config-ospf)#redistribute bgp 100
PE2(config-ospf)#exit
```

#On PE3, configure MP-IBGP, set up the BGP neighbor with PE1, PE2, and enable the VPNv4 address family; re-distribute the route with the IGP protocol in the VPN instance.

```
PE3(config)#router bgp 100
PE3(config-bgp)#neighbor 11.11.11.11 remote-as 100
PE3(config-bgp)#neighbor 11.11.11.11 update-source loopback0
PE3(config-bgp)#neighbor 22.22.22.22 remote-as 100
PE3(config-bgp)#neighbor 22.22.22.22 update-source loopback0
PE3(config-bgp)#address-family vpnv4
PE3(config-bgp-af)#neighbor 11.11.11.11 activate
PE3(config-bgp-af)#neighbor 11.11.11.11 send-community extended
PE3(config-bgp-af)#neighbor 22.22.22.22 activate
PE3(config-bgp-af)#neighbor 22.22.22.22 send-community extended
PE3(config-bgp-af)#exit-address-family
PE3(config-bgp)#address-family ipv4 vrf vpn-share
PE3(config-bgp-af)#redistribute ospf 200
PE3(config-bgp-af)#exit-address-family
PE3(config-bgp)#exit
PE3(config)#router ospf 200 vrf vpn-share
```

```
PE3(config-ospf)#redistribute bgp 100
PE3(config-ospf)#exit
```

Step 6: Check the result.

#On the PE, view the BGP neighbor information.

Take PE1 as an example:

```
PE1#show ip bgp vpnv4 all summary
BGP router identifier 11.11.11.11, local AS number 100
BGP table version is 2
1 BGP AS-PATH entries
0 BGP community entries

Neighbor        V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
33.33.33.33     4   100     305     302        2    0    0 04:16:40        2

Total number of neighbors 1
```

The content of the State/PfxRcd list is displayed as number (the number of the route prefixes received from the neighbor), and you can see that PE1 and PE3 set up the BGP neighbor successfully.

#View the BGP VPNv4 route table and VPN route table on the PE.

Take PE1 as an example:

```
PE1#show ip bgp vpnv4 vrf 1
BGP table version is 2, local router ID is 11.11.11.11
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network          Next Hop            Metric LocPrf Weight Path
Route Distinguisher: 100:1 (Default for VRF 1)
[0]*> 1.1.1.1/32         10.1.1.1                 2         32768 ?
[B]*>i3.3.3.3/32         33.33.33.33              2    100      0 ?
[0]*> 10.1.1.0/24        0.0.0.0                  1         32768 ?
[B]*>i10.1.3.0/24        33.33.33.33              1    100      0 ?

PE1#show ip route vrf 1
Codes: C - Connected, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external
```

C 10.1.1.0/24 is directly connected, 04:58:53, gigabitethernet0

B 10.1.3.0/24 [200/1] via 33.33.33.33, 04:46:00, gigabitethernet1

O 1.1.1.1/32 [110/2] via 10.1.1.1, 04:48:39, gigabitethernet0

B 3.3.3.3/32 [200/2] via 33.33.33.33, 04:46:00, gigabitethernet1

You can see that there is the route information to CE3 in the BGP VPNv4 route table and VPN1 route table of PE1.

#View the MPLS forwarding table on the PE.

Take PE1 as an example:

PE1#show mpls forwarding-table

Pro: L - LDP, O - OSPF, B - MP-BGP, R - RSVP, M - Mapped-Route, S - Static Label,ML - mLDP (ML FEC: Root address/OT/OV), RM - RSVP P2MP (RM FEC: P2MP ID/TID)

Pro	Ident	FEC	Inlabel	Outlabel	Outgoing	Next hop
B	1	0.0.0.0/0	25120	/	/	/

You can see that there is the route label information of VPN1 in the MPLS forwarding table of PE1.

Note:

- For the checking method of PE2 and PE3, refer to PE1.

#On CE3, ping the loopback ports of CE1 and CE2.

CE3#ping 1.1.1.1

Press key (ctrl + shift + 6) interrupt it.

Sending 5, 76-byte ICMP Echos to 1.1.1.1 , timeout is 2 seconds:

!!!!!

Success rate is 100% (5/5). Round-trip min/avg/max = 0/3/16 ms.

CE3#ping 2.2.2.2

Press key (ctrl + shift + 6) interrupt it.

Sending 5, 76-byte ICMP Echos to 2.2.2.2 , timeout is 2 seconds:

!!!!!

Success rate is 100% (5/5). Round-trip min/avg/max = 0/0/0 ms.

You can see that CE3 can ping the loopback ports of CE1 and CE2.

#On CE1, ping the loopback ports of CE2.

```
CE1#ping 2.2.2.2


Press key (ctrl + shift + 6) interrupt it.
Sending 5, 76-byte ICMP Echos to 2.2.2.2 , timeout is 2 seconds:
.....
Success rate is 0% (0/5).
```

You can see that CE1 cannot ping the loopback port of CE2.

3.3.11. Configure MPLS L3VPN over GRE

Network Requirements

- PE1, P, and PE2 run the OSPF protocol to realize the network interconnection.
- CE1 and CE2 belong VPN1; CE and PE use EBGP to advertise the route.
- PE1 and PE2 set up the GRE tunnel; PEs set up the MP-IBGP neighbor via the GRE tunnel and advertise the VPN route.
- CE1 and CE2 communicate with each other via the GRE tunnel between PEs.

Network Topology

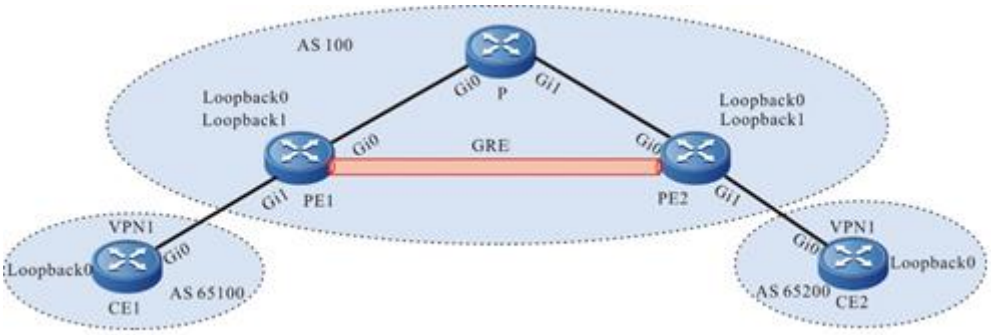

Figure 3-17 Configure MPLS L3VPN over GRE

Device	Interface	IP Address	Device	Interface	IP Address
CE1	Gi0	10.0.0.1/24	P	Gi1	2.1.1.1/24
	Loopback0	10.100.0.1/32	PE2	Gi0	2.1.1.2/24
PE1	Gi0	1.1.1.1/24		Gi1	10.2.1.1/24
	Gi1	10.0.0.2/24		Loopback0	22.22.22.22/32
	Loopback0	11.11.11.11/32		Loopback1	23.23.23.23/32
PE1	Loopback1	12.12.12.12/32	CE2	Gi0	10.2.1.2/24

Device	Interface	IP Address	Device	Interface	IP Address
P	Gi0	1.1.1.2/24		Loopback0	10.101.1.1/32

Step 1: Configure the IP address of the interface (omitted).

Step 2: Configure the global OSPF and advertise the global route.

#Configure the global OSPF on PE1.

```
PE1#configure terminal
PE1(config)#router ospf 100
PE1(config-ospf)#network 11.11.11.11 0.0.0.0 area 0
PE1(config-ospf)#network 1.1.1.0 0.0.0.255 area 0
PE1(config-ospf)#exit
```

#Configure the global OSPF on P.

```
P#configure terminal
P(config)#router ospf 100
P(config-ospf)#network 1.1.1.0 0.0.0.255 area 0
P(config-ospf)#network 2.1.1.0 0.0.0.255 area 0
P(config-ospf)#exit
```

#Configure the global OSPF on PE2.

```
PE2#configure terminal
PE2(config)#router ospf 100
PE2(config-ospf)#network 22.22.22.22 0.0.0.0 area 0
PE2(config-ospf)#network 2.1.1.0 0.0.0.255 area 0
PE2(config-ospf)#exit
```

#After the configuration is complete, view the global route table on the device.

Take PE1 as an example:

```
PE1#show ip route
Codes: C - Connected, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external



C   1.1.1.0/24 is directly connected, 01:44:04, gigabitethernet0
O   2.1.1.0/24 [110/2] via 1.1.1.2, 01:41:51, gigabitethernet0
C   127.0.0.0/8 is directly connected, 01:47:01, lo0
C   11.11.11.11/32 is directly connected, 01:46:21, loopback0
```

```
C   12.12.12.12/32 is directly connected, 01:46:21, loopback1
O   22.22.22.22/32 [110/3] via 1.1.1.2, 01:41:15, gigabitethernet0
```

You can see that there is the route information of PE2 Loopback0 in the global VPN route table of PE1.

Note:

- For the checking method of P and PE2, refer to PE1.

Step 3: On PE1 and PE2, configure the GRE tunnel.

#On PE1, configure the GRE tunnel tunnel1.

```
PE1(config)#interface tunnel1
PE1(config-if-tunnel1)#tunnel source 11.11.11.11
PE1(config-if-tunnel1)#tunnel destination 22.22.22.22
PE1(config-if-tunnel1)#ip address 192.0.1.1 255.255.255.0
PE1(config-if-tunnel1)#exit
```

#On PE2, configure the GRE tunnel tunnel1.

```
PE2(config)#interface tunnel1
PE2(config-if-tunnel1)#tunnel source 22.22.22.22
PE2(config-if-tunnel1)#tunnel destination 11.11.11.11
PE2(config-if-tunnel1)#ip address 192.0.1.2 255.255.255.0
PE2(config-if-tunnel1)#exit
```

#After the configuration is complete, view the GRE tunnel status on the device.

Take PE1 as an example:

```
PE1#show interface tunnel 1
tunnel1:
    line protocol is up
    Flags: (0xc1080f1) POINT-TO-POINT MULTICAST RUNNING
    Type: TUNNEL
    Internet address: 192.0.1.1/24
    Metric: 0, MTU: 1476, BW: 100 Kbps, DLY: 500000 usec, VRF: global
    Reliability 255/255, Txload 1/255, Rxload 1/255
    Last clearing of "show interface" counters is 0 hour 0 minute 27 seconds ago
    input peak rate 177 bits/sec,  0 hour 0 minute 14 seconds ago
    output peak rate 177 bits/sec,  0 hour 0 minute 14 seconds ago
    20 seconds input rate 149 bits/sec, 0 packet/sec, bandwidth utilization -
    20 seconds output rate 149 bits/sec, 0 packet/sec, bandwidth utilization -
    9 packets received; 10 packets sent
    507 bytes received; 569 bytes sent
    5 multicast packets received
```

```
6 multicast packets sent
0 input errors; 0 output errors
0 collisions; 0 dropped
```

You can see that the status of PE1 tunnel 1 is up.

Note:

- For the checking method of PE2, refer to PE1.

Step 4: Configure the static route, making Loopback1 of PE1 and PE2 intercommunicate with each other.

#On PE1, configure the static route to Loopback1 of PE2, and the gateway is the IP address of PE2 tunnel1.

```
PE1(config)#ip route 23.23.23.23 255.255.255.255 192.0.1.2
```

#On PE2, configure the static route to PE1 Loopback1, and the gateway is the IP address of PE1 tunnel1.

```
PE2(config)#ip route 12.12.12.12 255.255.255.255 192.0.1.1
```

#After the configuration is complete, view the route information on the device.

Take PE1 as an example.

```
PE1#show ip route
Codes: C - Connected, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
    U - Per-user Static route
    O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external

C   1.1.1.0/24 is directly connected, 02:25:43, gigabitethernet0
O   2.1.1.0/24 [110/2] via 1.1.1.2, 02:23:30, gigabitethernet0
C   127.0.0.0/8 is directly connected, 02:28:40, lo0
C   192.0.1.0/24 is directly connected, 02:22:54, tunnel1
C   11.11.11.11/32 is directly connected, 02:28:00, loopback0
C   12.12.12.12/32 is directly connected, 02:28:00, loopback1
O   22.22.22.22/32 [110/3] via 1.1.1.2, 02:22:54, gigabitethernet0
S   23.23.23.23/32 [1/100000] via 192.0.1.2, 02:22:54, tunnel1
```

You can see that there is the route information of PE2 Loopback1 in the global route table of PE1 and the egress interface is tunnel1.

Note:

- For the checking method of PE2, refer to PE1.

Step 5: PE1 and PE2 enable MPLS IP and MPLS LDP.

#On PE1, enable the global MPLS IP and MPLS LDP, and enable MPLS IP and MPLS LDP of the tunnel1 interface.

```
PE1(config)#mpls ip
PE1(config)#mpls ldp
PE1(config-ldp)#router-id 12.12.12.12
PE1(config-ldp)#address-family ipv4
PE1(config-ldp-af4)#transport-address 12.12.12.12
PE1(config-ldp-af4)#exit
PE1(config-ldp)#exit
PE1(config)#interface tunnel1
PE1(config-if-tunnel1)#mpls ip
PE1(config-if-tunnel1)#mpls ldp
PE1(config-if-tunnel1)#exit
```

#On PE2, enable the global MPLS IP and MPLS LDP, and enable MPLS IP and MPLS LDP of the tunnel1 interface.

```
PE2(config)#mpls ip
PE2(config)#mpls ldp
PE2(config-ldp)#router-id 23.23.23.23
PE2(config-ldp)#address-family ipv4
PE2(config-ldp-af4)#transport-address 23.23.23.23
PE2(config-ldp-af4)#exit
PE2(config-ldp)#exit
PE2(config)#interface tunnel1
PE2(config-if-tunnel1)#mpls ip
PE2(config-if-tunnel1)#mpls ldp
PE2(config-if-tunnel1)#exit
```

#After the configuration is complete, view the LDP session information on the device.

Take PE1 as an example:

```
PE1#show mpls ldp session
Peer IP Address   Peer Type    My Role  State        DS Cap   DeadTime
23.23.23.23       Multicast    Passive  OPERATIONAL  Disabled 00:02:07
Statistics for ldp sessions:
    Multicast sessions: 1
    Targeted sessions: 0
```

You can see that PE1 and PE2 set up the LDP session successfully.

#On the device, view the MPLS forwarding table.

Take PE1 as an example:

```
PE1#show ip route 23.23.23.23 detail
Codes: C - Connected, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external



O   23.23.23.23/32 [110/2] via 1.1.1.2, label 3, 00:45:23, tunnel1
                           1.1.1.2 [0], tunnel1
```

You can see that the loopback port route from PE1 to PE2 has the label information.

Note:

- For the checking method of PE2, refer to PE1.

Step 6: On the PE, configure the VPN instance and configure the BGP between PE and CE.

#On PE1, configure the VPN instance and set up the EBGP neighbor with the CE.

```
PE1(config)#ip vrf 1
PE1(config-vrf)#rd 100:1
PE1(config-vrf)#route-target export 100:1
PE1(config-vrf)#route-target import 100:1
PE1(config-vrf)#exit
PE1(config)#interface gigabitethernet1
PE1(config-if-gigabitethernet1)#ip vrf forwarding 1
PE1(config-if-gigabitethernet1)#ip address 10.0.0.2 255.255.255.0
PE1(config-if-gigabitethernet1)#exit
PE1(config)#router bgp 100
PE1(config-bgp)#address-family ipv4 vrf 1
PE1(config-bgp-af)#neighbor 10.0.0.1 remote-as 65100
PE1(config-bgp-af)#redistribute connected
PE1(config-bgp-af)#exit-address-family
PE1(config-bgp)#exit
```

#On CE1, configure the EBGP with the PE.

```
CE1#configure terminal
CE1(config)#router bgp 65100
CE1(config-bgp)#network 10.100.0.1 255.255.255.255
CE1(config-bgp)#network 10.0.0.0 255.255.255.0
CE1(config-bgp)#neighbor 10.0.0.2 remote-as 65100
CE1(config-bgp)#exit
```

#On PE2, configure the VPN instance and set up the EBGP neighbor with the CE.

```
PE2(config)#ip vrf 1
PE2(config-vrf)#rd 100:1
PE2(config-vrf)#route-target export 100:1
PE2(config-vrf)#route-target import 100:1
PE2(config-vrf)#exit
PE2(config)#interface gigabitethernet1
PE2(config-if-gigabitethernet1)#ip vrf forwarding 1
PE2(config-if-gigabitethernet1)#ip address 10.2.1.1 255.255.255.0
PE2(config-if-gigabitethernet1)#exit
PE2(config)#router bgp 100
PE2(config-bgp)#address-family ipv4 vrf 1
PE2(config-bgp-af)#neighbor 10.2.1.2 remote-as 65200
PE2(config-bgp-af)#redistribute connected
PE2(config-bgp-af)#exit-address-family
PE2(config-bgp)#exit
```

#On CE2, configure the EBGP with the PE.

```
CE2#configure terminal
CE2(config)#router bgp 65200
CE2(config-bgp)#network 10.101.1.1 255.255.255.255
CE2(config-bgp)#network 10.2.1.0 255.255.255.0
CE2(config-bgp)#neighbor 10.2.1.1 remote-as 100
CE2(config-bgp)#exit
```

#After the configuration is complete, view the EBGP neighbor information on the PE.

Take PE1 as an example:

```
PE1#show ip bgp vpnv4 all summary
BGP router identifier 12.12.12.12, local AS number 100BGP VRF 1 Route Distinguisher:
100:1
BGP table version is 1
3 BGP AS-PATH entries
0 BGP community entries

Neighbor        V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
10.0.0.1        4 65100     237     239        1    0    0 03:20:31        2

Total number of neighbors 1
```

The content of the State/PfxRcd list is displayed as numbers (the number of the route prefixed received from the neighbor), indicating that PE1 and CE1 set up the BGP neighbor successfully.

#On the PE, view the BGP VPNv4 route table and VPN route table.

```
PE1#show ip bgp vpnv4 vrf 1
BGP table version is 6, local router ID is 12.12.12.12
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network          Next Hop          Metric     LocPrf Weight Path
Route Distinguisher: 100:1 (Default for VRF 1)
[B]*  10.0.0.0/24        10.0.0.1               0             0 65100 i
[C]*>                    0.0.0.0                0         32768 ?
[B]*> 10.100.0.1/32      10.0.0.1               0             0 65100 i

PE1#show ip route vrf 1
Codes: C - Connected, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external



C   10.0.0.0/24 is directly connected, 02:47:51, gigabitethernet1
B   10.100.0.1/32 [20/0] via 10.0.0.1, 00:08:44, gigabitethernet1
```

You can see that there is the route to CE1 in the BGP route table and VPN route table of PE1.

Note:

- For the checking method of PE2, refer to PE1.

Step 7: Configure MP-IBGP, using the loopback interface as the peer address.

#On PE1, configure MP-IBGP and enable the VPNv4 address family.

```
PE1(config)#router bgp 100
PE1(config-bgp)#neighbor 23.23.23.23 remote-as 100
PE1(config-bgp)#neighbor 23.23.23.23 update-source loopback1
PE1(config-bgp)#address-family vpnv4
PE1(config-bgp-af)#neighbor 23.23.23.23 activate
PE1(config-bgp-af)#neighbor 23.23.23.23 send-community extended
PE1(config-bgp-af)#exit-address-family
PE1(config-bgp)#exit
```

#On PE2, configure MP-IBGP and enable the VPNv4 address family.

```
PE2(config)#router bgp 100
PE2(config-bgp)#neighbor 12.12.12.12 remote-as 100
PE2(config-bgp)#neighbor 12.12.12.12 update-source loopback1
PE2(config-bgp)#address-family vpnv4
PE2(config-bgp-af)#neighbor 12.12.12.12 activate
PE2(config-bgp-af)#neighbor 12.12.12.12 send-community extended
PE2(config-bgp-af)#exit-address-family
PE2(config-bgp)#exit
```

Step 8: Check the result.

#After the configuration is complete, view the BGP neighbor information on the PE.

Take PE1 as an example:

```
PE1#show ip bgp vpnv4 all summary
BGP router identifier 12.12.12.12, local AS number 100
BGP table version is 7
3 BGP AS-PATH entries
0 BGP community entries

Neighbor        V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
23.23.23.23     4   100       7       7        7    0    0 00:02:44        2

Total number of neighbors 1
BGP VRF 1 Route Distinguisher:
100:1
BGP table version is 1
3 BGP AS-PATH entries
0 BGP community entries

Neighbor        V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
10.0.0.1        4 65100     205     206        1    0    0 02:52:30        2

Total number of neighbors 1
```

The content of the State/PfxRcd list is displayed as numbers (the number of the route prefixed received from the neighbor), indicating that PE1 and PE2, CE1 set up the BGP neighbor successfully.

#On the PE, view the BGP VPNv4 route table and VPN route table.

Take PE1 as an example:

```
PE1#show ip bgp vpnv4 vrf 1
```

```
BGP table version is 7, local router ID is 12.12.12.12
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network          Next Hop            Metric     LocPrf Weight Path
Route Distinguisher: 100:1 (Default for VRF 1)
[B]*  10.0.0.0/24        10.0.0.1                 0             0 65100 i
[C]*>                    0.0.0.0                  0         32768 ?
[B]*>i10.2.1.0/24        23.23.23.23              0       100      0 ?
[B]*> 10.100.0.1/32      10.0.0.1                 0             0 65100 i
[B]*>i10.101.1.1/32      23.23.23.23              0       100      0 65200 i

PE1#show ip route vrf 1
Codes: C - Connected, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external



C   10.0.0.0/24 is directly connected, 02:57:18, gigabitethernet1
B   10.2.1.0/24 [200/0] via 23.23.23.23, 00:05:56, tunnel1
B   10.100.0.1/32 [20/0] via 10.0.0.1, 00:18:10, gigabitethernet1
B   10.101.1.1/32 [200/0] via 23.23.23.23, 00:05:56, tunnel1
```

You can see that there is the route information of CE2 in the BGP VPNv4 route table of PE1 and there is the route information of CE2 in the VPN1 route table of PE1.

#View the MPLS forwarding table on the device.

Take PE1 as an example:

```
PE1#show mpls forwarding-table
Pro: L - LDP, O - OSPF, B - MP-BGP, R - RSVP, M - Mapped-Route, S - Static
Label,ML - mLDP (ML FEC: Root address/OT/OV), RM - RSVP P2MP (RM FEC: P2MP
ID/TID)


Pro Ident       FEC             Inlabel Outlabel Outgoing          Next hop
B   1           0.0.0.0/0       24016   /        /                 /
```

You can see that there is the route label information of CE2 in the MPLS forwarding table of PE1.

Note:

- For the checking method of PE2, refer to PE1.

#View the route table on the CE.

Take CE1 as an example:

```
CE1#show ip route
Codes: C - Connected, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
    U - Per-user Static route
    O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external



C   10.0.0.0/24 is directly connected, 02:59:39, gigabitethernet0
B   10.2.1.0/24 [20/0] via 10.0.0.2, 00:08:15, gigabitethernet0
C   127.0.0.0/8 is directly connected, 1w5d:05:23:35, lo0
C   10.100.0.1/32 is directly connected, 03:41:32, loopback0
B   10.101.1.1/32 [20/0] via 10.0.0.2, 00:08:15, gigabitethernet0
```

You can see that there is the route information of CE2 in the route table of CE1.

On CE1, ping Loopback0 of CE2, and view whether the ping can be connected.

```
CE1#ping 10.101.1.1



Press key (ctrl + shift + 6) interrupt it.
Sending 5, 76-byte ICMP Echos to 10.101.1.1 , timeout is 2 seconds:
!!!!!
Success rate is 100% (5/5). Round-trip min/avg/max = 1/1/2 ms.
```

You can see that CE1 can ping Loopback0 of CE2.

3.3.12. Configure VPNv4 Route to Back up VPNv4 Route

Network Requirements

- In the whole MPLS network, there is only one AS domain. PE1 in AS 100 sets up the MP-IBGP neighbor with PE2, PE3 respectively to interact the route.
- PE1 sets up the EBGP neighbor with CE1 to interact the route.
- PE2, PE3 set up the EBGP neighbor with CE2 respectively to interact the route.
- The master path is CE1->PE1->PE2->CE2, and the standby path is CE1->PE1->PE3->CE2.
- Detect the connectivity of the master path via MPLS OAM BFD. When the master path fails, switch the standby path for forwarding.

Network Topology

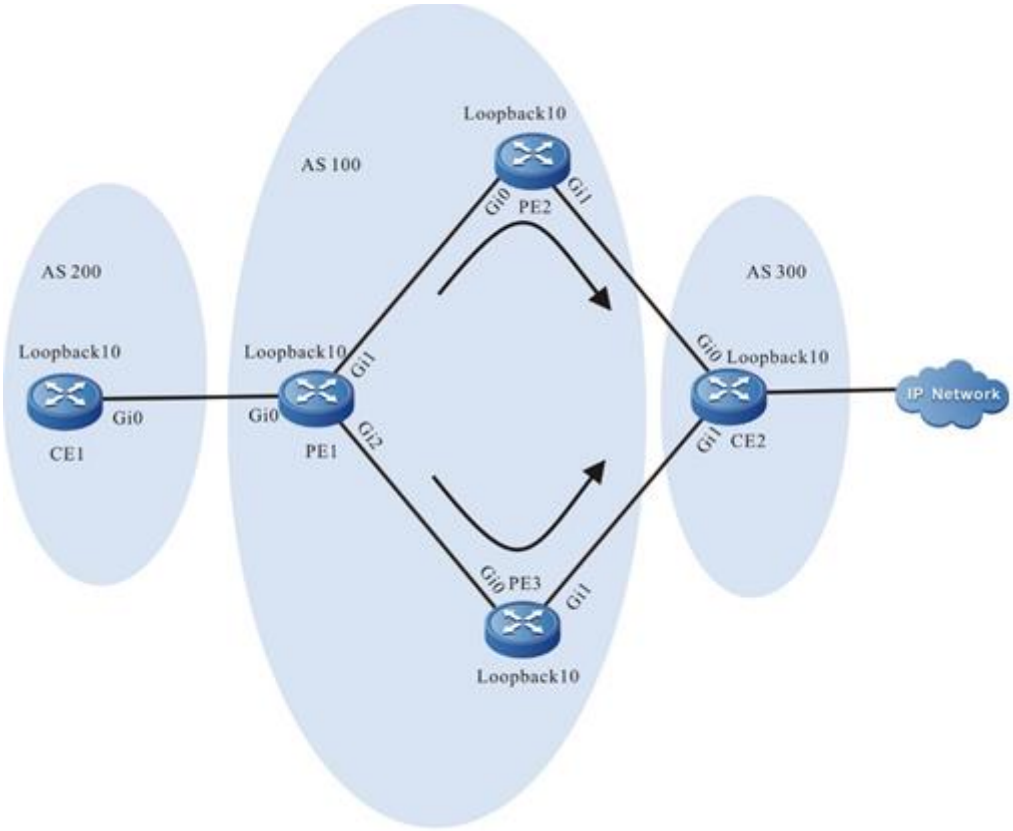

Figure 3-18 Configure VPNv4 route to back up VPNv4 route

Device	Interface	IP Address	Device	Interface	IP Address
CE1	Gi0	5.1.1.2/24		Loopback10	10.2.2.2/32
	Loopback10	110.1.1.1/32	PE3	Gi0	2.1.1.2/24
PE1	Gi0	5.1.1.1/24		Gi1	6.1.1.1/24
	Gi1	1.1.1.1/24		Loopback10	10.3.3.3/32
	Gi2	2.1.1.1/32	CE2	Gi0	4.1.1.2/24
	Loopback10	10.1.1.1/32		Gi1	6.1.1.2/24
PE2	Gi0	1.1.1.2/24		Loopback10	120.1.1.1/32
	Gi1	4.1.1.1/24			

Configuration Steps

Step 1: Configure the IP address of the interface (omitted).

Step 2: Configure the global OSPF and advertise the global route.

#Configure the global OSPF on PE1.

```
PE1#configure terminal
PE1(config)#router ospf 10
PE1(config-ospf)#network 1.1.1.0 0.0.0.255 area 0
PE1(config-ospf)#network 2.1.1.0 0.0.0.255 area 0
PE1(config-ospf)#network 10.1.1.1 0.0.0.0 area 0
PE1(config-ospf)#exit
```

#Configure the global OSPF on PE2.

```
PE2#configure terminal
PE2(config)#router ospf 10
PE2(config-ospf)#network 1.1.1.0 0.0.0.255 area 0
PE2(config-ospf)#network 10.2.2.2 0.0.0.0 area 0
PE2(config-ospf)#exit
```

#Configure the global OSPF on PE3.

```
PE3#configure terminal
PE3(config)#router ospf 10
PE3(config-ospf)#network 2.1.1.0 0.0.0.255 area 0
PE3(config-ospf)#network 10.3.3.3 0.0.0.0 area 0
PE3(config-ospf)#exit
```

#After the configuration is complete, view the global route table on the device.

Take PE1 as an example:

```
PE1#show ip route
Codes: C - Connected, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external



C   1.1.1.0/24 is directly connected, 00:41:40, gigabitethernet1
L   1.1.1.1/32 is directly connected, 00:41:40, gigabitethernet1
C   2.1.1.0/24 is directly connected, 00:42:06, gigabitethernet2
L   2.1.1.1/32 is directly connected, 00:42:06, gigabitethernet2
```

```
LC  10.1.1.1/32 is directly connected, 00:44:25, loopback10
O   10.2.2.2/32 [110/2] via 1.1.1.2, 00:40:55, gigabitethernet1
O   10.3.3.3/32 [110/2] via 2.1.1.2, 00:41:15, gigabitethernet2
```

You can see that there is the route information of PE2 and PE3 loopback ports in the global route table of PE1.

Note:

- For the checking method of PE2 and PE3, refer to PE1.

Step 3: Enable MPLS IP and MPLS LDP.

#On PE1, enable the global MPLS IP and MPLS LDP, and meanwhile, enable MPLS IP and MPLS LDP on the interface.

```
PE1(config)#mpls ip
PE1(config)#mpls ldp
PE1(config-ldp)#router-id 10.1.1.1
PE1(config-ldp)#address-family ipv4
PE1(config-ldp-af4)#transport-address 10.1.1.1
PE1(config-ldp-af4)#exit
PE1(config-ldp)#exit
PE1(config)#interface gigabitethernet1
PE1(config-if-gigabitethernet1)#mpls ip
PE1(config-if-gigabitethernet1)#mpls ldp
PE1(config-if-gigabitethernet1)#exit
PE1(config)#interface gigabitethernet2
PE1(config-if-gigabitethernet2)#mpls ip
PE1(config-if-gigabitethernet2)#mpls ldp
PE1(config-if-gigabitethernet2)#exit
```

#On PE2, enable the global MPLS IP and MPLS LDP, and meanwhile, enable MPLS IP and MPLS LDP on the interface.

```
PE2(config)#mpls ip
PE2(config)#mpls ldp
PE2(config-ldp)#router-id 10.2.2.2
PE2(config-ldp)#address-family ipv4
PE2(config-ldp-af4)#transport-address 10.2.2.2
PE2(config-ldp-af4)#exit
PE2(config-ldp)#exit
PE2(config)#interface gigabitethernet0
PE2(config-if-gigabitethernet0)#mpls ip
PE2(config-if-gigabitethernet0)#mpls ldp
```

```
PE2(config-if-gigabitethernet0)#exit
```

#On PE3, enable the global MPLS IP and MPLS LDP, and meanwhile, enable MPLS IP and MPLS LDP on the interface.

```
PE3(config)#mpls ip
PE3(config)#mpls ldp
PE3(config-ldp)#router-id 10.3.3.3
PE3(config-ldp)#address-family ipv4
PE3(config-ldp-af4)#transport-address 10.3.3.3
PE3(config-ldp-af4)#exit
PE3(config-ldp)#exit
PE3(config)#interface gigabitethernet0
PE3(config-if-gigabitethernet0)#mpls ip
PE3(config-if-gigabitethernet0)#mpls ldp
PE3(config-if-gigabitethernet0)#exit
```

#After configuration, query the LDP session information on the device.

Take PE1 as an example :

```
PE1#show mpls ldp session
Peer IP Address    Peer Type    My Role   State        DS Cap    DeadTime
10.3.3.3           Multicast    Passive   OPERATIONAL  Disabled  00:02:34
10.2.2.2           Multicast    Passive   OPERATIONAL  Disabled  00:02:09

Statistics for ldp sessions:
    Multicast sessions: 2
    Targeted sessions: 0
```

You can see that PE1 sets up the LDP session with PE2, PE3 successfully.

#Query the MPLS forwarding table on the device.

Take PE1 as an example :

```
PE1#show mpls forwarding-table
Pro: L - LDP, O - OSPF, B - MP-BGP, R - RSVP, M - Mapped-Route, S - Static
Label,ML - mLDP (ML FEC: Root address/OT/OV), RM - RSVP P2MP (RM FEC: P2MP
ID/TID)

Pro Ident       FEC             Inlabel Outlabel Outgoing          Next hop
L   global      10.2.2.2/32     24017   3        gigabitethernet1  1.1.1.2
L   global      10.3.3.3/32     24016   3        gigabitethernet2  2.1.1.2
```

You can see that there is the information about the label to the loopback port of PE2 and PE3 on PE1.

Note:

- For the checking method of PE2 and PE3, refer to PE1

Step 4: Configure the VPN instance and advertise the CE route to PE via EBGP.

#On PE1, configure the VPN instance and the EBGP neighbor in the VPN instance.

```
PE1(config)#ip vrf 1
PE1(config-vrf)#rd 1:1
PE1(config-vrf)#route-target export 1:1
PE1(config-vrf)#route-target import 1:1
PE1(config-vrf)#exit
PE1(config)#interface gigabitethernet0
PE1(config-if-gigabitethernet0)#ip vrf forwarding 1
PE1(config-if-gigabitethernet0)#ip address 5.1.1.1 255.255.255.0
PE1(config-if-gigabitethernet0)#exit
PE1(config)#router bgp 100
PE1(config-bgp)#address-family ipv4 vrf 1
PE1(config-bgp-af)#neighbor 5.1.1.2 remote-as 200
PE1(config-bgp-af)# exit-address-family
PE1(config-bgp)#exit
```

#On CE1, configure EBGP.

```
CE1#configure terminal
CE1(config)#router bgp 200
CE1(config-bgp)#neighbor 5.1.1.1 remote-as 100
CE1(config-bgp)#netwrok 110.1.1.1 255.255.255.255
CE1(config-bgp)#exit
```

#On PE2, configure the VPN instance and the EBGP neighbor in the VPN instance.

```
PE2(config)#ip vrf 1
PE2(config-vrf)#rd 1:1
PE2(config-vrf)#route-target export 1:1
PE2(config-vrf)#route-target import 1:1
PE2(config-vrf)#exit
PE2(config)#interface gigabitethernet1
PE2(config-if-gigabitethernet1)#ip vrf forwarding 1
PE2(config-if-gigabitethernet1)#ip address 4.1.1.1 255.255.255.0
PE2(config-if-gigabitethernet1)#exit
```

```
PE2(config)#router bgp 100
PE2(config-bgp)#address-family ipv4 vrf 1
PE2(config-bgp-af)#neighbor 4.1.1.2 remote-as 300
PE2(config-bgp-af)# exit-address-family
PE2(config-bgp)#exit
```

#On PE3, configure the VPN instance and the EBGP neighbor in the VPN instance.

```
PE3(config)#ip vrf 1
PE3(config-vrf)#rd 1:1
PE3(config-vrf)#route-target export 1:1
PE3(config-vrf)#route-target import 1:1
PE3(config-vrf)#exit
PE3(config)#interface gigabitethernet1
PE3(config-if-gigabitethernet1)#ip vrf forwarding 1
PE3(config-if-gigabitethernet1)#ip address 6.1.1.1 255.255.255.0
PE3(config-if-gigabitethernet1)#exit
PE3(config)#router bgp 100
PE3(config-bgp)#address-family ipv4 vrf 1
PE3(config-bgp-af)#neighbor 6.1.1.2 remote-as 300
PE3(config-bgp-af)# exit-address-family
PE3(config-bgp)#exit
```

#On CE2, configure EBGP.

```
CE2#configure terminal
CE2(config)#router bgp 300
CE2(config-bgp)#neighbor 4.1.1.1 remote-as 100
CE2(config-bgp)#neighbor 6.1.1.1 remote-as 100
CE2(config-bgp)#network 120.1.1.1 255.255.255.255
CE2(config-bgp)#exit
```

#After configuration, query the VPN route table on the PE.

Take PE1 as an example :

```
PE1#show  ip route  vrf 1
Codes: C - Connected, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external
```

```
C   5.1.1.0/24 is directly connected, 01:09:37, gigabitethernet0
L   5.1.1.1/32 is directly connected, 01:09:37, gigabitethernet0
B   110.1.1.1/32 [20/0] via 5.1.1.2, 00:00:51, gigabitethernet0
B   120.1.1.1/32 [200/0] via 10.3.3.3, 00:00:04, gigabitethernet2
```

You can see that there is the information about the route to CE1 in the VPN1 route table of PE1.

Note:

- For the checking method of PE2 and PE3, refer to PE1.

Step 5: Configure MP-IBGP between PE1 and PE2, PE3, and use the loopback interface as the peer address.

#On PE1, configure MP-IBGP with PE2, PE3, and enable the VPNv4 address family.

```
PE1(config)#router bgp 100
PE1(config-bgp)#neighbor 10.3.3.3 remote-as 100
PE1(config-bgp)#neighbor 10.3.3.3 update-source loopback10
PE1(config-bgp)#neighbor 10.2.2.2 remote-as 100
PE1(config-bgp)#neighbor 10.2.2.2 update-source loopback10
PE1(config-bgp)#address-family vpnv4
PE1(config-bgp-af)#neighbor 10.3.3.3 activate
PE1(config-bgp-af)#neighbor 10.3.3.3 send-community extended
PE1(config-bgp-af)#neighbor 10.2.2.2 activate
PE1(config-bgp-af)#neighbor 10.2.2.2 send-community extended
PE1(config-bgp-af)#exit-address-family
PE1(config-bgp)#exit
```

#On PE2, configure MP-IBGP with PE1, and enable the VPNv4 address family.

```
PE2(config)#router bgp 100
PE2(config-bgp)#neighbor 10.1.1.1 remote-as 100
PE2(config-bgp)#neighbor 10.1.1.1 update-source loopback10
PE2(config-bgp)#address-family vpnv4
PE2(config-bgp-af)#neighbor 10.1.1.1 activate
PE2(config-bgp-af)#neighbor 10.1.1.1 send-community extended
PE2(config-bgp-af)#exit-address-family
PE2(config-bgp)#exit#
```

#On PE3, configure MP-IBGP with PE1, and enable the VPNv4 address family.

```
PE3(config)#router bgp 100
PE3(config-bgp)#neighbor 10.1.1.1 remote-as 100
PE3(config-bgp)#neighbor 10.1.1.1 update-source loopback10
PE3(config-bgp)#address-family vpnv4
```

```
PE3(config-bgp-af)#neighbor 10.1.1.1 activate
PE3(config-bgp-af)#neighbor 10.1.1.1 send-community extended
PE3(config-bgp-af)#exit-address-family
PE3(config-bgp)#exit
```

#After configuration, query the VPN route table of BGP on PE.

Take PE1 as an example:

```
PE1#show ip bgp vpnv4 all
BGP table version is 19, local router ID is 10.1.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network          Next Hop          Metric     LocPrf Weight Path
Route Distinguisher: 1:1 (Default for VRF 1)
[B]*> 110.1.1.1/32       5.1.1.2                              0 200 i
[B]*>i120.1.1.1/32       10.2.2.2              0       100      0 300 200 i
[B]* i                   10.3.3.3              0       100      0 300 200 i
```

You can see that there is the information about the route to CE2 in the VPN route table of PE1, and there are two paths.

Note:

- For the checking method of PE2 and PE3, refer to PE1.

Step 6: On PE1, configure route-map, specify the backup next-hop as 10.3.3.3, and enable FRR in the VRF address family of BGP.

#On PE1, configure route-map, and specify the backup next-hop as 10.3.3.3.

```
PE1(config)#route-map vpnfrr
PE1(config-route-map)#match ip address 1000
PE1(config-route-map)#set fast-reroute backup-nexthop 10.3.3.3
PE1(config-route-map)#exit
PE1(config)#ip access-list standard 1000
PE1(config-std-nacl)#permit host 120.1.1.1
PE1(config-std-nacl)#exit
```

#On PE1, enable FRR in the VRF address family of BGP.

```
PE1(config)#router bgp 100
PE1(config-bgp)#address-family ipv4 vrf 1
PE1(config-bgp-af)#fast-reroute route-map vpnfrr
PE1(config-bgp-af)#exit-address-family
PE1(config-bgp)#exit
```

#After configuration, query whether BGP generates the standby VPN route on PE1.

```
PE1#show ip bgp vpnv4 all 120.1.1.1/32
Route Distinguisher: 1:1 (Default for VRF 1), Prefix: 120.1.1.1/32
  Advertised to peers:  5.1.1.2
  300 200
    10.2.2.2 (metric 2) from 10.2.2.2 (19.3.3.3)


     Origin IGP, metric 0, localpref 100, weight 300, valid, internal, best, vrf ftn
installed, vrf external, exist
       Extended Community: RT:1:1
       Recv label: 20480
       Last update: 00:06:18 ago
  300 200
10.3.3.3 (metric 2) from 10.3.3.3 (10.3.3.3)


     Origin IGP, metric 0, localpref 100, valid, internal, vrf ftn installed, vrf external,
exist, BkNexthop(S)
       Extended Community: RT:1:1
       Recv label: 20240
       Last update: 00:06:19 ago
```

You can see the VPN route of PE1, and the VPN route of the next hop 10.3.3.3 has the BkNexthop(S) tag.

Query the IP core, and you can see that there is the FRR route.

```
PE1#show ip frr route vrf 1
Codes: C - Connected, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external


B   120.1.1.1/32 [200/4294967295] via 10.3.3.3, 00:05:58, gigabitethernet2
```

Step 7: On the PE, configure mpls oam, enable oam bfd, and configure the bfd parameters.

#On PE1, configure mpls oam, enable oam bfd, and detect the connectivity of the master path.

```
PE1(config)#mpls oam
PE1(config-mpls-oam)#bfd enable
PE1(config-mpls-oam)#bfd ipv4 10.2.2.2 32 nexthop 1.1.1.2
```

```
PE1(config-mpls-oam)#exit
```

#On PE2, configure mpls oam, and enable oam bfd

```
PE2(config)#mpls oam
PE2(config-mpls-oam)#bfd enable
PE2(config-mpls-oam)#exit
```

#After configuration, query the generated bfd session on PE1. You can see that the generated bfd session is registered by mpls oam.

```
PE1#show bfd session mpls
Type        FEC-Type    FEC-Value       State    LD/RD       OurAddr
NexthopAddr     LabelStack
Dynamic     LDP IPv4    10.2.2.2/32     UP       67/183      1.1.1.1
1.1.1.2
3

PE1#show bfd session mpls detail
Total session number: 1
Type        FEC-Type    FEC-Value       State    LD/RD       OurAddr
NexthopAddr     LabelStack
Dynamic     LDP IPv4    10.2.2.2/32     UP       67/183      1.1.1.1
1.1.1.2
3
Role:Passive
Label Stack:
 label:implicit null
Local State:UP  Remote State:UP  Up for: 0h:1m:55s  Number of times UP:2
Send Interval:10ms  Detection time:30ms(10ms*3)
Local Diag:1  Demand mode:0  Poll bit:0
MinTxInt:10  MinRxInt:10  Multiplier:3
Remote MinTxInt:10  Remote MinRxInt:10  Remote Multiplier:3
Registered protocols:MPLS-OAM
Agent session info:
 Sender:slot 2  Recver:slot 2
```

Step 8: Check the result.

#When the master path does not fail, you can see the VPN forwarding table and the standby VPN forwarding table on PE1.

```
PE1#show ip route vrf 1
Codes: C - Connected, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
       U - Per-user Static route
```

O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external

C 5.1.1.0/24 is directly connected, 02:06:26, gigabitethernet0

L 5.1.1.1/32 is directly connected, 02:06:26, gigabitethernet0

B 110.1.1.1/32 [20/0] via 5.1.1.2, 00:30:03, gigabitethernet0

B 120.1.1.1/32 [200/0] via 10.2.2.2, 00:28:03, gigabitethernet1

PE1#show ip frr route vrf 1

Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS

U - Per-user Static route

O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external

B 120.1.1.1/32 [200/4294967295] via 10.3.3.3, 00:28:05, gigabitethernet2

3.3.13. Configure VPNv4 Route to Back up IPv4 VRF Route

Network Requirements

- In the whole MPLS network, there is only one AS domain. PE1 in AS 100 sets up the MP-IBGP neighbor with PE2, PE3 respectively to interact the route. Set up the MP-IBGP neighbor between PE2 and PE3 to interact the route.
- PE1 sets up the EBGP neighbor with CE1 to interact the route.
- PE2, PE3 set up the EBGP neighbor with CE2 respectively to interact the route.
- The master path is CE1->PE1->PE2->CE2, and the standby path is CE1->PE1->PE3->CE2.
- Detect the connectivity between PE2 and CE2 via ECHO BFD. When the link fails, switch to the standby path for forwarding.

Network Topology

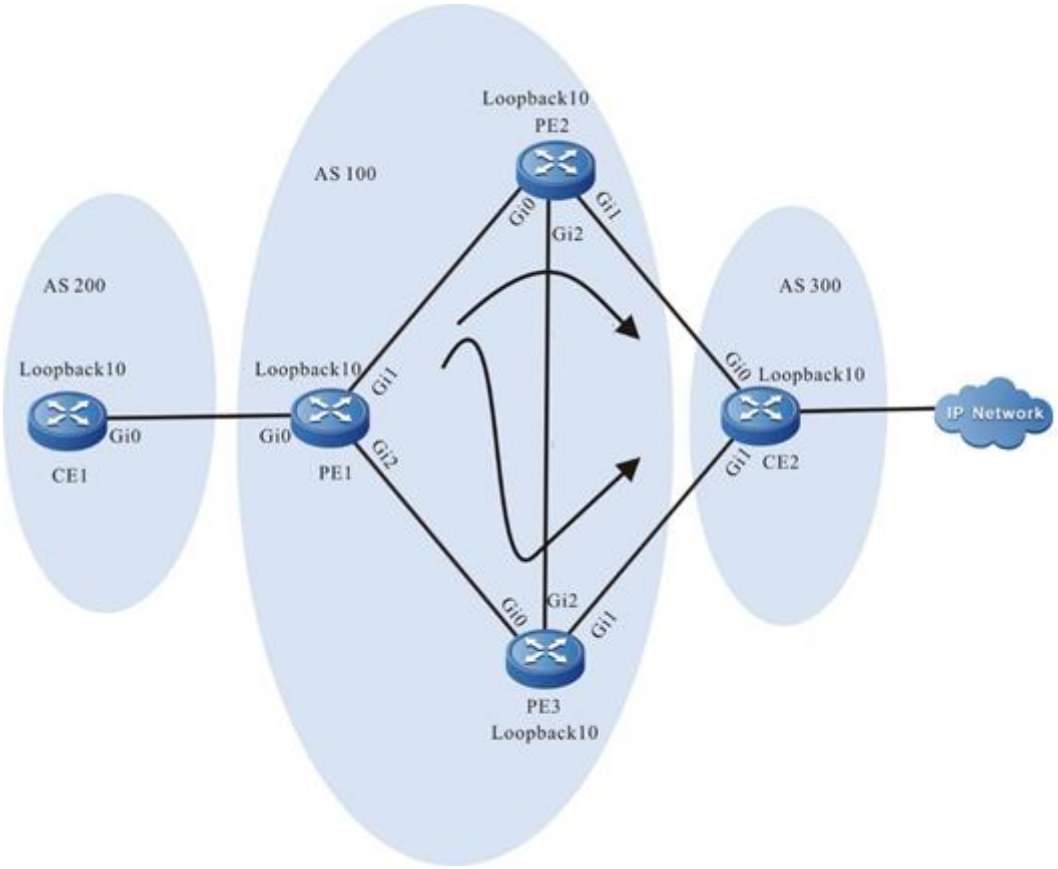

Figure 3-19 Configure VPNv4 route to back up the IPv4 VRF route

Device	Interface	IP Address	Device	Interface	IP Address
CE1	Gi0	5.1.1.2/24		Loopback10	10.2.2.2/32
	Loopback10	110.1.1.1/32	PE3	Gi0	2.1.1.2/24
PE1	Gi0	5.1.1.1/24		Gi1	6.1.1.1/24
	Gi1	1.1.1.1/24		Gi2	3.1.1.1/24
	Gi2	2.1.1.1/32		Loopback10	10.3.3.3/32
	Loopback10	10.1.1.1/32	CE2	Gi0	4.1.1.2/24
PE2	Gi0	1.1.1.2/24		Gi1	6.1.1.2/24
	Gi1	4.1.1.1/24		Loopback10	120.1.1.1/32
	Gi2	3.1.1.2/24			

Configuration Steps

Step 1: Configure the IP address of the interface (omitted).

Step 2: Configure the global OSPF and advertise the global route.

#Configure the global OSPF on PE1.

```
PE1#configure terminal
PE1(config)#router ospf 10
PE1(config-ospf)#network 1.1.1.0 0.0.0.255 area 0
PE1(config-ospf)#network 2.1.1.0 0.0.0.255 area 0
PE1(config-ospf)#network 10.1.1.1 0.0.0.0 area 0
PE1(config-ospf)#exit
```

#Configure the global OSPF on PE2.

```
PE2#configure terminal
PE2(config)#router ospf 10
PE2(config-ospf)#network 1.1.1.0 0.0.0.255 area 0
PE2(config-ospf)#network 3.1.1.0 0.0.0.255 area 0
PE2(config-ospf)#network 10.2.2.2 0.0.0.0 area 0
PE2(config-ospf)#exit
```

#Configure the global OSPF on PE3.

```
PE3#configure terminal
PE3(config)#router ospf 10
PE3(config-ospf)#network 2.1.1.0 0.0.0.255 area 0
PE3(config-ospf)#network 3.1.1.0 0.0.0.255 area 0
PE3(config-ospf)#network 10.3.3.3 0.0.0.0 area 0
PE3(config-ospf)#exit
```

#After the configuration is complete, view the global route table on the device.

Take PE1 as an example:

```
PE1#show ip route
Codes: C - Connected, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external



C   1.1.1.0/24 is directly connected, 00:41:40, gigabitethernet1
L   1.1.1.1/32 is directly connected, 00:41:40, gigabitethernet1
C   2.1.1.0/24 is directly connected, 00:42:06, gigabitethernet2
```

```
L   2.1.1.1/32 is directly connected, 00:42:06, gigabitethernet2
O   3.1.1.0/24 [110/2] via 2.1.1.2, 00:02:51, gigabitethernet2
                [110/2] via 1.1.1.2, 00:03:29, gigabitethernet1
LC  10.1.1.1/32 is directly connected, 20:21:03, loopback10
O   10.2.2.2/32 [110/2] via 1.1.1.2, 00:23:23, gigabitethernet1
O   10.3.3.3/32 [110/2] via 2.1.1.2, 20:17:53, gigabitethernet2
```

You can see that there is the route information of PE2 and PE3 loopback ports in the global route table of PE1.

Note:

- For the checking method of PE2 and PE3, refer to PE1.

Step 3: Enable MPLS IP and MPLS LDP.

#On PE1, enable the global MPLS IP and MPLS LDP, and meanwhile, enable MPLS IP and MPLS LDP on the interface.

```
PE1(config)#mpls ip
PE1(config)#mpls ldp
PE1(config-ldp)#router-id 10.1.1.1
PE1(config-ldp)#address-family ipv4
PE1(config-ldp-af4)#transport-address 10.1.1.1
PE1(config-ldp-af4)#exit
PE1(config-ldp)#exit
PE1(config)#interface gigabitethernet1
PE1(config-if-gigabitethernet1)#mpls ip
PE1(config-if-gigabitethernet1)#mpls ldp
PE1(config-if-gigabitethernet1)#exit
PE1(config)#interface gigabitethernet2
PE1(config-if-gigabitethernet2)#mpls ip
PE1(config-if-gigabitethernet2)#mpls ldp
PE1(config-if-gigabitethernet2)#exit
```

#On PE2, enable the global MPLS IP and MPLS LDP, and meanwhile, enable MPLS IP and MPLS LDP on the interface.

```
PE2(config)#mpls ip
PE2(config)#mpls ldp
PE2(config-ldp)#router-id 10.2.2.2
PE2(config-ldp)#address-family ipv4
PE2(config-ldp-af4)#transport-address 10.2.2.2
PE2(config-ldp-af4)#exit
PE2(config-ldp)#exit
```

```
PE2(config)#interface gigabitethernet0
PE2(config-if-gigabitethernet0)#mpls ip
PE2(config-if-gigabitethernet0)#mpls ldp
PE2(config-if-gigabitethernet0)#exit
PE2(config)#interface gigabitethernet2
PE2(config-if-gigabitethernet2)#mpls ip
PE2(config-if-gigabitethernet2)#mpls ldp
PE2(config-if-gigabitethernet2)#exit
```

#On PE3, enable the global MPLS IP and MPLS LDP, and meanwhile, enable MPLS IP and MPLS LDP on the interface.

```
PE3(config)#mpls ip
PE3(config)#mpls ldp
PE3(config-ldp)#router-id 10.3.3.3
PE3(config-ldp)#address-family ipv4
PE3(config-ldp-af4)#transport-address 10.3.3.3
PE3(config-ldp-af4)#exit
PE3(config-ldp)#exit
PE3(config)#interface gigabitethernet0
PE3(config-if-gigabitethernet0)#mpls ip
PE3(config-if-gigabitethernet0)#mpls ldp
PE3(config-if-gigabitethernet0)#exit
PE2(config)#interface gigabitethernet2
PE2(config-if-gigabitethernet2)#mpls ip
PE2(config-if-gigabitethernet2)#mpls ldp
PE2(config-if-gigabitethernet2)#exit
```

#After configuration, query the LDP session information on the device.

Take PE1 as an example:

```
PE1#show mpls ldp session
Peer IP Address   Peer Type    My Role  State        DS Cap    DeadTime
10.2.2.2          Multicast    Passive  OPERATIONAL  Disabled  00:02:34
10.3.3.3          Multicast    Passive  OPERATIONAL  Disabled  00:02:09

Statistics for ldp sessions:
    Multicast sessions: 2
    Targeted sessions: 0
```

You can see that PE1 sets up the LDP session with PE2, PE3 successfully.

#Query the MPLS forwarding table on the device.

Take PE1 as an example:

```
PE1#show mpls forwarding-table
Pro: L - LDP, O - OSPF, B - MP-BGP, R - RSVP, M - Mapped-Route, S - Static Label,ML - mLDP (ML FEC: Root address/OT/OV), RM - RSVP P2MP (RM FEC: P2MP ID/TID)
```

Pro	Ident	FEC	Inlabel	Outlabel	Outgoing	Next hop
L	global	10.2.2.2/32	24017	3	gigabitethernet1	1.1.1.2
L	global	10.3.3.3/32	24016	3	gigabitethernet2	2.1.1.2

You can see that there is the information about the label to the loopback port of PE2 and PE3 on PE1.

Note:

- For the checking method of PE2 and PE3, refer to PE1.

Step 4: Configure the VPN instance, and advertise the CE route to the PE via EBGP.

#On PE1, configure the VPN instance and the EBGP neighbor in the VPN instance.

```
PE1(config)#ip vrf 1
PE1(config-vrf)#rd 1:1
PE1(config-vrf)#route-target export 1:1
PE1(config-vrf)#route-target import 1:1
PE1(config-vrf)#exit
PE1(config)#interface gigabitethernet0
PE1(config-if-gigabitethernet0)#ip vrf forwarding 1
PE1(config-if-gigabitethernet0)#ip address 5.1.1.1 255.255.255.0
PE1(config-if-gigabitethernet0)#exit
PE1(config)#router bgp 100
PE1(config-bgp)#address-family ipv4 vrf 1
PE1(config-bgp-af)#neighbor 5.1.1.2 remote-as 200
PE1(config-bgp-af)#exit-address-family
PE1(config-bgp)#exit
```

#On CE1, configure EBGP.

```
CE1#configure terminal
CE1(config)#router bgp 200
CE1(config-bgp)#neighbor 5.1.1.1 remote-as 100
CE1(config-bgp)#netwrok 110.1.1.1 255.255.255.255
CE1(config-bgp)#exit
```

#On PE2, configure the VPN instance and the EBGP neighbor in the VPN instance.

```
PE2(config)#ip vrf 1
PE2(config-vrf)#rd 1:1
PE2(config-vrf)#route-target export 1:1
PE2(config-vrf)#route-target import 1:1
PE2(config-vrf)#exit
PE2(config)#interface gigabitethernet1
PE2(config-if-gigabitethernet1)#ip vrf forwarding 1
PE2(config-if-gigabitethernet1)#ip address 4.1.1.1 255.255.255.0
PE2(config-if-gigabitethernet1)#exit
PE2(config)#router bgp 100
PE2(config-bgp)#address-family ipv4 vrf 1
PE2(config-bgp-af)#neighbor 4.1.1.2 remote-as 300
PE2(config-bgp-af)# exit-address-family
PE2(config-bgp)#exit
```

#On PE3, configure the VPN instance and the EBGP neighbor in the VPN instance.

```
PE3(config)#ip vrf 1
PE3(config-vrf)#rd 1:1
PE3(config-vrf)#route-target export 1:1
PE3(config-vrf)#route-target import 1:1
PE3(config-vrf)#exit
PE3(config)#interface gigabitethernet1
PE3(config-if-gigabitethernet1)#ip vrf forwarding 1
PE3(config-if-gigabitethernet1)#ip address 6.1.1.1 255.255.255.0
PE3(config-if-gigabitethernet1)#exit
PE3(config)#router bgp 100
PE3(config-bgp)#address-family ipv4 vrf 1
PE3(config-bgp-af)#neighbor 6.1.1.2 remote-as 300
PE3(config-bgp-af)# exit-address-family
PE3(config-bgp)#exit
```

#On CE2, configure EBGP.

```
CE2#configure terminal
CE2(config)#router bgp 300
CE2(config-bgp)#neighbor 4.1.1.1 remote-as 100
CE2(config-bgp)#neighbor 6.1.1.1 remote-as 100
CE2(config-bgp)#network 120.1.1.1 255.255.255.255
CE2(config-bgp)#exit
```

#After configuration, query the VPN route table on PE.

Take PE1 as an example:

```
PE1#show ip route vrf 1
Codes: C - Connected, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external



C   5.1.1.0/24 is directly connected, 01:09:37, gigabitethernet0
L   5.1.1.1/32 is directly connected, 01:09:37, gigabitethernet0
B   110.1.1.1/32 [20/0] via 5.1.1.2, 00:00:51, gigabitethernet0
B   120.1.1.1/32 [200/0] via 10.3.3.3, 00:00:04, gigabitethernet2
```

You can see that there is the information about the route to CE1 in the VPN1 route table of PE1.

Note:

- For the checking method of PE2 and PE3, refer to PE1.

Step 5: Configure MP-IBGP between PE1 and PE2, PE3, and use the loopback interface as the peer address.

#On PE1, configure MP-IBGP with PE2, PE3, and enable the VPNv4 address family.

```
PE1(config)#router bgp 100
PE1(config-bgp)#neighbor 10.3.3.3 remote-as 100
PE1(config-bgp)#neighbor 10.3.3.3 update-source loopback10
PE1(config-bgp)#neighbor 10.2.2.2 remote-as 100
PE1(config-bgp)#neighbor 10.2.2.2 update-source loopback10
PE1(config-bgp)#address-family vpnv4
PE1(config-bgp-af)#neighbor 10.3.3.3 activate
PE1(config-bgp-af)#neighbor 10.3.3.3 send-community extended
PE1(config-bgp-af)#neighbor 10.2.2.2 activate
PE1(config-bgp-af)#neighbor 10.2.2.2 send-community extended
PE1(config-bgp-af)#exit-address-family
PE1(config-bgp)#exit
```

#On PE2, configure MP-IBGP with PE1, PE3, and enable the VPNv4 address family.

```
PE2(config)#router bgp 100
PE2(config-bgp)#neighbor 10.1.1.1 remote-as 100
PE2(config-bgp)#neighbor 10.1.1.1 update-source loopback10
PE2(config-bgp)#neighbor 10.3.3.3 remote-as 100
PE2(config-bgp)#neighbor 10.3.3.3 update-source loopback10
PE2(config-bgp)#address-family vpnv4
```

```
PE2(config-bgp-af)#neighbor 10.1.1.1 activate
PE2(config-bgp-af)#neighbor 10.1.1.1 send-community extended
PE2(config-bgp-af)#neighbor 10.3.3.3 activate
PE2(config-bgp-af)#neighbor 10.3.3.3 send-community extended
PE2(config-bgp-af)#exit-address-family
PE2(config-bgp)#exit#
```

#On PE3, configure MP-IBGP with PE1, PE2, and enable the VPNv4 address family.

```
PE3(config)#router bgp 100
PE3(config-bgp)#neighbor 10.1.1.1 remote-as 100
PE3(config-bgp)#neighbor 10.1.1.1 update-source loopback10
PE3(config-bgp)#neighbor 10.2.2.2 remote-as 100
PE3(config-bgp)#neighbor 10.2.2.2 update-source loopback10
PE3(config-bgp)#address-family vpnv4
PE3(config-bgp-af)#neighbor 10.1.1.1 activate
PE3(config-bgp-af)#neighbor 10.1.1.1 send-community extended
PE3(config-bgp-af)#neighbor 10.2.2.2 activate
PE3(config-bgp-af)#neighbor 10.2.2.2 send-community extended
PE3(config-bgp-af)#exit-address-family
PE3(config-bgp)#exit
```

#After configuration, query the VPN route table of BGP on PE.

Take PE2 as an example :

```
PE2#show ip bgp vpnv4 all
BGP table version is 289, local router ID is 19.3.3.3
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network          Next Hop            Metric     LocPrf Weight Path
Route Distinguisher: 1:1 (Default for VRF 1)
[B]*>i110.1.1.1/32      10.1.1.1                 0      100      0 300 i
[B]*> 120.1.1.1/32      4.1.1.2                  0               0 300 200 i
[B]* i                  10.3.3.3                 0      100      0 300 200 i
```

You can see that there is the information about the route to CE2 in the VPN route table of PE2, and there are two paths.

Note:

- For the checking method of PE1 and PE3, refer to PE2.

Step 6: On PE1, configure route-map, specify the backup next-hop as 10.3.3.3, and enable FRR in the VRF address family of BGP.

#On PE2, configure route-map, and specify the backup next-hop as 10.3.3.3.

```
PE2(config)#route-map vpnfrr
PE2(config-route-map)#match ip address 1000
PE2(config-route-map)#set fast-reroute backup-nexthop 10.2.2.2
PE2(config-route-map)#exit
PE2(config)#ip access-list standard 1000
PE2(config-std-nacl)#permit host 120.1.1.1
PE2(config-std-nacl)#exit
```

#On PE2, enable FRR in the VRF address family of BGP.

```
PE2(config)#router bgp 100
PE2(config-bgp)#address-family ipv4 vrf 1
PE2(config-bgp-af)#fast-reroute route-map vpnfrr
PE2(config-bgp-af)#exit-address-family
PE2(config-bgp)#exit
```

#After configuration, query whether BGP generates the standby VPN route on PE1.

```
PE2#show ip bgp vpnv4 all 120.1.1.1/32
Route Distinguisher: 1:1 (Default for VRF 1), Prefix: 120.1.1.1/32
 Advertised to peers:  10.1.1.1 10.3.3.3
 300 200
  4.1.1.2 from 4.1.1.2 (200.1.1.1)


   Origin IGP, metric 0, localpref 100, valid, external, best, vrf orign, vrf ce, ILM installed
    Extended Community: RT:1:1
    ILM info: label 20480,Per-Route
    Last update: 00:13:21 ago
 300 200
  10.3.3.3 (metric 2) from 10.3.3.3 (10.3.3.3)


   Origin IGP, metric 0, localpref 100, valid, internal, vrf ftn installed, vrf external, exist, BkNexthop(S)
    Extended Community: RT:1:1
    Recv label: 20240
    Last update: 00:25:24 ago
```

You can see that the VPN route of PE2 with the next hop 10.3.3.3 has the BkNexthop(S) tag.

Query the IP core, and you can see that there is the FRR route.

```
PE2#show ip frr route vrf 1
```

```
Codes: C - Connected, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external

B   120.1.1.1/32 [20/4294967295] via 10.3.3.3, 00:00:02, gigabitethernet2
```

Step 7: Check the result.

On PE2, query the bfd session information.

```
PE2#show bfd session
OurAddr          NeighAddr          LD/RD          State      Holddown
Interface
4.1.1.1          4.1.1.2            188/188        UP         500        gigabitethernet1
PE2#show  bfd session  detail
Total session number: 1
OurAddr          NeighAddr          LD/RD          State      Holddown
Interface
4.1.1.1          4.1.1.2            188/188        UP         500        gigabitethernet1
Type:ipv4 direct  Mode:echo
Local State:UP  Remote State:UP  Up for: 0h:6m:19s  Number of times UP:1
Send Interval:100ms  Detection time:500ms(100ms*5)
Local Diag:0  Demand mode:0  Poll bit:0
Registered protocols:FIB_MGR
Agent session info:
  Sender:slot 0  Recver:slot 0
```

You can see the bfd session generated by PE2.

#When the master path does not fail, you can see the VPN forwarding table and the standby VPN forwarding table on PE2.

```
PE2#show ip route vrf 1
Codes: C - Connected, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external

C   4.1.1.0/24 is directly connected, 00:23:08, gigabitethernet1
L   4.1.1.1/32 is directly connected, 00:23:08, gigabitethernet1
```

B 110.1.1.1/32 [200/0] via 10.1.1.1, 00:34:14, gigabitethernet0

B 120.1.1.1/32 [20/0] via 4.1.1.2, 00:09:05, gigabitethernet1

PE2#show ip frr route vrf 1

Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS

U - Per-user Static route

O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external

B 120.1.1.1/32 [20/4294967295] via 10.3.3.3, 00:09:10, gigabitethernet2

4. MPLS TE

4.1. Overview

In the early 1990s, the carrier just simply uses the shortest path calculated by IGP (Interior Gateway Protocol) to map the service flow of the customer to the physical topology of the network, which results in the “hot spot” problem, that is, the partial congestion caused by the un-balance of the network resource load. This will affect the network performance seriously.

To solve the above “Hot spot” problem, put forward the TE (Traffic Engineering) technology. The core of the TE technology is to adopt the traffic transferring to avoid the congestion caused by the unbalanced load. It can balance the service load between different links and devices in the network, improve the operation performance of the network, optimize the network traffic distributing, and improve traffic performance indexes, such as delay, jitter, packet loss and throughput, so as to make full use of the present network resource and meet the user service demands.

In the early core network, the TE technology is realized by changing the metric of the specified route, but with the increasing of the IP network scale, this mode is showing its limitations. To deploy TE in the large backbone network, you should adopt the solution, which is easy to use and has great scalability. MPLS (Multiprotocol Label Switching) is one routing and forwarding separating technology in the middle 1990s. Because the technical advantage of its routing and forwarding separation, it is convenient to set up one virtual topology not depending on the route on the physical network topology, and then map the traffic to the topology. Combining the MPLS overlapping model with TE, the MPLS TE technology appears. The MPLS TE includes the following four technical components:

- Information releasing component: MPLS TE expands the present IGP to release the link TE information and generate the TEDB (Traffic Engineering DataBase).
- Path selection component: The path selection component uses the data in TEDB, and adopts CSPF (Constraint Shortest Path First) algorithm to calculate the path meeting the specified restriction conditions for the MPLS P2P TE tunnel.
- Signaling protocol component: The signaling protocol component sets up one LSP (Label Switched Path) along the explicit path LSR (Label Switching Router), and reserves the resources. Currently, the process is realized by RSVP-TE (Resource Reservation Protocol - Traffic Engineering extension).
- Packet forwarding component: The packet forwarding component uses the static route, policy route or auto route to import the traffic to the MPLS P2P TE tunnel for forwarding.

Compared with other traffic engineering solution, MPLS TE has many advantages, such as support tunnel path control and priority preemption, support FRR (Fast Reroute), and high maintainability. This makes MPLS TE become the first scheme for bandwidth guarantee and traffic deployment in the IP network.

4.2. MPLS TE Function Configuration

Table 4-1 MPLS TE function configuration list

Configuration Task	
Configure MPLS TE basic functions	Configure MPLS TE basic functions
Configure MPLS P2P TE tunnel	Configure MPLS TE attribute of the link
	Configure the OSPF expanding and IS-IS expanding for TE
	Configure the MPLS TE explicit path
	Configure the MPLS P2P TE tunnel
	Configure the MPLS P2P TE tunnel attribute
Configure RSVP-TE advanced features	Configure the refresh timer of the RSVP-TE message
	Configure RSVP-TE message confirming
	Configure RSVP-TE refresh suppression
	Configure the route/label recording
	Configure RSVP-TE loop detection
	Configure the PHP features of the MPLS P2P TE tunnel
	Configure RSVP-TE tunnel re-optimization
	Configure the RSVP-TE Hello mechanism
	Configure auto bandwidth adjusting of the MPLS P2P TE tunnel
	Configure the interval of re-establishing the MPLS P2P TE tunnel regularly

Configuration Task	
Configure the MPLS P2P TE tunnel traffic forwarding	Configure the static route to make the traffic be forwarded along the MPLS P2P TE tunnel
	Configure the policy route to make the traffic be forwarded along the MPLS P2P TE tunnel
	Configure the auto route to make the traffic be forwarded along the MPLS P2P TE tunnel
	Configure the forwarding adjacency to make the traffic be forwarded along the MPLS P2P TE tunnel
Configure the parameters of affecting the traffic forwarding of the MPLS P2P TE tunnel	Configure the auto route metric of the MPLS P2P TE tunnel
	Configure the load balance share of the MPLS P2P TE tunnel
Configure RSVP-TE to link with BFD	Configure RSVP-TE to link with BFD
Configure MPLS TE fast re-routing	Configure MPLS TE fast re-routing
Configure MPLS TE GR	Configure MPLS TE GR

4.2.1. Configure MPLS TE Basic Functions

Configuration Condition

Before configuring the MPLS TE basic functions, first complete the following tasks:

- Configure the link layer protocol, ensuring the normal communication of the link layer
- Configure the network layer address of the interface, making the neighboring network nodes reachable at the network layer
- Configure IGP, ensuring the intercommunication of the LSRs at the network layer
- Configure MPLS basic functions, ensuring that the MPLS packet can be received and sent

Configure MPLS TE Basic Functions

Configuring MPLS TE basic functions includes enabling the MPLS TE capability globally and on the interface, and configuring the Router ID of RSVP-TE. If the Router ID of RSVP-TE is not configured, elect according to the following rule:

- First, select the maximum one from the IP addresses of the Loopback interfaces as Router ID

- If the Loopback interface is not configured with the IP address, select the maximum one from the IP addresses of the other interfaces as the Router ID.
- The interface address can be selected as Router ID only when the interface is UP.

Table 4-2 Configure MPLS TE basic functions

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enable the global MPLS TE capability and enter the RSVP-TE configuration mode	**mpls traffic-eng tunnels**	Mandatory By default, do not enable the global MPLS TE capability.
Configure the Router ID of RSVP-TE	**router-id** *ip-address*	Optional By default, generate according to the selecting rule of RSVP-TE Router ID.
Exit the RSVP-TE configuration mode	**exit**	-
Enter the interface configuration mode	**interface** *interface-name*	-
Enable the MPLS TE capability of the interface	**mpls traffic-eng tunnels**	Mandatory By default, do not enable the MPLS TE capability of the interface.

Note:

- It is suggested to configure the Router ID of RSVP-TE as one routable Loopback interface address at the local.

4.2.2. Configure MPLS P2P TE Tunnel

Configuration Condition

Before configuring the MPLS P2P TE tunnel, first complete the following tasks:

- Configure the link layer protocol, ensuring the normal communication of the link layer
- Configure the network layer address of the interface, making the neighboring network nodes reachable at the network layer
- Configure IGP, ensuring the intercommunication of the LSRs at the network layer

- Configure MPLS basic functions, ensuring that the MPLS packet can be received and sent
- Configure MPLS TE basic functions.

Configure the MPLS TE Attributes of the Link

The MPLS TE attribute of the link is released to the network via the TE expanding of the IGP and generate TEDB. The MPLS TE attributes of the link include:

- MPLS TE maximum reserved bandwidth of the link: You should configure the MPLS TE maximum reserved bandwidth. Otherwise, the MPLS P2P TE tunnel cannot be set up successfully.
- MPLS TE management weight of the link: It can be regarded as the MPLS TE metric of the link. After configuring the MPL TE management weight of the link and when CSPF calculates the path of the MPLS P2P TE tunnel, use the MPL TE management weight of the link as the metric of the link, but not use the IGP metric of the link.
- MPLS TE attribute flag of the link: The flag is one 32-bit number. If one digit of the number is 1, it indicates that the link has one attribute. If it is 0, it indicates that the link does not have one attribute. The specific meanings of the attributes are defined according to the demand of the application management.

Table 4-3 Configure the MPLS TE attributes of the link

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the interface configuration mode	**interface** *interface-name*	-
Configure the maximum reserved bandwidth of the link MPLS TE	**ip rsvp bandwidth** *bandwidth-value*	Optional By default, the maximum reserved bandwidth of the link MPLS TE is 0kbps.
Configure the management weight of the link MPLS TE	**mpls traffic-eng admin-weight** *weight-value*	Optional By default, the management weight of the link MPLS TE is the LGP metric of the link.
Configure the MPLS TE attribute flag of the link	**mpls traffic-eng attribute-flags** *flags-value*	Optional By default, the MPLS TE attribute flag of the link is 0.

Configure OSPF Expanding and IS-IS Expanding for TE

MPLS TE releases the TE information by expanding OSPF or IS-IS. After configuring the OSPF expanding and IS-IS expanding for TE, enable the MPLS TE capability of the corresponding protocol, and enable the CSPF service.

When the CSPF path calculation has multiple results of meeting the requirement, CSPF adopts the following arbitration modes:

- Select the one with the smallest metric
- If the metric is equal, select the one with the least route hops
- If the route hops are the same, adopt the CSPF highest arbitration mode.

There are three CSPF highest arbitration modes:

- random: Select at random
- least-fill: Select the one with minimum reserved bandwidth
- most-fill: Select the one with maximum reserved bandwidth

1. Configure TE OSPF expanding

When using OSPF, it is necessary to enable the OSPF opaque LSA function. By default, enable OSPF opaque LSA function. For the details and configuration of OSPF opaque LSA function, refer to the unicast route configuration manual-OSPF chapter. If not specifying the MPLS TE Router ID of OSPF, use the Router ID of the OSPF process as its MPLS TE Router ID.

Table 4-4 Configure the TE OSPF expanding

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the OSPF configuration mode	**router ospf** *process-id*	-
Enable the OSPF opaque LSA function	**capability opaque**	Optional By default, enable the OSPF opaque LSA function.
Enable the MPLS TE capability of the OSPF specified area and enable the CSPF service	**mpls traffic-eng area** *area-id*	Mandatory By default, do not enable the MPLS TE capability of the OSPF, and do not enable the CSPF service.

Step	Command	Description
Configure the MPLS TE Router ID of OSPF	**mpls traffic-eng router-id** *ip-address*	Optional By default, use the Router ID of the OSPF process as its MPLS TE Router ID.
Configure the highest arbitration mode of CSPF	**mpls traffic-eng cspf tie-break** { **least-fill** | **most-fill** | **random** }	Optional By default, the highest arbitration mode of CSPF is random.

2. Configure the IS-IS expanding of TE

When using IS-IS, it is necessary to configure the IS-IS metric type as the wide metric type (metric-style wide). By default, the IS-IS metric type is the narrow metric type. Besides, the IS-IS overload flag bit (overload bit) will affect the CSPF calculation, that is, CSPF calculation will ignore the network node set with overload flag bit. For the details and configuration of the IS-IS metric type and overload flag, refer to the unicast route configuration manual-IS-IS chapter. If not specifying MPLS TE Router ID of IS-IS, elect according to the following rules:

- Select the maximum IP address of the Loopback interface as Router ID
- If there is no Loopback interface configured with IP address, select the maximum from the IP addresses of other interfaces as Router ID
- The interface address can be selected as Router ID only when the interface is UP.

Table 4-5 Configure the TE IS-IS expanding

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the IS-IS configuration mode	**router isis** [*area-tag*]	-
Configure the IS-IS metric type as the wide metric type	**metric-style wide**	Mandatory By default, the IS-IS metric type is narrow metric type.
Enter IS-IS IPv4 address family configuration mode	**address-family ipv4 unicast**	-

Step	Command	Description
Enable the MPLS TE capability of the IS-IS specified layer and enable the CSPF service	**mpls traffic-eng** { **level-1** | **level-2** }	Mandatory By default, do not enable the IS-IS MPLS TE capability, and do not enable the CSPF service.
Configure MPLS TE Router ID of IS-IS	**mpls traffic-eng router-id** *ip-address*	Optional By default, generate according to the electing rules of the IS-IS MPLS TE Router ID.

Note:

- MPLS TE capability can only be enabled in one area of the OSPF process or in one layer of IS-IS.
- Currently, the CSPF highest arbitration mode can be configured only in the OSPF configuration mode.
- To ensure that the released MPLS TE information is correct, it is suggested to configure MPLS TE Router ID of IGP and Router ID of RSVP-TE as the same address.

Configure MPLS TE Explicit Path

MPLS TE explicit path consists of a series of node addresses (MPLS TE Router ID or interface address). You can add and delete the node address to specify the nodes or links passed or bypassed by the MPLS P2P TE tunnel. The explicit path will serve as the input limitation condition of the CSPF calculation.

The node on the explicit path has two attributes:

- strict: strict node, indicating that the node and the last node in the explicit path do not permit other node during the CSPF calculation.
- Loose: loose node, indicating that the node and the last node in the explicit path permit other nodes during the CSPF calculation.

The strict node and loose node are both the nodes that should be passed by the MPLS P2P TE tunnel. If using the **exclude** parameter to add one node, it indicates that the node is not passed by the MPLS P2P TE tunnel path and should be excluded during the CSPF calculation.

Table 4-6 Configure MPLS TE explicit path

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Create one explicit path and enter the explicit path configuration mode	**ip explicit-path** *path-name*	-
Add one strict/loose node in the explicit path	**address** *ip-address* { **strict** | **loose** }	Optional
Add one node not passed by MPLS P2P TE tunnel path in the explicit path	**exclude** *ip-address*	Optional
Specify the index number to add one loose/strict node in the explicit path	**index** *index-value* **address** *ip-address* { **strict** | **loose** }	Optional
Specify one index number to add one node not passed by the MPLS P2P TE tunnel path in the explicit path	**index** *index-value* **exclude** *ip-address*	Optional
Add one strict/loose node before the specified index number in the explicit path	**before** *index-value* **address** *ip-address* { **strict** | **loose** }	Optional
Add one node not passed by the MPLS P2P TE tunnel path before the specified index number in the explicit path	**before** *index-value* **exclude** *ip-address*	Optional
Display the node list of the explicit path	**list**	Optional

Note:

- The strict node, loose node and the node not passed by the MPLS P2P TE tunnel path can be mixed to use in one explicit path, but do not permit configuring one node in one explicit path as the strict node and loose node at the same time, or configuring as the

strict/loose node and the node not passed by the MPLS P2P TE tunnel path at the same time.

- When specifying the index to add a node in the explicit path, the index number can be inconsecutive. It just reflects the order between the nodes. After saving the configuration and restarting the device, the index will be numbered from 1 again.
- When adding a node before the specified index in the explicit path and if the node of the specified index does not exist, the added node uses the specified index.
- After configuring the node of the explicit path every time, display the current node list of the explicit path automatically.

Configure MPLS P2P TE Tunnel

The MPLS P2P TE tunnel is one logical virtual interface. The interface can be configured with the un-numbered IP address. For the details and configuration of the Tunnel interface and interface address, refer to the interface configuration manual-tunnel interface chapter.

Table 4-7 Configure the MPLS P2P TE tunnel

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Create one Tunnel interface and enter the Tunnel interface configuration mode	**interface tunnel** *tunnel-unit*	-
Configure the work mode of the Tunnel interface as MPLS TE	**tunnel mode mpls traffic-eng**	Mandatory By default, the work mode of the Tunnel interface is GRE over IPv4.
Configure the destination address of the Tunnel interface	**tunnel destination** *ip-address*	Mandatory By default, do not configure the destination address of the Tunnel interface.
Configure the IP address of the Tunnel interface	**ip** { **unnumbered** *reference-interface* | **address** *ip-address* { *network-mask* | *mask-len* } }	Optional By default, do not configure the IP address of the Tunnel interface.

Note:

- If it is necessary to configure the Tunnel interface of the MPLS P2P TE tunnel as the egress interface of the route for traffic forwarding, you should configure the IP address for the Tunnel interface and the IGP route protocol should contain the segment address.

Configure MPLS P2P TE tunnel Attributes

The MPLS P2P TE tunnel attributes include:

- Required bandwidth
- Path option: The tunnel can be configured with multiple path options with different priorities. The path option can be explicit path or dynamic path. The value range of the path option priority is 1-1000. The small the value, the higher the priority. When the tunnel is set up, calculate the LSP path according to the priority order of the configured path options. After configuring the path option, it will not trigger the path calculation according to the new priority order until the tunnel is re-set up or re-optimized.
- Setup priority and hold priority: The value range is 0-7. The smaller the value, the higher the priority. When setting up one tunnel and if it is necessary to compete for the link bandwidth with another setup tunnel, compare the setup priority of the new tunnel with the hold priority of the previous setup tunnel. Decide whether to preempt according to the comparison result. In the actual application, configure the setup priority and the hold priority of the tunnel as the same value except for the special requirement.
- Affinity attribute: Configuring the affinity attribute of the tunnel includes enabling the advertising capability of the tunnel affinity attribute signaling, and configuring the tunnel affinity attribute requirement. The advertising capability of the tunnel affinity attribute signaling indicates that RSVP-TE carries the tunnel affinity attribute information in the PATH message sent for the MPLS P2P TE tunnel. The tunnel affinity attribute requirement consists of attribute value and attribute policy. The attribute value is one 32-bit number. If the attribute policy is include-all, it indicates that the link passed by the tunnel is required to have the MPLS TE attribute flag matching with each 1 bit of the attribute value. If the attribute policy is include-any, it indicates that the link passed by the tunnel is required to have the MPLS TE attribute flag matching with any 1 bit of the attribute value. If the attribute policy is exclude, itn indicates that the link passed by the tunnel cannot have the MPLS TE attribute flag matching with any 1 bit of the attribute value. For the configuration of the link MPLS TE attribute flag, refer to the chapter of configuring the link MPLS TE attribute.

Table 4-8 Configure the MPLS P2P TE tunnel attributes

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the Tunnel interface configuration mode	**interface tunnel** *tunnel-unit*	-

Step	Command	Description
Configure the required bandwidth of the MPLS P2P TE tunnel	**tunnel mpls traffic-eng bandwidth** *bandwidth-value*	Mandatory By default, do not configure the required bandwidth of the MPLS P2P TE tunnel.
Configure the path option of the MPLS P2P TE tunnel	**tunnel mpls traffic-eng path-option** *path-priority* [**dynamic** | **explicit-path** *path-name*]	Optional By default, do not configure the path option of the MPLS P2P TE tunnel.
Configure the setup priority and hold priority of the MPLS P2P TE tunnel	**tunnel mpls traffic-eng priority** *setup-priority hold-priority*	Optional By default, the setup priority and hold priority of the MPLS P2P TE tunnel are 7 and 0 respectively.
Enable the advertising capability of the affinity attribute signaling of the MPLS P2P TE tunnel	**tunnel mpls traffic-eng affinity-signalling**	Optional By default, do not enable the advertising capability of the affinity attribute signaling of the MPLS P2P TE tunnel.
Configure the affinity attribute requirement of the MPLS P2P TE tunnel	**tunnel mpls traffic-eng affinity** { **exclude** | **include-all** | **include-any** } *affinity-value*	Optional By default, do not configure the affinity attribute requirement of the MPLS P2P TE tunnel.

Note:

- You should configure the required bandwidth of the tunnel. Otherwise, the tunnel cannot be set up successfully.
- The required bandwidth of the tunnel cannot exceed the physical bandwidth of the egress interface. Otherwise, the tunnel cannot be set up successfully.
- If configuring multiple path options with the same priority for one tunnel, only the last configured path option takes effect.
- To ensure the stability of the setup tunnel, the hold priority of the tunnel cannot be smaller than the setup priority, that is, the hold priority value should be larger than or equal to the setup priority value.

- You cannot configure the affinity attribute requirements with attribute policy as include-all and include-any for one tunnel at the same time.

4.2.3. Configure Auto MPLS P2MP TE Tunnel

At present, more and more applications related to multicast have appeared in the lives of people. Auto MPLS P2MP TE tunnel can help simplify multicast deployment, and make multicast gain the advantages of MPLS TE in terms of QoS guarantee and fast rerouting.

Configuration Condition

Before configuring the MPLS P2MP TE tunnel, first complete the following tasks:

- Configure the link layer protocol, ensuring the normal communication of the link layer
- Configure the network layer address of the interface, making the neighboring network nodes reachable at the network layer
- Configure IGP, ensuring the intercommunication of the LSRs at the network layer
- Configure MPLS basic functions, ensuring that the MPLS packet can be received and sent
- Configure MPLS TE basic functions.
- Configure the MPLS TE attributes of the link.
- Configure the OSPF extension and IS-IS extension for TE

Configure Enabling MPLS P2MP TE Function

Table 4-9 Configure enabling the MPLS P2MP TE function

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the RSVP-TE configuration mode	**mpls traffic-eng tunnels**	-
Enable the MPLS P2MP TE function	**p2mp**	Mandatory By default, do not enable the MPLS P2MP TE function.

Configure MPLS P2MP TE Leaf Node List

By default, MPLS P2MP TE tunnels dynamically select leaf nodes based on the service-aware access nodes. If you want to control the MPLS P2MP TE tunnel to select the range of leaf nodes or specify the explicit path of leaf nodes, you can configure the list of leaf nodes.

Table 4-10 Configure MPLS P2MP TE leaf node list

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Create one MPLS P2MP TE leaf node list and enter the leaf node list configuration mode	**mpls traffic-eng leaf-list** *leaf-list-name*	Mandatory By default, do not create the MPLS P2MP TE leaf node list.
Add one leaf node and specify the path options	**destination** *ip-address* **path-option** { **dynamic** | **explicit-path** *path-name* }	Optional By default, the MPLS P2MP TE leaf node list do not contain any leaf node.

Note:

- The maximum number of the MPLS P2MP TE leaf node lists is 1024, and one MPLS P2MP TE leaf node list can contain 255 leaf nodes at most.
- If the MPLS P2MP TE tunnel references one leaf node list without any leaf node, the MPLS P2MP TE tunnel will dynamically select the leaf node according to the service-aware access node.
- When making explicit path planning for each leaf node, it is necessary to avoid path re-convergence error and path crossover error. Otherwise, the corresponding sub-LSP of the MPLS P2MP TE tunnel will not be established successfully. The path re-convergence error indicates that two sub-LSPs enter an intermediate node through different input interfaces, but use the same exit interface to leave the node; the path overlap error indicates that two sub-LSPs enter an intermediate node through different input interfaces, and use different output interfaces to leave the node.

Configure MPLS P2MP TE Profile

By configuring the MPLS P2MP TE profile, you can set various properties of the MPLS P2MP TE tunnel that references the profile. Since the auto MPLS P2MP TE tunnel does not have a configurable tunnel interface, to set its properties, it is necessary to create an MPLS P2MP TE profile and configure the tunnel properties in the profile configuration mode, and then, reference the profile when deploying the business, so that the auto MPLS P2MP TE tunnel inherits all the properties configured under the profile.

The configurable tunnel attributes in the MPLS P2MP TE profile include:

- Demand bandwidth
- Leaf node list
- Setup priority and hold priority
- Affinity attribute

Except for the leaf node list, the meanings of the other tunnel attributes are the same as the MPLS P2P TE tunnel.

Table 4-11 Configure the MPLS P2MP TE profile

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Create one MPLS P2MP TE mode and enter the profile configuration mode	**mpls traffic-eng p2mp-template** *p2mp-template-name*	Mandatory By default, do not create the MPLS P2MP TE profile.
Configure the demand bandwidth of the MPLS P2MP TE profile	**tunnel mpls traffic-eng bandwidth** *bandwidth-value*	Mandatory By default, do not configure the demand bandwidth of the MPLS P2MP TE profile.
Configure the MPLS P2MP TE profile to reference the MPLS P2MP TE leaf node list	**tunnel mpls traffic-eng leaf-list** *leaf-list-name*	Optional By default, the MPLS P2MP TE does not reference the MPLS P2MP TE leaf node list.
Configure the setup priority and hold priority of the MPLS P2MP TE profile	**tunnel mpls traffic-eng priority** *setup-priority hold-priority*	Optional By default, the setup priority and hold priority of the MPLS P2MP TE profile are 7 and 0 respectively.
Enable the affinity attribute signaling advertising capability of the MPLS P2MP TE profile	**tunnel mpls traffic-eng affinity-signalling**	Optional By default, the MPLS P2MP TE profile does not enable the affinity attribute signaling advertising capability.
Configure the affinity attribute requirement of the MPLS P2MP TE profile	**tunnel mpls traffic-eng affinity** { **exclude** | **include-all** | **include-any** } *affinity-value*	Optional By default, the MPLS P2MP TE profile is not configured with the affinity attribute requirement.

Note:

- The maximum number of the MPLS P2MP TE profile is 1024.
- The demand bandwidth of the MPLS P2MP TE profile must be configured. Otherwise, the MPLS P2MP TE tunnel that references the profile will not be set up successfully.
- The demand bandwidth of the MPLS P2MP TE profile cannot exceed the physical bandwidth of the corresponding egress interface. Otherwise, the MPLS P2MP TE tunnel that references the profile cannot be set up successfully.
- To ensure the stability after the MPLS P2MP TE tunnel is set up, the hold priority of the MPLS P2MP TE profile cannot be smaller than the setup priority, that is, the value of the hold priority must be no less than the value of the setup priority.
- You cannot configure the affinity attribute requirement with the attribute policy as include-all and include-any for one MPLS P2MP TE profile at the same time.

4.2.4. Configure RSVP-TE Advanced Features

Configuration Condition

Before configuring the MPLS TE advanced features, first complete the following tasks:

- Configure the link layer protocol, ensuring the normal communication of the link layer
- Configure the network layer address of the interface, making the neighboring network nodes reachable at the network layer
- Configure IGP, ensuring the intercommunication of the LSRs at the network layer
- Configure MPLS basic functions, ensuring that the MPLS packet can be received and sent
- Configure MPLS TE basic functions.
- Configure MPLS TE tunnel.

Configure Refresh Timer of RSVP-TE Message

RSVP-TE is one soft-state protocol. It needs to refresh the message in the network regularly to update the reserved resources. Configuring the RSVP-TE state timer includes:

- Configure the timeout multiplier of the RSVP-TE message. The value can be configured globally and also can be configured on the interface separately. The global configuration is valid for all interfaces. If configuring globally and on the specified interface at the same time, the configuration on the interface is prior.
- Configure the refresh interval of the RSVP-TE message: The value can only be configured on the interface. To prevent the RSVP-TE message of the whole network from being synchronized, the actual refresh interval of the message has 50% jitter.

The timeout calculation formula of the RSVP-TE message is: (timeout multiplier + 0.5) * 1.5 *refresh interval. The default timeout multiplier is 3, and the default refresh interval is 30s. Therefore, the default timeout is 157.5s.

Table 4-12 Configure the refresh timer of the RSVP-TE message

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the RSVP-TE configuration mode	**mpls traffic-eng tunnels**	-
Configure the timeout multiplier of the global RSVP-TE message	**keep-multiplier** *multiplier*	Optional By default, the timeout multiplier of the global RSVP-TE message is 3.
Exit the RSVP-TE configuration mode	**exit**	-
Enter the interface configuration mode	**interface** *interface-name*	-
Configure the RSVP-TE message timeout multiplier of the interface	**ip rsvp keep-multiplier** *multiplier*	Optional By default, the timeout multiplier of the RSVP-TE message is 3.
Configure the refresh interval of the RSVP-TE message	**ip rsvp refresh-interval** *interval*	Optional By default, the refresh interval of the RSVP-TE message is 30s.

Configure RSVP-TE Message Confirm

To improve the reliability of the RSVP-TE message sending, RSVP-TE expands (RFC2961), that is, use the MESSAGE_ID object and MESSAGE_ID_ACK object to confirm the message.

Configuring the RSVP-TE message confirm includes:

- Enable the RSVP-TE message confirm capability: That is, permit sending the RSVP-TE request confirm message containing MESSAGE_ID object and ACK_Desired flag. Meanwhile, permit sending the RSVP-TE message containing the MESSAGE_ID_ACK object to confirm the request confirm message.
- Configure the timeout of the RSVP-TE message confirm. If the RSVP-TE request confirm message does not receive the confirm message within the timeout and the request confirm message type is PATH and RESV, re-transmit the message.

Both can be configured globally and also can be configured on the interface separately. The global configuration takes effect for all interfaces. If it is configured globally and on the specified

interface at the same time, the interface configuration is prior. Currently, support confirming the PATH message and ESV message.

Table 4-13 Configure the RSVP-TE message confirm

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the RSVP-TE configuration mode	**mpls traffic-eng tunnels**	-
Enable the confirming capability of the global RSVP-TE message	**message-ack**	Mandatory By default, do not enable the confirming capability of the global RSVP-TE message.
Configure the timeout of the global RSVP-TE message confirm	**ack-wait-timeout** *timeout-value*	Optional By default, the timeout of the global RSVP-TE message confirm is 10s.
Exit the RSVP-TE configuration mode	**exit**	-
Enter the interface configuration mode	**interface** *interface-name*	-
Enable the RSVP-TE message confirming capability of the interface	**ip rsvp message-ack**	Optional By default, do not enable the RSVP-TE message confirming capability of the interface
Configure the timsout of the interface RSVP-TE message confirm	**ip rsvp ack-wait-timeout** *timeout-value*	Optional By default, the timeout of the interface RSVP-TE message confirm is 10s.

Note:

- The RSVP-TE message confirm function can take effect only when the RSVP-TE message confirm capability is enabled on all interfaces between the neighbors.

Configure RSVP-TE Refresh Suppression

RSVP-TE refresh suppression (Refresh Reduction) mechanism uses the message summary, but not standard PATH message and RESV message to refresh the RSVP-TE status, so as to reduce the traffic of the RSVP-TE message in the network and reduce the processing load of the receiver for the RSVP-TE refresh message.

To configure the RSVP-TE refresh suppression function, it is necessary to enable the global RSVP-TE refresh suppression function, and then enable the interface RSVP-TE refresh suppression function on the specified interface.

Table 4-14 Configure RSVP-TE refresh suppression

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the RSVP-TE configuration mode	**mpls traffic-eng tunnels**	-
Enable the global RSVP-TE refresh suppression function	**refresh-reduction**	Mandatory By default, do not enable the global RSVP-TE refresh suppression function.
Exit the RSVP-TE configuration mode	**exit**	-
Enter the interface configuration mode	**interface** *interface-name*	-
Enable the RSVP-TE refresh suppression function of the interface	**ip rsvp refresh-reduction**	Optional By default, do not enable the RSVP-TE refresh suppression function of the interface.

Note:

- The function can take effect only when two neighbors enable the RSVP-TE refresh suppression function globally and on the interface.

Configure Route/Label Record

The route/label record function is configured based on each MPLS P2P TE tunnel or each MPLS P2MP TE profile. If the MPLS TE tunnel enables the route/label record function, add RRO (Record Route Object) in the PATH message and RESV message sent for the MPLS TE tunnel. In RRO, record the route/label information of each hop on the MPLS TE tunnel path.

The MPLS P2P TE tunnel enables the route/label record function in the Tunnel interface configuration mode. The MPLS P2MP TE tunnel enables the route/label record function in the referenced MPLS P2MP TE profile configuration mode.

Table 4-15 Configure the route/label record

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the Tunnel interface configuration mode	**interface tunnel** *tunnel-unit*	-
Enable the route/label record function of the MPLS P2P TE tunnel	**tunnel mpls traffic-eng record-route**	Mandatory By default, do not enable the route/label record function of the MPLS P2P TE tunnel.
Exit the Tunnel interface configuration mode	**exit**	-
Enter the MPLS P2MP TE profile configuration mode	**mpls traffic-eng p2mp-template** *template-name*	-
Enable the route/label record function of the MPLS P2MP TE profile	**tunnel mpls traffic-eng record-route**	Mandatory By default, do not enable the route/label record function of the MPLS P2MP TE profile.

Configure RSVP-TE Loop Detection

After enabling the RSVP-TE loop detection function, LSR compares the interface address of the received RSVP-TE message with the address in the RRO of the message. If there is the same address, regard that there is loop in the network and terminate the setup of the MPLS TE tunnel.

Table 4-16 Configure the RSVP-TE loop detection

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the RSVP-TE configuration mode	**mpls traffic-eng tunnels**	-
Enable the RSVP-TE loop detection function	**loop-detection**	Optional By default, enable the RSVP-TE loop detection function.

Note:

- The RSVP-TE loop detection function relies on RRO in the RSVP-TE message, so it is necessary to enable the route/label record function of the MPLS TE tunnel so that the loop detection of the MPLS TE tunnel can take effect.

Configure PHP Feature of the MPLS P2P TE Tunnel

The Egress node of the MPLS P2P TE tunnel distributes the implicit label (the label value is 3) to the penultimate node to realize PHP. The implicit null label will not be pressed to the label stack. In some cases, if the Egress node of the MPLS P2P TE tunnel needs to decide the QoS policy according to the EXP information in the label stack, configure to make the Egress node distribute the explicit null label (the label value is 0) to the penultimate node, the explicit null label will be pressed to the label stack, and the Egress node will directly pop up the explicit null label, so as to reserve the label stack information and simplify the processing of the Egress node.

Table 4-17 Configure the PHP feature of the MPLS P2P TE tunnel

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the RSVP-TE configuration mode	**mpls traffic-eng tunnels**	-
Configure the Egress node of the MPLS P2P TE tunnel to distribute the explicit null label to the penultimate node	**explicit-null**	Optional By default, the Egress node of the MPLS P2P TE tunnel distributes the implicit null label to the penultimate node.

Note:

- After configuring the PHP feature, it is necessary to re-set up or re-optimize the MPLS P2P TE tunnel so that it can take effect.
- The Egress node of the MPLS P2MP TE tunnel distributes the non-reserved label to the second-to-last hop, so the configuration does not take effect for the MPLS P2MP TE tunnel.

Configure MPLS P2P TE tunnel Re-optimizing

The MPLS P2P TE tunnel re-optimizing indicates that the tunnel head re-calculates the tunnel path according to the current network topology information for the setup MPLS P2P TE tunnel, so as to confirm one best path and transfer the tunnel to the path. The MPLS P2P TE tunnel re-optimizing uses MBB (Make-Before-Break) mechanism, so it will not affect the tunnel status and traffic forwarding.

MPLS P2P TE tunnel re-optimizing includes regular re-optimizing and manual re-optimizing. The manual re-optimizing is only applicable to the MPLS P2P TE tunnel. By default, all MPLS P2P TE tunnels are re-optimized regularly. Each MPLS P2P TE tunnel owns separate re-optimizing timer. The interval of the regular re-optimizing can be configured in a unified manner. In some application scenario, if not hoping the setup MPLS P2P TE tunnel is transferred to another path because of re-optimizing, you can disable the re-optimizing function of the specified tunnel, that is, lock the tunnel.

The MPLS P2P TE tunnel enables the tunnel lock function in the Tunnel interface configuration mode. The MPLS P2MP TE tunnel enables the tunnel lock function in the referenced MPLS P2MP TE profile configuration mode.

Table 4-18 Configure MPLS P2P TE tunnel re-optimizing

Step	Command	Description
Re-optimize the MPLS P2P TE tunnel manually	**mpls traffic-eng tunnels reoptimize tunnel** *tunnel-unit*	Optional
Enter the global configuration mode	**configure terminal**	-
Enter the RSVP-TE configuration mode	**mpls traffic-eng tunnels**	-
Configure the interval of re-optimizing the MPLS P2P TE tunnel	**reoptimize-interval** *interval*	Optional By default, the interval of re-optimizing the MPLS P2P TE tunnel is 3600s.
Exit the RSVP-TE configuration mode	**exit**	-

Step	Command	Description
Enter the Tunnel interface configuration mode	**interface tunnel** *tunnel-unit*	-
Enable the MPLS P2P TE tunnel lock function	**tunnel mpls traffic-eng lockdown**	Optional By default, the MPLS P2P TE tunnel does not enable the tunnel lock function.
Exit the Tunnel interface configuration mode	**exit**	-

Configure RSVP-TE Hello Mechanism

The Hello mechanism of RSVP-TE is used for keeping alive between neighbors, helpful for RSVP-TE to respond to the network change fast.

Table 4-19 Configure the RSVP-TE Hello mechanism

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the interface configuration mode	**interface** *interface-name*	-
Enable the RSVP-TE Hello message sending capability of the interface	**ip rsvp hello-signalling**	Mandatory By default, do not enable the RSVP-TE Hello message sending capability of the interface.
Configure the interval of sending the RSVP-TE Hello message	**ip rsvp hello-interval** *interval*	Optional By default, the interval of sending the RSVP-TE Hello message is 2s.
Configure the timeout of receiving the RSVP-TE Hello message	**ip rsvp hello-timeout** *timeout-value*	Optional By default, the timeout of receiving the RSVP-TE Hello message is 10s.

Note:

- The RSVP-TE Hello mechanism can take effect only after the RSVP-TE Hello message sending capability is enabled on the interfaces between the neighbors.
- The commands **ip rsvp hello-signalling** and **ip rsvp bfd-signalling** cannot be configured on the interface at the same time.
- The commands **ip rsvp hello-signalling** and **ip rsvp graceful-restart hello-signalling** cannot be configured on the interface at the same time.

Configure Auto Bandwidth Adjust of the MPLS P2P TE Tunnel

Auto bandwidth adjust of the MPLS P2P TE tunnel indicates that the tunnel head regularly monitors the traffic rate on the tunnel interface and adjusts the required bandwidth of the tunnel according to the monitoring result and corresponding rules, making it close to the actual rate of the traffic forwarded along the tunnel.

Configuring the auto bandwidth adjust of the MPLS P2P TE tunnel includes:

- Enable bandwidth collect timer: After enabling the timer, record the output rate of all MPLS P2P TE tunnels regularly (the MPLS P2P TE tunnel does not have input rate).
- Configure bandwidth collect frequency: The bandwidth collect frequency is the frequency executed by the bandwidth collect timer.
- Enable the auto bandwidth adjust function of the MPLS P2P TE tunnel.
- Configure the application frequency of the auto bandwidth adjust of the MPLS P2P TE tunnel: The application frequency of the auto bandwidth adjust indicates the frequency of regularly adjusting the MPLS P2P TE tunnel bandwidth
- Configure the minimum and maximum apply bandwidth of the auto bandwidth adjust of the MPLS P2P TE tunnel: The maximum and minimum apply bandwidth defines the upper threshold and lower threshold of the required bandwidth that can be adjusted automatically.
- Configure the non-apply bandwidth collection of the auto bandwidth adjust of the MPLS P2P TE tunnel: In some cases, you just need to get the current actual used bandwidth and bandwidth adjust calculation information of the MPLS P2P TE tunnel, but do not need to change the required bandwidth, so as to configure the non-apply bandwidth collection of the MPLS P2P TE tunnel.

Table 4-20 Configure the auto bandwidth adjust of the MPLS P2P TE tunnel

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the RSVP-TE configuration mode	**mpls traffic-eng tunnels**	-
Enable the bandwidth collecting timer	**auto-bw timers**	Mandatory By default, do not enable the bandwidth collecting timer.

Step	Command	Description
Configure the bandwidth collecting frequency	**auto-bw timers frequency** *collect-frequency*	Optional By default, the bandwidth collecting frequency is 300s/times.
Exit the RSVP-TE configuration mode	**exit**	-
Enter the Tunnel interface configuration mode	**interface tunnel** *tunnel-unit*	-
Enable the auto bandwidth adjusting function of the MPLS P2P TE tunnel	**tunnel mpls traffic-eng auto-bw**	Mandatory By default, do not enable the auto bandwidth adjust function of the MPLS P2P TE tunnel.
Configure the application frequency of the auto bandwidth adjust of the MPLS P2P TE tunnel and the maximum/minimum applicable bandwidth	**tunnel mpls traffic-eng auto-bw frequency** *apply-frequency* **max-bw** *max-bandwidth* **min-bw** *min-bandwidth*	Optional By default, the application frequency of the auto bandwidth adjust of the MPLS P2P TE tunnel is 86400s/times, the maximum and minimum applicable bandwidth are both 0lbps, indicating no limitation.
Configure the non-apply bandwidth collect of the auto bandwidth adjust of the MPLS P2P TE tunnel	**tunnel mpls traffic-eng auto-bw collect-bw**	Optional By default, the non-apply bandwidth collect of the auto bandwidth adjust of the MPLS P2P TE tunnel is not configured.

Note:

- First enable the bandwidth collect timer so that you can enable the auto bandwidth adjust function of the MPLS P2P TE tunnel and configure the apply frequency, maximum and minimum applicable bandwidth or non-apply bandwidth collect of the auto bandwidth adjust of the MPLS P2P TE tunnel.
- The latest auto bandwidth adjust of the MPLS P2P TE tunnel takes effect and the un-specified parameters are restored to the default values.

- The bandwidth collect frequency should be higher than the apply frequency of the auto bandwidth adjust of the MPLS P2P TE tunnel.
- The maximum applicable bandwidth of the auto bandwidth adjust of the MPLS P2P TE tunnel should be larger than the minimum applicable bandwidth.
- If the required bandwidth of the MPLS P2P TE tunnel is adjusted automatically, the corresponding configuration will change, but the configuration will be saved automatically.

Configure the Interval of Re-establishing the MPLS P2P TE Tunnel Regularly

The scheduled reconstruction interval is configured based on each MPLS P2P TE tunnel. After the tunnel state changes to down, a tunnel based timer will be started to periodically try to re-establish the tunnel. If the tunnel is not configured with a scheduled reconstruction interval, it will be periodically re-established at the default 30s interval until the tunnel is up; If the tunnel is configured with a scheduled reconstruction interval, the tunnel will be periodically re-established at the configured interval until the tunnel is up.

Table 4-21 Configure the interval of re-establishing the MPLS P2P TE tunnel regularly

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the Tunnel interface configuration mode	**interface tunnel** *tunnel-unit*	-
Configure the interval of re-establishing the MPLS P2P TE tunnel regularly	**tunnel mpls traffic-eng primary retry-timer** *timer*	Mandatory By default, do not configure the interval of re-establishing the MPLS P2P TE tunnel regularly.
Exit the Tunnel interface configuration mode	exit	-

4.2.5. Configure Traffic Forwarding of MPLS P2P TE tunnel

Configuration Condition

Before configuring the MPLS P2P TE tunnel traffic forwarding, first complete the following tasks:

- Configure the link layer protocol, ensuring the normal communication of the link layer
- Configure the network layer address of the interface, making the neighboring network nodes reachable at the network layer
- Configure IGP, ensuring the intercommunication of the LSRs at the network layer
- Configure MPLS basic functions, ensuring that the MPLS packet can be received and sent
- Configure MPLS TE basic functions.

- Configure MPLS P2P TE tunnel.

Configure Static Route to Make Traffic Be Forwarded along MPLS P2P TE tunnel

The simplest mode of making the traffic be forwarded along the MPLS P2P TE tunnel is to configure the static route. Configure one static route to the destination network address via the MPLS P2P TE tunnel so that the traffic can be imported to the MPLS P2P TE tunnel for forwarding.

For the details and configuration of the static route, refer to the unicast route configuration manual-the static route chapter.

Table 4-22 Configure the static route to make the traffic be forwarded along the MPLS P2P TE tunnel

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Configure egress interface as the static route of the MPLS P2P TE tunnel	**ip route** *destination-ip-address destination-mask* **tunnel** *tunnel-unit*	Mandatory

Configure Policy Route to Make Traffic Be Forwarded along MPLS P2P TE tunnel

Configure the policy route and specify its egress interface as the MPLS P2P TE tunnel to make the traffic matching the policy be forwarded along the MPLS P2P TE tunnel, so as to provide the QoS guarantee for the service. The work mode of the policy route with egress interface as the MPLS P2P TE tunnel is the same as the work mode of the policy route with egress interface as any other point-to-point interface.

Before configuring the policy route to make the traffic be forwarded along the MPLS P2P TE tunnel, first create the route map and set the match attributes, such as specify the interface matched by the route map or the route prefix. And then set the egress interface as the MPLS P2P TE tunnel in the route map, and at last, apply the policy route on the interface. In some cases, the match attribute of the route map depends on the ACL. Here, you also need to complete the ACL configuration.

For the details and configuration of the policy route and ACL, refer to the unicast route configuration manual-the policy route chapter and the security configuration-the ACL chapter. The manual does not describe the configuration.

Table 4-23 Configure the policy route to make the traffic be forwarded along the MPLS P2P TE tunnel

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the route map configuration mode	**route-map** *map-name*	-
Set the egress interface as the MPLS P2P TE tunnel	**set interface tunnel** *tunnel-unit*	Mandatory By default, do not set the egress interface as the MPLS P2P TE tunnel.

Configure Auto Route to Make Traffic Be Forwarded along MPLS P2P TE tunnel

Auto route is also called IGP Shortcut. Auto route just needs to be configured at the Ingress node of the MPLS P2P TE tunnel. After enabling the auto route function of the MPLS P2P TE tunnel, the Ingress node will take the MPLS P2P TE tunnel as one link interface to take part in the route calculation. According to the destination address of the MPLS P2P TE tunnel, use the MPLS P2P TE tunnel to replace the egress interface of the related route, so as to the traffic to the Egress node of the tunnel and after the Egress node be forwarded along the MPLS P2P TE tunnel.

Table 4-24 Configure the auto route be forwarded along the MPLS P2P TE tunnel

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the Tunnel interface configuration mode	**interface tunnel** *tunnel-unit*	-
Enable the auto route function of the MPLS P2P TE tunnel	**tunnel mpls traffic-eng autoroute announce**	Mandatory By default, do not enable the auto route function of the MPLS P2P TE tunnel.

Configure Forwarding Adjacency to Make Traffic Be Forwarded along MPLS P2P TE tunnel

Forwarding adjacency indicates that IGP takes the MPLS P2P TE tunnel as one network adjacency to advertise so that the MPLS P2P TE tunnel not only can be sensed and used by the Ingress node, bu also can be sensed by the node before the Ingress node of the MPLS P2P TE

tunnel and make it as one link to take part in the route calculation and generate the route with the egress interface as the MPLS P2P TE tunnel for traffic forwarding.

The MPLS P2P TE tunnel is uni-directional, so you should set up two MPLS P2P TE tunnels between two nodes to make the forwarding adjacency take effect, and enable the forwarding adjacency function on the MPLS P2P TE tunnels of the two nodes.

Table 4-25 Configure forwarding adjacency to make the traffic be forwarded along the MPLS P2P TE tunnel

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the Tunnel interface configuration mode	**interface tunnel** *tunnel-unit*	-
Enable the forwarding adjacency function of the MPLS P2P TE tunnel	**tunnel mpls traffic-eng forwarding-adjacency**	Mandatory By default, do not enable the forwarding adjacency function of the MPLS P2P TE tunnel.

Note:

- To avoid the repeated route calculation, it is suggested not to enable the auto route function and forwarding adjacency function on one MPLS P2P TE tunnel at the same time.
- The MPLS P2P TE tunnel metric advertised by the forwarding adjacency is the IGP route protocol metric of the MPLS P2P TE tunnel.

4.2.6. Configure Parameters of Affecting the Traffic Forwarding of MPLS P2P TE tunnel

Configuration Condition

Before configuring the parameters of the MPLS P2P TE tunnel traffic forwarding, first complete the following tasks:

- Configure the link layer protocol, ensuring the normal communication of the link layer
- Configure the network layer address of the interface, making the neighboring network nodes reachable at the network layer
- Configure IGP, ensuring the intercommunication of the LSRs at the network layer
- Configure MPLS basic functions, ensuring that the MPLS packet can be received and sent
- Configure MPLS TE basic functions.
- Configure MPLS P2P TE tunnel.

Configure Auto Route Metric of MPLS P2P TE tunnel

By default, the metric of the route generated by the auto route function of the MPLS P2P TE tunnel is the metric calculated by IGP. In some special cases, if hoping that the traffic is imported to the MPLS P2P TE tunnel for forwarding only when the IGP shortest path is unavailable, it is necessary to change the metric of the route generated by the auto route function of the MPLS P2P TE tunnel, making it larger than the metric of the IGP shortest path.

There are three modes to configure the metric of the route generated by the auto route function of the MPLS P2P TE tunnel:

- Configure the tunnel metric: Tunnel metric indicates the metric of the MPLS P2P TE tunnel in the route generated by the auto route function. If the route generated by the auto route function is to reach the node after the Egress node of the MPLS P2P TE tunnel, the metric of the route is the metric of the MPLS P2P TE tunnel plus the IGP metric from the Egress node to the destination node. The default value of the tunnel metric is the metric calculated by IGP.
- Configure the absolute metric: The absolute metric indicates the constant metric of the route generated by the auto route function. After configuring the absolute metric, even the route generated by the auto route function is is to reach the node after the Egress node of the MPLS P2P TE tunnel, the metric of the route is constantly the configured absolute metric.
- Configure the relative metric: The relative metric indicates the metric offset of the route generated by the auto route function. The relative metric can be negative. After configuring the relative metric, the metric calculated by IGP plus the relative metric is the metric of the route generated by the auto route function.

On one MPLS P2P TE tunnel, only one of the above three metric can take effect and the new metric configuration will replace the old metric configuration.

Table 4-26 Configure the auto route metric of the MPLS P2P TE tunnel

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the Tunnel interface configuration mode	**interface tunnel** *tunnel-unit*	-
Configure the tunnel metric of the auto route of the MPLS P2P TE tunnel	**tunnel mpls traffic-eng autoroute metric** *tunnel-metric*	Optional By default, the tunnel metric of the auto metric of the MPLS P2P TE tunnel is the metric calculated by IGP.

Step	Command	Description
Configure the absolute metric of the auto route of the MPLS P2P TE tunnel	**tunnel mpls traffic-eng autoroute metric absolute** *absolute-metric*	Optional By default, do not configure the absolute metric of the auto route of the MPLS P2P TE tunnel.
Configure the relative metric of the auto route of the MPLS P2P TE tunnel	**tunnel mpls traffic-eng autoroute metric relative** *relative-metric*	Optional By default, do not configure the relative metric of the auto route of the MPLS P2P TE tunnel.

Note:

- When the configured relative metric is negative and if the metric calculated by IGP plus the relative metric is smaller than or equal to 0, the metric of the route generated by the auto route function is set to 1.

Configure Load Share of MPLS P2P TE tunnel

The load share takes effect only when there are multiple MPLS P2P TE tunnels with the same destination. The load share of the MPLS P2P TE tunnel decides the share ratio of the tunnel forwarding traffic. By default, calculate the load share ratio of the tunnel according to the required bandwidth of the MPLS P2P TE tunnel. The larger the required bandwidth, the larger the share ratio.

Table 4-27 Configure the load share of the MPLS P2P TE tunnel

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the Tunnel interface configuration mode	**interface tunnel** *tunnel-unit*	-
Configure the load share of the MPLS P2P TE tunnel	**tunnel mpls traffic-eng load-share** *load-share-value*	Optional By default, do not configure the load share of the MPLS P2P TE tunnel.

Note:

- When the traffic share ratio calculated by using the configured load share of the MPLS P2P TE tunnel is not an integer, round it to an integer.

4.2.7. Configure RSVP-TE to Link with BFD

Configuration Condition

Before configuring RSVP-TE to link with BFD, first complete the following tasks:

- Configure the link layer protocol, ensuring the normal communication of the link layer
- Configure the network layer address of the interface, making the neighboring network nodes reachable at the network layer
- Configure IGP, ensuring the intercommunication of the LSRs at the network layer
- Configure MPLS basic functions, ensuring that the MPLS packet can be received and sent
- Configure MPLS TE basic functions.
- Configure MPLS TE tunnel.

Configure RSVP-TE to Link with BFD

BFD (Bidirectional Forwarding Detection) is one method of fast detecting the line status between two devices. After enabling the BFD detection between the RSVP-TE neighbor devices and if the line between the devices fails, BFD fast detects the fault and informs RSVP-TE, triggering RSVP-TE to re-set up the tunnel or switch over the tunnel.

The function of linking RSVP-TE with BFD is often used with the MPLS TE fast re-route. For the details and configuration of BFD, refer to the reliability configuration manual-the BFD chapter.

Table 4-28 Configure RSVP-TE to link with BFD

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the interface configuration mode	**interface** *interface-name*	-
Enable the interface RSVP-TE to link with BFD	**ip rsvp bfd-signalling**	Mandatory By default, do not enable the interface RSVP-TE to link with BFD.

Note:

- The function can take effect after enabling RSVP-TE to link with BFD on the interfaces at the two sides of the link.
- Do not permit configuring the commands **ip rsvp bfd-signalling** and **ip rsvp hello-signalling** on the interface.
- Do not permit configuring the commands ip rsvp bfd-signalling and ip rsvp graceful-restart hello-signalling on the interface.

4.2.8. Configure MPLS TE Fast Re-Route

Configuration Condition

Before configuring MPLS TE fast re-routing, first complete the following tasks:

- Configure the link layer protocol, ensuring the normal communication of the link layer
- Configure the network layer address of the interface, making the neighboring network nodes reachable at the network layer
- Configure IGP, ensuring the intercommunication of the LSRs at the network layer
- Configure MPLS basic functions, ensuring that the MPLS packet can be received and sent
- Configure MPLS TE basic functions.
- Configure active MPLS TE tunnel
- Configure standby MPLS P2P TE tunnel.

Configure MPLS TE Fast Re-Route

MPLS TE Fast Reroute is one partial protect technology for the MPLS P2P TE tunnel. When the link or node on the master tunnel path fails, the traffic will switch to the pre-setup standby tunnel for forwarding, so as to ensure that the traffic forwarding is not interrupted. Meanwhile, the Ingress node of the master tunnel will try to re-set up the master tunnel without removing the master tunnel. After re-setting up the master tunnel successfully, the traffic will be switched back to the master tunnel for forwarding. To fast detect the link or node fault, it is necessary to enable RSVP-TE to link with BFD on the interfaces at the two sides of the partial protected link.

There are two modes to realize the MPLS TE fast re-route: Detour and Bypass. Detour is also called One-to-One mode, that is, one standby tunnel can only protect one master tunnel. Bypass is also called Faciltiy, that is, one standby tunnel can protect multiple master tunnels. Currently, support the Bypass mode.

The standby tunnel set up by the Bypass mode of the MPLS TE fast re-route is called Bypass LSP. Bypass LSP needs to be configured manually or created automatically. The mode of configuring Bypass LSP manually is the same as the setup mode of other MPLS P2P TE tunnel. The Ingress node of Bypass LSP is called PLR (Point of Local Repair), and Egress node is called MP (Merge Point). To ensure that the MPLS TE fast re-route can protect the master tunnel successfully after the fault happens, it is necessary to avoid that the master tunnel and Bypass LSP coincide. Therefore, when using the manual configured Bypass LSP, configure the explicit path to specify the paths of the master tunnel and Bypass LSP. When using the auto created Bypass LSP, the Bypass LSP path will automatically ensure that it does not coincide with the path of the main tunnel.

MPLS TE fast re-route includes two networking modes, that is, link protect and node protect. Both have different protect ranges. On the path of the master tunnel, when there is no other node between PLR node and MP node, it is called link protect. The protect rang of the link protect is the link between the PLR node and the MP node. When there is one node between the PLR node and MP node, it is called node protect. The protect range of the node protect is the link between the PLR node and the next node, and the next node of the PLR node.

Some configuration contents are described in the previous chapters, such as configure MPLS explicit path, and configure RSVP-TE to link with BFD. Therefore, this chapter does not describe the configuration contents any more. For the complete configuration flow, refer to MPLS TE typical configuration example. Besides, the MPLS TE fast re-route also needs to be configured on the Ingress node and PLR node of the master tunnel.

On the Ingress node of the master tunnel, it is necessary to enable the fast re-route function of the master tunnel. The MPLS P2P TE tunnel enables the fast re-routing function of the active tunnel in the Tunnel interface configuration mode.

Table 4-29 Configure the MPLS TE fast re-route of the master tunnel Ingress node

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the Tunnel interface configuration mode	**interface tunnel** *tunnel-unit*	-
Enable the fast re-route function of the MPLS P2P TE tunnel	**tunnel mpls traffic-eng fast-reroute**	Mandatory By default, do not enable the fast re-route function of the MPLS P2P TE tunnel.
Exit the Tunnel interface configuration mode	**exit**	-

On the PLR node, when configuring the standby tunnel manually, it is necessary to bind the standby tunnel for the egress interface of the master tunnel. After the interface is bound with the standby tunnel, the standby tunnel will protect all master tunnels that pass the interface and enable the fast re-route function.

Table 4-30 Configure the MPLS TE fast re-route of the PLR node

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the interface configuration mode	**interface** *interface-name*	-
The interface is bound with the standby MPLS P2P TE tunnel.	**mpls traffic-eng backup-path tunnel** *tunnel-unit*	Mandatory By default, the interface is not bound with the standby MPLS P2P TE tunnel.

Note:

- The PLR node needs to use the RRO of the master tunnel to get the label information distributed by the MP node for the master tunnel. Therefore, after enabling the fast re-route function of the master tunnel, RSVP-TE will automatically enable the route/label record function of the master tunnel.
- Because PLR nodes need to use the RO of the standby tunnel to judge the protection mode for the active tunnel, RSVP-TE will automatically enable the route/label recording function of the standby tunnel after the interface binds the standby tunnel, but will not add corresponding configuration in the configuration of the standby tunnel.
- If the egress interface of the standby tunnel is the same as the bound interface, the active/standby binding calculation of the PLR node will fail.
- If the tunnel enables the fast re-route function, it cannot serve as the standby tunnel to bind.

Do not permit configuring the commands **mpls traffic-eng backup-path tunnel** and **ip rsvp graceful-restart hello-signalling** on the interface at the same time.

4.2.9. Configure MPLS TE GR

Configuration Condition

Before configuring the MPLS TE GR capability, first complete the following tasks:

- Configure the link layer protocol, ensuring the normal communication of the link layer
- Configure the network layer address of the interface, making the neighboring network nodes reachable at the network layer
- Configure IGP, ensuring the intercommunication of the LSRs at the network layer; the IGP protocol enables the GR capability
- Configure MPLS basic functions, ensuring that the MPLS packet can be received and sent
- Configure MPLS TE basic functions.

Configure MPLS TE GR

The MPLS forwarding plane is separate from the control plane. When the control plane becomes abnormal, MPLS TE GR reserves the MPLS label forwarding entry and the LSR still forwards the packet according to the entry, so as to ensure that the data transmission is not interrupted.

During the GR process, the devices in the MPLS network are divided to two roles:

- GR restarter: GR restart router, indicating the device with dual control cards that still can keep forwarding data when restarting the control layer protocol because the user switches over the control card manually or the device fails.
- GR helper: The neighbor of GR restarter, keeping the neighbor relationship with the restarted GR restarter and negotiating the GR capability with the GR restarter. After the GR restarter restarts, help it restore the forwarding status before restarting.

For the above two roles, MPLS TE GR has two work modes:

- full mode: fully support mode, it can serves as GR restarter and GR helper at the same time
- helper mode: It can only serve as GR helper.

The work process of MPLS TE GR is as follows:

- After the RSVP-TE neighbor is set up, negotiate the GR capability via the expanded RSVP-TE Hello message with the GR capability information,
- After the neighbor status between GR helper and GR restarter, GR helper will enable one restart timer. The timeout of the timer is the restart time advertised by GR restarter. Before restart timer times out, GR helper will reserve the RSVP-TE protocol status and MPLS label forwarding entry related with GR restarter. If the Hello message sent by GR restarter is re-received before the restart timer times out, GR helper stops the restart timer, and enables one recovery timer. The timeout of the timer is the recovery time advertised by GR restarter. After the restart timer times out, GR helper will delete the RSVP-TE protocol status and MPLS label forwarding entry related with GR restarter.
- If the Hello packet between GR helper and GR restarter does not time out, GR helper directly detects that the GR restarter is restarted via the received Hello packet, and will not enable the restart timer, but directly enables recovery timer. Before the recovery timer times out and if GR helper is the upstream neighbor of GR restarter, GR helper will periodically sends the PATH message with Recovery Label object to GR restarter. If GR helper is the downstream neighbor of GR restarter, GR helper will periodically send the Recovery PATH message to GR restarter.
- GR restarter restores the RSVP-TE protocol status and MPLS label forwarding entry according to the message sent by GR helper, and then GR helper updates the RSVP-TE protocol status and MPLS label forwarding entry according to the message sent by GR restarter. After the recovery timer times out, GR helper will delete the RSVP-TE protocol status and MPLS label forwarding entry related with GR restarter.

Table 4-31 Configure MPLS.TE.GR

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the RSVP-TE configuration mode	**mpls traffic-eng tunnels**	-
Enable the GR capability and configure the GR mode	**graceful-restart helper**	Mandatory
Configure the GR restart time	**graceful-restart restart-time** *restart-time-value*	Optional By default, the GR restart time is 120s.
Exit the RSVP-TE configuration mode	**exit**	-
Enter the interface configuration mode	**interface** *interface-name*	-

Step	Command	Description
Enable the capability of sending the RSVP-TE GR extended Hello message of the interface	**ip rsvp graceful-restart hello-signalling**	Mandatory By default, do not enable the capability of sending the RSVP-TE GR extended Hello message of the interface.
Configure the interval of sending the RSVP-TE GR extended Hello message of the interface	**ip rsvp graceful-restart hello-interval** *interval*	Optional By default, the interval of sending the RSVP-TE GR extended Hello message of the interface is 10s.
Configure the timeout of receiving the RSVP-TE GR extended Hello message of the interface	**ip rsvp graceful-restart hello-timeout** *timeout-value*	Optional By default, the timeout of receiving the RSVP-TE GR extended Hello message of the interface is 40s.

Note:

- The full mode of MPLS TE GR can only be configured on the device with dual control.
- MPLS TE GR only supports the MPLS P2P TE tunnel.
- Do not configure the commands **ip rsvp graceful-restart hello-signalling** and **ip rsvp hello-signalling** on the interface at the same time.
- Do not configure the commands **ip rsvp graceful-restart hello-signalling** and **ip rsvp bfd-signalling** on the interface at the same time.
- Do not configure the commands ip rsvp graceful-restart hello-signalling and mpls traffic-eng backup-path tunnel on the interface at the same time.

4.2.10. MPLS TE Monitoring and Maintaining

Table 4-32 MPLS TE Monitoring and Maintaining

Command	Description
clear mpls traffic-eng error-statistics	Clear the MPLS TE error statistics information
clear mpls traffic-eng statistics	Clear the MPLS TE statistics information

Command	Description
show mpls traffic-eng autoroute [*dst-ip-address*]	Display the auto route information of MPLS TE
show mpls traffic-eng debugging	Display the MPLS TE debugging switch information
show mpls traffic-eng error-statistics	Display the MPLS TE error statistics information
show mpls traffic-eng explicit-path [*path-name*]	Display the MPLS TE explicit path information
show mpls traffic-eng forwarding-adjacency [*dst-ip-address*]	Display the MPLS TE forwarding adjacency information
show mpls traffic-eng graceful-restart [**neighbor**]	Display the MPLS TE GR information
show mpls traffic-eng interface [*interface-name*]	Display the MPLS TE information of the interface
show mpls traffic-eng memory	Display the memory status information of the RSVP-TE protocol
show mpls traffic-eng neighbor	Display the RSVP-TE neighbor information
show mpls traffic-eng statistics	Display the statistics information of the received and sent RSVP-TE packets
show mpls traffic-eng summary	Display the summary information of the RSVP-TE protocol
show mpls traffic-eng topology [**brief** | *ip-address* [**brief**] | **igp-id** { **isis** *nsap-address-id* [**brief**] | **ospf** *ip-address-id* [**brief** | **network** [**brief**] | **router** [**brief**]] }]	Display the network topology information of MPLS TE
show mpls traffic-eng topology path [**destination** *ip-address* | **tunnel** *tunnel-unit*]	Display the CSPF path calculation information of the MPLS TE tunnel

Command	Description
show mpls traffic-eng tunnels [**tunnel** *tunnel-unit* | **ingress** | **transit** | **egress** | **from** *source-ip-address* | **to** *destination-ip-address*]	Display the details of the MPLS P2P TE tunnel
show mpls traffic-eng tunnels summary	Display the summary information of the MPLS P2P TE tunnel
show mpls traffic-eng version	Display the RSVP-TE software version information

4.3. MPLS TE Typical Configuration Example

4.3.1. Configure MPLS TE Basic Functions Based on OSPF

Network Requirements

- All devices run the OSPF protocol. Device1, Device2, and Device3 enable the TE OSPF scalability.
- Use RSVP-TE to create the MPLS P2P TE tunnel along Device1→Device2→Device3 and Device3→Device2→Device1, the the required bandwidth of the tunnel is 1000 kbps, and maximum reserved bandwidth of the link passed by the MPLS P2P TE tunnel is 100000 kbps.
- On Device1 and Device3, configure the MPLS TE auto route, making the data traffic between Device4 and Device5 be forwarded along the MPLS P2P TE tunnel.

Network Topology

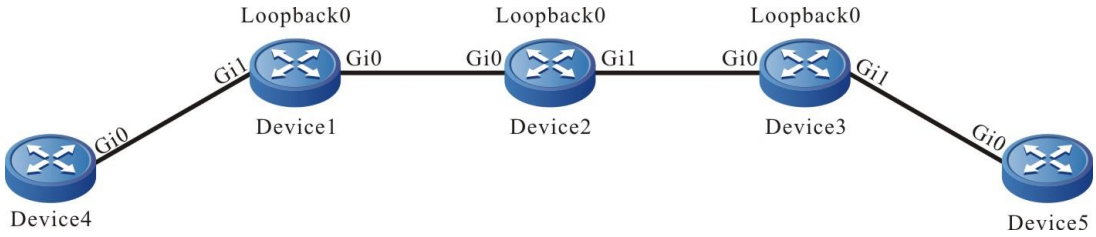

Figure 4-1 Networking of configuring the MPLS TE basic functions based on OSPF

Device	Interface	IP Address	Device	Interface	IP Address
Device1	Gi0	10.1.1.1/24	Device3	Gi0	20.1.1.2/24
	Gi1	100.1.1.1/24		Gi1	110.1.1.1/24
	Loopback0	1.1.1.1/32		Loopback0	3.3.3.3/32
Device2	Gi0	10.1.1.2/24	Device4	Gi0	100.1.1.2/24

Device	Interface	IP Address	Device	Interface	IP Address
	Gi1	20.1.1.1/24	Device5	Gi0	110.1.1.2/24
	Loopback0	2.2.2.2/32			

Configuration Steps

Step 1: Configure the IP address of the interface (omitted).

Step 2: Configure the OSPF protocol, all interfaces are covered to area 0, and area 0 of Device1, Device2, and Device3 enables the MPLS TE capability.

#Configure Device1.

```
Device1#configure terminal
Device1(config)#router ospf 100
Device1(config-ospf)#router-id 1.1.1.1
Device1(config-ospf)#network 10.1.1.0 0.0.0.255 area 0
Device1(config-ospf)#network 100.1.1.0 0.0.0.255 area 0
Device1(config-ospf)#network 1.1.1.1 0.0.0.0 area 0
Device1(config-ospf)#mpls traffic-eng router-id 1.1.1.1
Device1(config-ospf)#mpls traffic-eng area 0
Device1(config-ospf)#exit
```

#Configure Device2.

```
Device2#configure terminal
Device2(config)#router ospf 100
Device2(config-ospf)#router-id 2.2.2.2
Device2(config-ospf)#network 10.1.1.0 0.0.0.255 area 0
Device2(config-ospf)#network 20.1.1.0 0.0.0.255 area 0
Device2(config-ospf)#network 2.2.2.2 0.0.0.0 area 0
Device2(config-ospf)#mpls traffic-eng router-id 2.2.2.2
Device2(config-ospf)#mpls traffic-eng area 0
Device2(config-ospf)#exit
```

#Configure Device3

```
Device3#configure terminal
Device3(config)#router ospf 100
Device3(config-ospf)#router-id 3.3.3.3
Device3(config-ospf)#network 20.1.1.0 0.0.0.255 area 0
Device3(config-ospf)#network 110.1.1.0 0.0.0.255 area 0
Device3(config-ospf)#network 3.3.3.3 0.0.0.0 area 0
```

```
Device3(config-ospf)#mpls traffic-eng router-id 3.3.3.3
Device3(config-ospf)#mpls traffic-eng area 0
Device3(config-ospf)#exit
```

#Configure Device4.

```
Device4#configure terminal
Device4(config)#router ospf 100
Device4(config-ospf)#router-id 4.4.4.4
Device4(config-ospf)#network 100.1.1.0 0.0.0.255 area 0
Device4(config-ospf)#exit
```

#Configure Device5.

```
Device5#configure terminal
Device5(config)#router ospf 100
Device5(config-ospf)#router-id 5.5.5.5
Device5(config-ospf)#network 110.1.1.0 0.0.0.255 area 0
Device5(config-ospf)#exit
```

Step 3: Enable the MPLS TE function and MPLS forwarding capability. Meanwhile, configure the maximum reserved bandwidth of the link passed by the MPLS P2P TE tunnel.

#Configure Device1, enable the MPLS TE function and MPLS forwarding capability globally and on the interface gigabitethernet0, and configure the maximum reserved bandwidth of the link on the interface gigabitethernet0 as 100000 kbps.

```
Device1(config)#mpls ip
Device1(config)#mpls traffic-eng tunnels
Device1(config-rsvp-te)#router-id 1.1.1.1
Device1(config-rsvp-te)#exit
Device1(config)#interface gigabitethernet 0
Device1(config-if-gigabitethernet0)#mpls ip
Device1(config-if-gigabitethernet0)#mpls traffic-eng tunnels
Device1(config-if-gigabitethernet0)#ip rsvp bandwidth 100000
Device1(config-if-gigabitethernet0)#exit
```

#Configure Device2, enable the MPLS TE function and MPLS forwarding capability globally and on the interface gigabitethernet0, gigabitethernet1, and configure the maximum reserved bandwidth of the link on the interface gigabitethernet0, gigabitethernet1 as 100000 kbps.

```
Device2(config)#mpls ip
Device2(config)#mpls traffic-eng tunnels
Device2(config-rsvp-te)#router-id 2.2.2.2
Device2(config-rsvp-te)#exit
```

```
Device2(config)#interface gigabitethernet 0
Device2(config-if-gigabitethernet0)#mpls ip
Device2(config-if-gigabitethernet0)#mpls traffic-eng tunnels
Device2(config-if-gigabitethernet0)#ip rsvp bandwidth 100000
Device2(config-if-gigabitethernet0)#exit
Device2(config)#interface gigabitethernet 1
Device2(config-if-gigabitethernet1)#mpls ip
Device2(config-if-gigabitethernet1)#mpls traffic-eng tunnels
Device2(config-if-gigabitethernet1)#ip rsvp bandwidth 100000
Device2(config-if-gigabitethernet1)#exit
```

#Configure Device3, enable the MPLS TE function and MPLS forwarding capability globally and on the interface gigabitethernet0, and configure the maximum reserved bandwidth of the link on the interface gigabitethernet0 as 100000 kbps.

```
Device3(config)#mpls ip
Device3(config)#mpls traffic-eng tunnels
Device3(config-rsvp-te)#router-id 3.3.3.3
Device3(config-rsvp-te)#exit
Device3(config)#interface gigabitethernet 0
Device3(config-if-gigabitethernet0)#mpls ip
Device3(config-if-gigabitethernet0)#mpls traffic-eng tunnels
Device3(config-if-gigabitethernet0)#ip rsvp bandwidth 100000
Device3(config-if-gigabitethernet0)#exit
```

Step 4: Create one MPLS P2P TE tunnel.

#Configure Device1, create one MPLS P2P TE tunnel Tunnel1, and configure the required bandwidth of the tunnel as 1000kbps.

```
Device1(config)#interface tunnel 1
Device1(config-if-tunnel1)#tunnel mode mpls traffic-eng
Device1(config-if-tunnel1)#ip unnumbered loopback 0
Device1(config-if-tunnel1)#tunnel destination 3.3.3.3
Device1(config-if-tunnel1)#tunnel mpls traffic-eng bandwidth 1000
Device1(config-if-tunnel1)#exit
```

#Configure Device3, create one MPLS P2P TE tunnel Tunnel1, and configure the required bandwidth of the tunnel as 1000kbps.

```
Device3(config)#interface tunnel 1
Device3(config-if-tunnel1)#tunnel mode mpls traffic-eng
Device3(config-if-tunnel1)#ip unnumbered loopback 0
Device3(config-if-tunnel1)#tunnel destination 1.1.1.1
Device3(config-if-tunnel1)#tunnel mpls traffic-eng bandwidth 1000
```

```
Device3(config-if-tunnel1)#exit
```

#View the details of the MPLS P2P TE tunnel on Device1.

```
Device1#show mpls traffic-eng tunnels tunnel 1

*Tunnel 1  (Device1_t1)              Destination: 3.3.3.3
  Status:
    Admin: UP      Oper: UP (Using Primary LSP)   Signalling: Connected

  Config Parameters:
    Reoptimize: Enabled  interval: 3600 seconds
    Update type: Make-before-break
    Auto Route:  Disabled
    Forwarding adjacency:  Disabled
    Bandwidth: 1m       Setup-priority: 7  Hold-priority: 0
    Affinity: include-any 0x0, include-all 0x0, exclude-any 0x0
    Explicit path: None
    Record route: Disabled
    auto-bw: Disabled
    Fast-reroute:  Disabled

  Tunnel Out-Label: 24016   gigabitethernet0

  RSVP-TE Signalling Info:
    Primary LSP:
 From 1.1.1.1,   To 3.3.3.3,   Tunnel-Id 1,   LSP-Id 1
       Status:  UP
       RSVP-TE Path Info:
          Explicit Route:  10.1.1.2       20.1.1.2
          Tspec: average rate 1m, burst rate 1m, peak rate 0
          Bandwidth: 1m       Setup-priority: 7  Hold-priority: 0
          Affinity: include-any 0x0, include-all 0x0, exclude-any 0x0
       RSVP-TE Resv Info:
          Record Route:
          Fspec: average rate 1m, burst rate 1m, peak rate 0
          Out-Label: 24016   gigabitethernet0
          LSP Minimum MTU: 1500
```

```
Other Info:
  Tunnel created:     0 hour 30 minutes 15 seconds
  Current LSP Uptime: 0 hour 30 minutes 15 seconds
```

You can see that Tunnel1 is set up successfully on Device1, the status is UP, the egress label of the tunnel is 24016, and the egress interface is gigabitethernet0.

#View the details of the MPLS P2P TE tunnel on Device3.

```
Device3#show mpls traffic-eng tunnels tunnel 1

*Tunnel 1  (Device3_t1)              Destination: 1.1.1.1
 Status:
   Admin: UP      Oper: UP (Using Primary LSP)   Signalling: Connected

 Config Parameters:
   Reoptimize: Enabled  interval: 3600 seconds
   Update type: Make-before-break
   Auto Route:  Disabled
   Forwarding adjacency:  Disabled
   Bandwidth: 1m       Setup-priority: 7  Hold-priority: 0
   Affinity: include-any 0x0, include-all 0x0, exclude-any 0x0
   Explicit path: None
   Record route: Disabled
   auto-bw: Disabled
   Fast-reroute:  Disabled

 Tunnel Out-Label: 24017   gigabitethernet0

 RSVP-TE Signalling Info:
  Primary LSP:
     From 3.3.3.3,   To 1.1.1.1,   Tunnel-Id 1,   LSP-Id 1
     Status:  UP
     RSVP-TE Path Info:
        Explicit Route:  20.1.1.1       10.1.1.1
        Tspec: average rate 1m, burst rate 1m, peak rate 0
        Bandwidth: 1m       Setup-priority: 7  Hold-priority: 0
        Affinity: include-any 0x0, include-all 0x0, exclude-any 0x0
     RSVP-TE Resv Info:
        Record Route:
```

```
Fspec: average rate 1m, burst rate 1m, peak rate 0
Out-Label: 24017   gigabitethernet0
LSP Minimum MTU: 1500


Other Info:
  Tunnel created:    0 hour 17 minutes 18 seconds
  Current LSP Uptime: 0 hour 17 minutes 18 seconds
```

Similarly, Tunnel1 is set up successfully on Device3, the status is UP, the egress label of the tunnel is 24017, and the egress interface is gigabitethernet0.

Step 5: Configure the MPLS TE auto route.

#Configure Device1.

```
Device1(config)#interface tunnel 1
Device1(config-if-tunnel1)#tunnel mpls traffic-eng autoroute announce
Device1(config-if-tunnel1)#exit
```

#Configure Device3

```
Device3(config)#interface tunnel 1
Device3(config-if-tunnel1)#tunnel mpls traffic-eng autoroute announce
Device3(config-if-tunnel1)#exit
```

#View the route information on Device1.

```
Device1#show ip route
Codes: C - Connected, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
    U - Per-user Static route
    O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external


C   10.1.1.0/24 is directly connected, 02:01:51, gigabitethernet0
O   20.1.1.0/24 [110/2] via 10.1.1.2, 01:25:57, gigabitethernet0
C   100.1.1.0/24 is directly connected, 02:00:40, gigabitethernet1
O   110.1.1.0/24 [110/3] is directly connected, 00:00:05, tunnel1
C   127.0.0.0/8 is directly connected, 05:01:22, lo0
C   1.1.1.1/32 is directly connected, 04:26:39, loopback0
O   2.2.2.2/32 [110/2] via 10.1.1.2, 01:25:52, gigabitethernet0
O   3.3.3.3/32 [110/3] is directly connected, 00:00:05, tunnel1
```

The egress interfaces of the routes 110.1.1.0/24 and 3.3.3.3/32 advertised by the Egress node of the tunnel Device3 both point to Tunnel1.

#View the route information on Device3.

```
Device3#show ip route
Codes: C - Connected, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
    U - Per-user Static route
    O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external



O   10.1.1.0/24 [110/2] via 20.1.1.1, 01:20:25, gigabitethernet0
C   20.1.1.0/24 is directly connected, 02:01:46, gigabitethernet0
O   100.1.1.0/24 [110/3] is directly connected, 00:00:14, tunnel1
C   110.1.1.0/24 is directly connected, 02:01:34, gigabitethernet1
C   127.0.0.0/8 is directly connected, 04:57:18, lo0
O   1.1.1.1/32 [110/3] is directly connected, 00:00:14, tunnel1
O   2.2.2.2/24 [110/2] via 20.1.1.1, 01:20:23, gigabitethernet0
C   3.3.3.3/32 is directly connected, 04:26:43, loopback0
```

Similarly, the egress interfaces of the routes 100.1.1.0/24 and 1.1.1.1/32 advertised by the Egress node of the tunnel Device1 both point to Tunnel1.

Step 6: Check the result.

#On Device4, use the ping command to check the connectivity with Device5.

```
Device4#ping 110.1.1.2

Press key (ctrl + shift + 6) interrupt it.
Sending 5, 76-byte ICMP Echos to 110.1.1.2 , timeout is 2 seconds:
!!!!!
Success rate is 100% (5/5). Round-trip min/avg/max = 0/0/0 ms.
```

On Device5, use the ping command to check the connectivity with Device4.

```
Device5#ping 100.1.1.2

Press key (ctrl + shift + 6) interrupt it.
Sending 5, 76-byte ICMP Echos to 100.1.1.2 , timeout is 2 seconds:
!!!!!
Success rate is 100% (5/5). Round-trip min/avg/max = 0/0/0 ms.
```

Device4 and Device5 can ping each other.

#On Device1, view the MPLS forwarding information.

```
Device1#show mpls forwarding-table
```

```
Pro: L - LDP, O - OSPF, B - MP-BGP, R - RSVP, M - Mapped-Route, S - Static
Label,ML - mLDP (ML FEC: Root address/OT/OV), RM - RSVP P2MP (RM FEC: P2MP
ID/TID)

Pro Ident       FEC             Inlabel Outlabel Outgoing       Next hop
R   -TNL-       tunnel1         /       24016   gigabitethernet0 10.1.1.2
```

According to the packet statistics (TxPkts) of the MPLS forwarding table, the ICMP request packets and response packets of Device4 are forwarded along the MPLS P2P TE tunnel.

#On Device3, view the MPLS forwarding information.

```
Device3#show mpls forwarding-table
Pro: L - LDP, O - OSPF, B - MP-BGP, R - RSVP, M - Mapped-Route, S - Static
Label,ML - mLDP (ML FEC: Root address/OT/OV), RM - RSVP P2MP (RM FEC: P2MP
ID/TID)

Pro Ident       FEC             Inlabel Outlabel Outgoing       Next hop
R   -TNL-       tunnel1         /       24017   gigabitethernet0 20.1.1.1
```

Similarly, according to the packet statistics information, the ICMP request packets and response packets of Device54 are forwarded along the MPLS P2P TE tunnel.

Therefore, it indicates that the data traffic between Device4 and Device5 is forwarded along the MPLS P2P TE tunnel.

4.3.2. Configure MPLS TE Basic Functions Based on IS-IS

Network Requirements

- All devices run the OSPF protocol. Device1, Device2, and Device3 enable the TE OSPF scalability.
- Use RSVP-TE to create the MPLS P2P TE tunnel along Device1→Device2→Device3 and Device3→Device2→Device1, the required bandwidth of the tunnel is 1000 kbps, and maximum reserved bandwidth of the link passed by the MPLS P2P TE tunnel is 100000 kbps.
- On Device1 and Device3, configure the static route, making the data traffic between Device4 and Device5 be forwarded along the MPLS P2P TE tunnel.

Network Topology

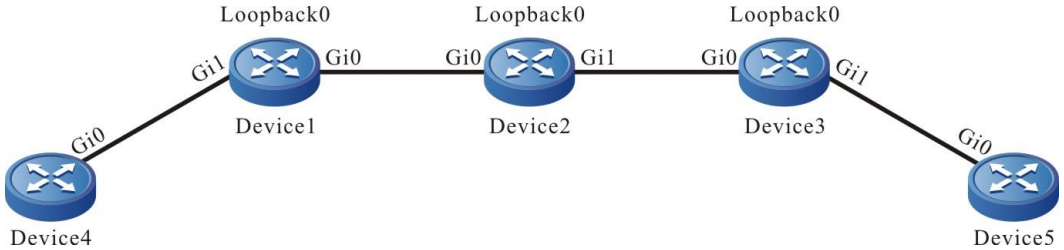

Figure 4-2 Configure the MPLS TE basic functions based on IS-IS

Device	Interface	IP Address	Device	Interface	IP Address
Device1	Gi0	10.1.1.1/24	Device3	Gi0	20.1.1.2/24
	Gi1	100.1.1.1/24		Gi1	110.1.1.1/24
	Loopback0	1.1.1.1/32		Loopback0	3.3.3.3/32
Device2	Gi0	10.1.1.2/24	Device4	Gi0	100.1.1.2/24
	Gi1	20.1.1.1/24	Device5	Gi0	110.1.1.2/24
	Loopback0	2.2.2.2/32			

Configuration Steps

Step 1: Configure the IP address of the interface (omitted).

Step 2: Configure the IS-IS protocol, all interfaces are covered to Level-2, and Level-2 of Device1, Device2, and Device3 enables the MPLS TE capability.

#Configure Device1.

```
Device1#configure terminal
Device1(config)#router isis 100
Device1(config-isis)#is-type level-2
Device1(config-isis)#net 00.0001.0000.0000.0001.00
Device1(config-isis)#metric-style wide
Device1(config-isis)#address-family ipv4 unicast
Device1(config-isis-af)#mpls traffic-eng level-2
Device1(config-isis-af)#mpls traffic-eng router-id 1.1.1.1
Device1(config-isis-af)#exit
Device1(config-isis)#exit
Device1(config)#interface gigabitethernet 0
Device1(config-if-gigabitethernet0)#ip router isis 100
Device1(config-if-gigabitethernet0)#exit
Device1(config)#interface gigabitethernet 1
Device1(config-if-gigabitethernet1)#ip router isis 100
Device1(config-if-gigabitethernet1)#exit
Device1(config)#interface loopback 0
Device1(config-if-loopback0)#ip router isis 100
Device1(config-if-loopback0)#exit
```

#Configure Device2.

```
Device2#configure terminal
Device2(config)#router isis 100
Device2(config-isis)#is-type level-2
Device2(config-isis)#net 00.0001.0000.0000.0002.00
Device2(config-isis)#metric-style wide
Device2(config-isis)#address-family ipv4 unicast
Device2(config-isis-af)#mpls traffic-eng level-2
Device2(config-isis-af)#mpls traffic-eng router-id 2.2.2.2
Device2(config-isis-af)#exit
Device2(config-isis)#exit
Device2(config)#interface gigabitethernet 0
Device2(config-if-gigabitethernet0)#ip router isis 100
Device2(config-if-gigabitethernet0)#exit
Device2(config)#interface gigabitethernet 1
Device2(config-if-gigabitethernet1)#ip router isis 100
Device2(config-if-gigabitethernet1)#exit
Device2(config)#interface loopback 0
Device2(config-if-loopback0)#ip router isis 100
Device2(config-if-loopback0)#exit
```

#Configure Device3

```
Device3#configure terminal
Device3(config)#router isis 100
Device3(config-isis)#is-type level-2
Device3(config-isis)#net 00.0001.0000.0000.0003.00
Device3(config-isis)#metric-style wide
Device3(config-isis)#address-family ipv4 unicast
Device3(config-isis-af)#mpls traffic-eng level-2
Device3(config-isis-af)#mpls traffic-eng router-id 3.3.3.3
Device3(config-isis-af)#exit
Device3(config-isis)#exit
Device3(config)#interface gigabitethernet 0
Device3(config-if-gigabitethernet0)#ip router isis 100
Device3(config-if-gigabitethernet0)#exit
Device3(config)#interface gigabitethernet 1
Device3(config-if-gigabitethernet1)#ip router isis 100
Device3(config-if-gigabitethernet1)#exit
```

```
Device3(config)#interface loopback 0
Device3(config-if-loopback0)#ip router isis 100
Device3(config-if-loopback0)#exit
```

#Configure Device4.

```
Device4#configure terminal
Device4(config)#router isis 100
Device4(config-isis)#is-type level-2
Device4(config-isis)#net 00.0001.0000.0000.0004.00
Device4(config-isis)#metric-style wide
Device4(config-isis)#exit
Device4(config)#interface gigabitethernet 0
Device4(config-if-gigabitethernet0)#ip router isis 100
Device4(config-if-gigabitethernet0)#exit
```

#Configure Device5.

```
Device5#configure terminal
Device5(config)#router isis 100
Device5(config-isis)#is-type level-2
Device5(config-isis)#net 00.0001.0000.0000.0005.00
Device5(config-isis)#metric-style wide
Device5(config-isis)#exit
Device5(config)#interface gigabitethernet 0
Device5(config-if-gigabitethernet0)#ip router isis 100
Device5(config-if-gigabitethernet0)#exit
```

Step 3: Enable the MPLS TE function and MPLS forwarding capability. Meanwhile, configure the maximum reserved bandwidth of the link passed by the MPLS P2P TE tunnel.

#Configure Device1, enable the MPLS TE function and MPLS forwarding capability globally and on the interface gigabitethernet0, and configure the maximum reserved bandwidth of the link on the interface gigabitethernet0 as 100000 kbps.

```
Device1(config)#mpls ip
Device1(config)#mpls traffic-eng tunnels
Device1(config-rsvp-te)#router-id 1.1.1.1
Device1(config-rsvp-te)#exit
Device1(config)#interface gigabitethernet 0
Device1(config-if-gigabitethernet0)#mpls ip
Device1(config-if-gigabitethernet0)#mpls traffic-eng tunnels
Device1(config-if-gigabitethernet0)#ip rsvp bandwidth 100000
Device1(config-if-gigabitethernet0)#exit
```

#Configure Device2, enable the MPLS TE function and MPLS forwarding capability globally and on the interface gigabitethernet0, gigabitethernet1, and configure the maximum reserved bandwidth of the link on the interface gigabitethernet0, gigabitethernet1 as 100000 kbps.

```
Device2(config)#mpls ip
Device2(config)#mpls traffic-eng tunnels
Device2(config-rsvp-te)#router-id 2.2.2.2
Device2(config-rsvp-te)#exit
Device2(config)#interface gigabitethernet 0
Device2(config-if-gigabitethernet0)#mpls ip
Device2(config-if-gigabitethernet0)#mpls traffic-eng tunnels
Device2(config-if-gigabitethernet0)#ip rsvp bandwidth 100000
Device2(config-if-gigabitethernet0)#exit
Device2(config)#interface gigabitethernet 1
Device2(config-if-gigabitethernet1)#mpls ip
Device2(config-if-gigabitethernet1)#mpls traffic-eng tunnels
Device2(config-if-gigabitethernet1)#ip rsvp bandwidth 100000
Device2(config-if-gigabitethernet1)#exit
```

#Configure Device3, enable the MPLS TE function and MPLS forwarding capability globally and on the interface gigabitethernet0, and configure the maximum reserved bandwidth of the link on the interface gigabitethernet0 as 100000 kbps.

```
Device3(config)#mpls ip
Device3(config)#mpls traffic-eng tunnels
Device3(config-rsvp-te)#router-id 3.3.3.3
Device3(config-rsvp-te)#exit
Device3(config)#interface gigabitethernet 0
Device3(config-if-gigabitethernet0)#mpls ip
Device3(config-if-gigabitethernet0)#mpls traffic-eng tunnels
Device3(config-if-gigabitethernet0)#ip rsvp bandwidth 100000
Device3(config-if-gigabitethernet0)#exit
```

Step 4: Create one MPLS P2P TE tunnel.

#Configure Device1, create one MPLS P2P TE tunnel Tunnel1, and configure the required bandwidth of the tunnel as 1000kbps.

```
Device1(config)#interface tunnel 1
Device1(config-if-tunnel1)#tunnel mode mpls traffic-eng
Device1(config-if-tunnel1)#ip unnumbered loopback 0
Device1(config-if-tunnel1)#tunnel destination 3.3.3.3
Device1(config-if-tunnel1)#tunnel mpls traffic-eng bandwidth 1000
```

```
Device1(config-if-tunnel1)#exit
```

#Configure Device3, create one MPLS P2P TE tunnel Tunnel1, and configure the required bandwidth of the tunnel as 1000kbps.

```
Device3(config)#interface tunnel 1
Device3(config-if-tunnel1)#tunnel mode mpls traffic-eng
Device3(config-if-tunnel1)#ip unnumbered loopback 0
Device3(config-if-tunnel1)#tunnel destination 1.1.1.1
Device3(config-if-tunnel1)#tunnel mpls traffic-eng bandwidth 1000
Device3(config-if-tunnel1)#exit
```

#View the details of the MPLS P2P TE tunnel on Device1.

```
Device1#show mpls traffic-eng tunnels tunnel 1

*Tunnel 1  (Device1_t1)              Destination: 3.3.3.3
  Status:
    Admin: UP      Oper: UP (Using Primary LSP)   Signalling: Connected

  Config Parameters:
    Reoptimize: Enabled  interval: 3600 seconds
    Update type: Make-before-break
    Auto Route:  Disabled
    Forwarding adjacency:  Disabled
    Bandwidth: 1m       Setup-priority: 7  Hold-priority: 0
    Affinity: include-any 0x0, include-all 0x0, exclude-any 0x0
    Explicit path: None
    Record route: Disabled
    auto-bw: Disabled
    Fast-reroute:  Disabled

  Tunnel Out-Label: 24016   gigabitethernet0

  RSVP-TE Signalling Info:
 Primary LSP:
      From 1.1.1.1,   To 3.3.3.3,   Tunnel-Id 1,   LSP-Id 2
      Status:  UP
      RSVP-TE Path Info:
        Explicit Route:  10.1.1.2       20.1.1.2
        Tspec: average rate 1m, burst rate 1m, peak rate 0
```

```
    Bandwidth: 1m       Setup-priority: 7  Hold-priority: 0
    Affinity: include-any 0x0, include-all 0x0, exclude-any 0x0
  RSVP-TE Resv Info:
    Record Route:
    Fspec: average rate 1m, burst rate 1m, peak rate 0
    Out-Label: 24016   gigabitethernet0
    LSP Minimum MTU: 1500

 Other Info:
   Tunnel created:    18 hours 36 minutes 15 seconds
   Current LSP Uptime: 0 hour 1 minute 47 seconds
```

You can see that Tunnel1 is set up successfully on Device1, the status is UP, the egress label of the tunnel is 24016, and the egress interface is gigabitethernet0.

#View the details of the MPLS P2P TE tunnel on Device3.

```
Device3#show mpls traffic-eng tunnels tunnel 1

*Tunnel 1  (Device3_t1)              Destination: 1.1.1.1
 Status:
   Admin: UP      Oper: UP (Using Primary LSP)   Signalling: Connected

 Config Parameters:
   Reoptimize: Enabled  interval: 3600 seconds
   Update type: Make-before-break
   Auto Route:  Disabled
   Forwarding adjacency:  Disabled
   Bandwidth: 1m       Setup-priority: 7  Hold-priority: 0
   Affinity: include-any 0x0, include-all 0x0, exclude-any 0x0
   Explicit path: None
   Record route: Disabled
   auto-bw: Disabled
   Fast-reroute:  Disabled

 Tunnel Out-Label: 24017   gigabitethernet0

 RSVP-TE Signalling Info:
Primary LSP:
     From 3.3.3.3,   To 1.1.1.1,   Tunnel-Id 1,   LSP-Id 2
```

Status: UP

RSVP-TE Path Info:

Explicit Route: 20.1.1.1 10.1.1.1

Tspec: average rate 1m, burst rate 1m, peak rate 0

Bandwidth: 1m Setup-priority: 7 Hold-priority: 0

Affinity: include-any 0x0, include-all 0x0, exclude-any 0x0

RSVP-TE Resv Info:

Record Route:

Fspec: average rate 1m, burst rate 1m, peak rate 0

Out-Label: 24017 gigabitethernet0

LSP Minimum MTU: 1500

Other Info:

Tunnel created: 18 hours 23 minutes 21 seconds

Current LSP Uptime: 0 hour 2 minutes 58 seconds

Similarly, Tunnel1 is set up successfully on Device3, the status is UP, the egress label of the tunnel is 24017, and the egress interface is gigabitethernet0.

Step 5: Configure the static route, making the data traffic between Device4 and Device5 be forwarded along the MPLS P2P TE tunnel.

#Configure Device1.

Device1(config)#ip route 110.1.1.0 255.255.255.0 tunnel1

#Configure Device3

Device3(config)#ip route 100.1.1.0 255.255.255.0 tunnel1

#View the route information on Device1.

Device1#show ip route

Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS

U - Per-user Static route

O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external

C 10.1.1.0/24 is directly connected, 00:12:17, gigabitethernet0

i 20.1.1.0/24 [115/20] via 10.1.1.2, 00:12:11, gigabitethernet0

C 100.1.1.0/24 is directly connected, 00:12:21, gigabitethernet1

S 110.1.1.0/24 [1/1111111] is directly connected, 00:00:23, tunnel1

C 127.0.0.0/8 is directly connected, 23:13:54, lo0

C 1.1.1.1/32 is directly connected, 22:39:11, loopback0

```
i   2.2.2.2/24 [115/20] via 10.1.1.2, 00:12:06, gigabitethernet0
i   3.3.3.3/32 [115/30] via 10.1.1.2, 00:12:07, gigabitethernet0
```

You can see that the egress interface of the route 110.1.1.0/24 points to Tunnel1.

#View the route information on Device3.

```
Codes: C - Connected, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external



i   10.1.1.0/24 [115/20] via 20.1.1.1, 00:12:07, gigabitethernet0
C   20.1.1.0/24 is directly connected, 00:12:11, gigabitethernet0
S   100.1.1.0/24 [1/1111111] is directly connected, 00:00:05, tunnel1
C   110.1.1.0/24 is directly connected, 00:12:07, gigabitethernet1
C   127.0.0.0/8 is directly connected, 23:09:34, lo0
i   1.1.1.1/32 [115/30] via 20.1.1.1, 00:12:07, gigabitethernet0
i   2.2.2.2/24 [115/20] via 20.1.1.1, 00:12:07, gigabitethernet0
C   3.3.3.3/32 is directly connected, 22:38:59, loopback0
Similarly, the egress interface of the route 100.1.1.0/24 points to Tunnel1.
```

Step 6: Check the result.

#On Device4, use the ping command to check the connectivity with Device5.

```
Device4#ping 110.1.1.2

Press key (ctrl + shift + 6) interrupt it.
Sending 5, 76-byte ICMP Echos to 110.1.1.2 , timeout is 2 seconds:
!!!!!
Success rate is 100% (5/5). Round-trip min/avg/max = 0/0/0 ms.
```

On Device5, use the ping command to check the connectivity with Device4.

```
Device5#ping 100.1.1.2

Press key (ctrl + shift + 6) interrupt it.
Sending 5, 76-byte ICMP Echos to 100.1.1.2 , timeout is 2 seconds:
!!!!!
Success rate is 100% (5/5). Round-trip min/avg/max = 0/0/0 ms.
```

Device4 and Device5 can ping each other.

#On Device1, view the MPLS forwarding information.

Device1#show mpls forwarding-table

Pro: L - LDP, O - OSPF, B - MP-BGP, R - RSVP, M - Mapped-Route, S - Static Label,ML - mLDP (ML FEC: Root address/OT/OV), RM - RSVP P2MP (RM FEC: P2MP ID/TID)

Pro	Ident	FEC	Inlabel	Outlabel	Outgoing	Next hop
R	-TNL-	tunnel1	/	24016	gigabitethernet0	10.1.1.2

According to the packet statistics (TxPkts) of the MPLS forwarding table, the ICMP request packets and response packets of Device4 are forwarded along the TE tunnel.

#On Device3, view the MPLS forwarding information.

Device3#show mpls forwarding-table

Pro: L - LDP, O - OSPF, B - MP-BGP, R - RSVP, M - Mapped-Route, S - Static Label,ML - mLDP (ML FEC: Root address/OT/OV), RM - RSVP P2MP (RM FEC: P2MP ID/TID)

Pro	Ident	FEC	Inlabel	Outlabel	Outgoing	Next hop
R	-TNL-	tunnel1	/	24017	gigabitethernet0	20.1.1.1

Similarly, according to the packet statistics information, the ICMP request packets and response packets of Device5 are forwarded along the TE tunnel.

Therefore, it indicates that the data traffic between Device4 and Device5 is forwarded along the MPLS P2P TE tunnel.

4.3.3. Configure MPLS TE Fast Re-route of Link Protect Type

Network Requirements

- All devices run the OSPF protocol and enable the TE OSPF scalability.
- Use the explicit path to create one MPLS P2P TE tunnel along the link Device1→Device2→Device3→Device4, and it is required to perform the link protect for the link Device2→Device3 via the fast re-route.
- Device2 serves as the local repair point PLR, Device3 serves as the aggregation point MP, use the explicit path to create one MPLS P2P TE tunnel along the link Device2→Device5→Device3, the tunnel serves as the Bypass tunnel, protecting the link between Device2 and Device3, and configure RSVP-TE to link with BFD on the protected link; when the link fails, switch the master tunnel to the Bypass tunnel on PLR.

Network Topology

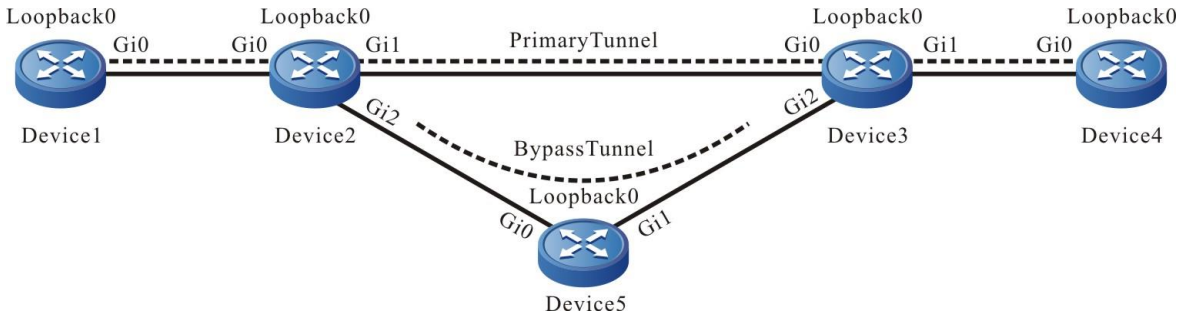

Figure 4-3 Configure the MPLS TE fast re-route of the link protect type

Device	Interface	IP Address	Device	Interface	IP Address
Device1	Gi0	10.1.1.1/24	Device3	Gi2	50.1.1.2/24
	Loopback0	1.1.1.1/32		Loopback0	3.3.3.3/32
Device2	Gi0	10.1.1.2/24	Device4	Gi0	30.1.1.2/24
	Gi1	20.1.1.1/24		Loopback0	4.4.4.4/32
	Gi2	40.1.1.1/24	Device5	Gi0	40.1.1.2/24
	Loopback0	2.2.2.2/32		Gi1	50.1.1.1/24
Device3	Gi0	20.1.1.2/24		Loopback0	5.5.5.5/32
	Gi1	30.1.1.1/24			

Configuration Steps

Step 1: Configure the IP address of the interface (omitted).

Step 2: Configure the OSPF protocol, all interfaces are covered to area 0, and area 0 enables the MPLS TE capability.

#Configure Device1.

```
Device1#configure terminal
Device1(config)#router ospf 100
Device1(config-ospf)#router-id 1.1.1.1
Device1(config-ospf)#network 10.1.1.0 0.0.0.255 area 0
Device1(config-ospf)#network 1.1.1.1 0.0.0.0 area 0
Device1(config-ospf)#mpls traffic-eng router-id 1.1.1.1
```

```
Device1(config-ospf)#mpls traffic-eng area 0
Device1(config-ospf)#exit
```

#Configure Device2.

```
Device2#configure terminal
Device2(config)#router ospf 100
Device2(config-ospf)#router-id 2.2.2.2
Device2(config-ospf)#network 10.1.1.0 0.0.0.255 area 0
Device2(config-ospf)#network 20.1.1.0 0.0.0.255 area 0
Device2(config-ospf)#network 40.1.1.0 0.0.0.255 area 0
Device2(config-ospf)#network 2.2.2.2 0.0.0.0 area 0
Device2(config-ospf)#mpls traffic-eng router-id 2.2.2.2
Device2(config-ospf)#mpls traffic-eng area 0
Device2(config-ospf)#exit
```

#Configure Device3

```
Device3#configure terminal
Device3(config)#router ospf 100
Device3(config-ospf)#router-id 3.3.3.3
Device3(config-ospf)#network 20.1.1.0 0.0.0.255 area 0
Device3(config-ospf)#network 30.1.1.0 0.0.0.255 area 0
Device3(config-ospf)#network 50.1.1.0 0.0.0.255 area 0
Device3(config-ospf)#network 3.3.3.3 0.0.0.0 area 0
Device3(config-ospf)#mpls traffic-eng router-id 3.3.3.3
Device3(config-ospf)#mpls traffic-eng area 0
Device3(config-ospf)#exit
```

#Configure Device4.

```
Device4#configure terminal
Device4(config)#router ospf 100
Device4(config-ospf)#router-id 4.4.4.4
Device4(config-ospf)#network 30.1.1.0 0.0.0.255 area 0
Device4(config-ospf)#network 4.4.4.4 0.0.0.0 area 0
Device4(config-ospf)#mpls traffic-eng router-id 4.4.4.4
Device4(config-ospf)#mpls traffic-eng area 0
Device4(config-ospf)#exit
```

#Configure Device5.

```
Device5#configure terminal
Device5(config)#router ospf 100
Device5(config-ospf)#router-id 5.5.5.5
```

```
Device5(config-ospf)#network 40.1.1.0 0.0.0.255 area 0
Device5(config-ospf)#network 50.1.1.0 0.0.0.255 area 0
Device5(config-ospf)#network 5.5.5.5 0.0.0.0 area 0
Device5(config-ospf)#mpls traffic-eng router-id 5.5.5.5
Device5(config-ospf)#mpls traffic-eng area 0
Device5(config-ospf)#exit
```

Step 3: Enable the MPLS TE function and MPLS forwarding capability. Meanwhile, configure the maximum reserved bandwidth of the link passed by the MPLS P2P TE tunnel.

#Configure Device1, enable the MPLS TE function and MPLS forwarding capability globally and on the interface gigabitethernet0, and configure the maximum reserved bandwidth of the link on the interface gigabitethernet0 as 100000 kbps.

```
Device1(config)#mpls ip
Device1(config)#mpls traffic-eng tunnels
Device1(config-rsvp-te)#router-id 1.1.1.1
Device1(config-rsvp-te)#exit
Device1(config)#interface gigabitethernet 0
Device1(config-if-gigabitethernet0)#mpls ip
Device1(config-if-gigabitethernet0)#mpls traffic-eng tunnels
Device1(config-if-gigabitethernet0)#ip rsvp bandwidth 100000
Device1(config-if-gigabitethernet0)#exit
```

#Configure Device2, enable the MPLS TE function and MPLS forwarding capability globally and on the interface gigabitethernet0, gigabitethernet1, gigabitethernet2, and configure the maximum reserved bandwidth of the link on the interface gigabitethernet0, gigabitethernet1, gigabitethernet2 as 100000 kbps.

```
Device2(config)#mpls ip
Device2(config)#mpls traffic-eng tunnels
Device2(config-rsvp-te)#router-id 2.2.2.2
Device2(config-rsvp-te)#exit
Device2(config)#interface gigabitethernet 0
Device2(config-if-gigabitethernet0)#mpls ip
Device2(config-if-gigabitethernet0)#mpls traffic-eng tunnels
Device2(config-if-gigabitethernet0)#ip rsvp bandwidth 100000
Device2(config-if-gigabitethernet0)#exit
Device2(config)#interface gigabitethernet 1
Device2(config-if-gigabitethernet1)#mpls ip
Device2(config-if-gigabitethernet1)#mpls traffic-eng tunnels
Device2(config-if-gigabitethernet1)#ip rsvp bandwidth 100000
```

```
Device2(config-if-gigabitethernet1)#exit
Device2(config)#interface gigabitethernet 2
Device2(config-if-gigabitethernet2)#mpls ip
Device2(config-if-gigabitethernet2)#mpls traffic-eng tunnels
Device2(config-if-gigabitethernet2)#ip rsvp bandwidth 100000
Device2(config-if-gigabitethernet2)#exit
```

#Configure Device3, enable the MPLS TE function and MPLS forwarding capability globally and on the interface gigabitethernet0, gigabitethernet1, gigabitethernet2, and configure the maximum reserved bandwidth of the link on the interface gigabitethernet0, gigabitethernet1, gigabitethernet2 as 100000 kbps.

```
Device3(config)#mpls ip
Device3(config)#mpls traffic-eng tunnels
Device3(config-rsvp-te)#router-id 3.3.3.3
Device3(config-rsvp-te)#exit
Device3(config)#interface gigabitethernet 0
Device3(config-if-gigabitethernet0)#mpls ip
Device3(config-if-gigabitethernet0)#mpls traffic-eng tunnels
Device3(config-if-gigabitethernet0)#ip rsvp bandwidth 100000
Device3(config-if-gigabitethernet0)#exit
Device3(config)#interface gigabitethernet 1
Device3(config-if-gigabitethernet1)#mpls ip
Device3(config-if-gigabitethernet1)#mpls traffic-eng tunnels
Device3(config-if-gigabitethernet1)#ip rsvp bandwidth 100000
Device3(config-if-gigabitethernet1)#exit
Device3(config)#interface gigabitethernet 2
Device3(config-if-gigabitethernet2)#mpls ip
Device3(config-if-gigabitethernet2)#mpls traffic-eng tunnels
Device3(config-if-gigabitethernet2)#ip rsvp bandwidth 100000
Device3(config-if-gigabitethernet2)#exit
```

#Configure Device4, enable the MPLS TE function and MPLS forwarding capability globally and on the interface gigabitethernet0, and configure the maximum reserved bandwidth of the link on the interface gigabitethernet0 as 100000 kbps.

```
Device4(config)#mpls ip
Device4(config)#mpls traffic-eng tunnels
Device4(config-rsvp-te)#router-id 4.4.4.4
Device4(config-rsvp-te)#exit
Device4(config)#interface gigabitethernet 0
Device4(config-if-gigabitethernet0)#mpls ip
Device4(config-if-gigabitethernet0)#mpls traffic-eng tunnels
```

```
Device4(config-if-gigabitethernet0)#ip rsvp bandwidth 100000
Device4(config-if-gigabitethernet0)#exit
```

#Configure Device5, enable the MPLS TE function and MPLS forwarding capability globally and on the interface gigabitethernet0, gigabitethernet1, and configure the maximum reserved bandwidth of the link on the interface gigabitethernet0, gigabitethernet1 as 100000 kbps.

```
Device5(config)#mpls ip
Device5(config)#mpls traffic-eng tunnels
Device5(config-rsvp-te)#router-id 5.5.5.5
Device5(config-rsvp-te)#exit
Device5(config)#interface gigabitethernet 0
Device5(config-if-gigabitethernet0)#mpls ip
Device5(config-if-gigabitethernet0)#mpls traffic-eng tunnels
Device5(config-if-gigabitethernet0)#ip rsvp bandwidth 100000
Device5(config-if-gigabitethernet0)#exit
Device5(config)#interface gigabitethernet 1
Device5(config-if-gigabitethernet1)#mpls ip
Device5(config-if-gigabitethernet1)#mpls traffic-eng tunnels
Device5(config-if-gigabitethernet1)#ip rsvp bandwidth 100000
Device5(config-if-gigabitethernet1)#exit
```

Step 4: Configure the explicit path and the MPLS P2P TE tunnel.

#On Device1, configure the explicit path along Device1→Device2→Device3→Device4, create MPLS TE master tunnel, and configure the path option of the tunnel as the explicit path.

```
Device1(config)#ip explicit-path 1
Device1(config-ip-expl-path)#address 10.1.1.2 strict
Device1(config-ip-expl-path)#address 20.1.1.2 strict
Device1(config-ip-expl-path)#address 30.1.1.2 strict
Device1(config-ip-expl-path)#exit
Device1(config)#interface tunnel 1
Device1(config-if-tunnel1)#tunnel mode mpls traffic-eng
Device1(config-if-tunnel1)#ip unnumbered loopback 0
Device1(config-if-tunnel1)#tunnel destination 4.4.4.4
Device1(config-if-tunnel1)#tunnel mpls traffic-eng bandwidth 1000
Device1(config-if-tunnel1)#tunnel mpls traffic-eng path-option 1 explicit-path 1
Device1(config-if-tunnel1)#exit
```

#On Device2, configure the explicit path along Device2→Device5→Device3, create Bypass tunnel, and configure the path option of the tunnel as the explicit path.

```
Device2(config)#ip explicit-path 1
Device2(config-ip-expl-path)#address 40.1.1.2 strict
Device2(config-ip-expl-path)#address 50.1.1.2 strict
Device2(config-ip-expl-path)#exit
Device2(config)#interface tunnel 1
Device2(config-if-tunnel1)#tunnel mode mpls traffic-eng
Device2(config-if-tunnel1)#ip unnumbered loopback 0
Device2(config-if-tunnel1)#tunnel destination 3.3.3.3
Device2(config-if-tunnel1)#tunnel mpls traffic-eng bandwidth 1000
Device2(config-if-tunnel1)#tunnel mpls traffic-eng path-option 1 explicit-path 1
Device2(config-if-tunnel1)#exit
Device2(config)#exit
```

#View the details of the MPLS P2P TE tunnel on Device1.

```
Device1#show mpls traffic-eng tunnels tunnel 1

*Tunnel 1  (Device1_t1)              Destination: 4.4.4.4
  Status:
    Admin: UP      Oper: UP (Using Primary LSP)   Signalling: Connected
    path option 1, type explicit 1 (Basis for Setup)

  Config Parameters:
    Reoptimize: Enabled  interval: 3600 seconds
    Update type: Make-before-break
    Auto Route:  Disabled
    Forwarding adjacency:  Disabled
    Bandwidth: 1m       Setup-priority: 7  Hold-priority: 0
    Affinity: include-any 0x0, include-all 0x0, exclude-any 0x0
    Explicit path: 1
    Record route: Disabled
    auto-bw: Disabled
    Fast-reroute:  Disabled

  Tunnel Out-Label: 24016   gigabitethernet0

  RSVP-TE Signalling Info:
    Primary LSP:
      From 1.1.1.1,   To 4.4.4.4,   Tunnel-Id 1,   LSP-Id 1
```

Status: UP
RSVP-TE Path Info:
Explicit Route: 10.1.1.2 20.1.1.2 30.1.1.2
Tspec: average rate 1m, burst rate 1m, peak rate 0
Bandwidth: 1m Setup-priority: 7 Hold-priority: 0
Affinity: include-any 0x0, include-all 0x0, exclude-any 0x0
RSVP-TE Resv Info:
Record Route:
Fspec: average rate 1m, burst rate 1m, peak rate 0
Out-Label: 24016 gigabitethernet0
LSP Minimum MTU: 1500

Other Info:
Tunnel created: 0 hour 17 minutes 18 seconds
Current LSP Uptime: 0 hour 0 minute 22 seconds

You can see that the tunnel is set up successfully along the specified explicit path Device1→Device2→Device3→Device4 on Device1.

#On Device2, view the details of the MPLS P2P TE tunnel.

```
Device2#show mpls traffic-eng tunnels tunnel 1

*Tunnel 1  (Device2_t1)              Destination: 3.3.3.3
 Status:
   Admin: UP      Oper: UP (Using Primary LSP)   Signalling: Connected
   path option 1, type explicit 1 (Basis for Setup)

 Config Parameters:
   Reoptimize: Enabled  interval: 3600 seconds
   Update type: Make-before-break
   Auto Route:  Disabled
   Forwarding adjacency:  Disabled
   Bandwidth: 1m       Setup-priority: 7  Hold-priority: 0
   Affinity: include-any 0x0, include-all 0x0, exclude-any 0x0
   Explicit path: 1
   Record route: Disabled
   auto-bw: Disabled
   Fast-reroute:  Disabled
```

```
Tunnel Out-Label: 24017   gigabitethernet2

RSVP-TE Signalling Info:
Primary LSP:
    From 2.2.2.2,   To 3.3.3.3,   Tunnel-Id 1,   LSP-Id 1
    Status:  UP
    RSVP-TE Path Info:
      Explicit Route:  40.1.1.2       50.1.1.2
      Tspec: average rate 1m, burst rate 1m, peak rate 0
      Bandwidth: 1m       Setup-priority: 7  Hold-priority: 0
      Affinity: include-any 0x0, include-all 0x0, exclude-any 0x0
    RSVP-TE Resv Info:
      Record Route:
      Fspec: average rate 1m, burst rate 1m, peak rate 0
      Out-Label: 24017   gigabitethernet2
      LSP Minimum MTU: 1500

Other Info:
  Tunnel created:    0 hour 0 minute 34 seconds
  Current LSP Uptime: 0 hour 0 minute 34 seconds
```

Similarly, the tunnel is set up successfully along the specified explicit path Device2→Device5→Device3 on Device2.

Step 5: Enable the fast re-route function of the master tunnel, bind the Bypass tunnel on the protected link of PLR, and enable RSVP-TE to link with BFD.

#Configure Device1, and the master tunnel enables the fast re-route function.

```
Device1(config)#interface tunnel 1
Device1(config-if-tunnel1)#tunnel mpls traffic-eng fast-reroute
Device1(config-if-tunnel1)#tunnel mpls traffic-eng record-route
Device1(config-if-tunnel1)#exit
```

#Configure Device2, bind the Bypass tunnel on the protected link, and enable RSVP-TE to link with BFD.

```
Device2(config)#interface gigabitethernet 1
Device2(config-if-gigabitethernet1)#mpls traffic-eng backup-path tunnel 1
Device2(config-if-gigabitethernet1)#ip rsvp bfd-signalling
Device2(config-if-gigabitethernet1)#exit
```

#Configure Device3, and enable RSVP-TE to link with BFD on the protected link.

```
Device3(config)#interface gigabitethernet 0
```

```
Device3(config-if-gigabitethernet0)#ip rsvp bfd-signalling
Device3(config-if-gigabitethernet0)#exit
```

#View the details of the MPLS P2P TE tunnel on Device1.

```
Device1#show mpls traffic-eng tunnels tunnel 1

*Tunnel 1  (Device1_t1)              Destination: 4.4.4.4
  Status:
    Admin: UP      Oper: UP (Using Primary LSP)   Signalling: Connected
    path option 1, type explicit 1 (Basis for Setup)

  Config Parameters:
    Reoptimize: Enabled  interval: 3600 seconds
    Update type: Make-before-break
    Auto Route:  Disabled
    Forwarding adjacency:  Disabled
    Bandwidth: 1m       Setup-priority: 7  Hold-priority: 0
    Affinity: include-any 0x0, include-all 0x0, exclude-any 0x0
    Explicit path: 1
    Record route: Enabled
    auto-bw: Disabled
    Fast-reroute:  FACILITY Enabled

  Tunnel Out-Label: 24016   gigabitethernet0


  RSVP-TE Signalling Info:
Primary LSP:
      From 1.1.1.1,   To 4.4.4.4,   Tunnel-Id 1,   LSP-Id 1
      Status:  UP
      RSVP-TE Path Info:
        Explicit Route:  10.1.1.2       20.1.1.2       30.1.1.2
        Tspec: average rate 1m, burst rate 0, peak rate 0
        Bandwidth: 1m       Setup-priority: 7  Hold-priority: 0
        Affinity: include-any 0x0, include-all 0x0, exclude-any 0x0
        Desires LINK local protection
      RSVP-TE Resv Info:
        Record Route (A: Local Protect Available):
```

```
                10.1.1.2(A)      2.2.2.2(A)      20.1.1.2      3.3.3.3      30.1.1.2
                4.4.4.4
            Fspec: average rate 1m, burst rate 0, peak rate 0
            Out-Label: 24016   gigabitethernet0
            LSP Minimum MTU: 1500

        Other Info:
          Tunnel created:    0 hour 51 minutes 43 seconds
          Current LSP Uptime: 0 hour 34 minutes 47 seconds
```

From the details of the master tunnel, you can see that the fast re-route function is enabled, the PLR information is recorded in the Record Route information, and the standby tunnel is available on PLR.

#On Device2, view the master tunnel and Bypass tunnel binding information.

```
Device2#show mpls traffic-eng tunnels summary
name                role   lspid  ingress      egress       ext-id       status   res-id
ref

Device2_t1          Ingress 2     2.2.2.2      3.3.3.3      2.2.2.2      up       2      1

Device1_t1          Transit 1     1.1.1.1      4.4.4.4      1.1.1.1      up       3      1
Device2_t1          Ingress 2     2.2.2.2      3.3.3.3      2.2.2.2      up       2      1
(backup)
```

You can see that the binding relation of the master tunnel and Bypass tunnel is set up.

```
Device2#show mpls traffic-eng tunnels transit

*Tunnel  Device1_t1 (LSP-id 1)  Signalled from 1.1.1.1  Destination: 4.4.4.4

 In-Label:  24016   gigabitethernet0   Out-Label: 24016   gigabitethernet1

 RSVP-TE Signalling Info:
   Primary LSP:
     From 1.1.1.1,   To 4.4.4.4,   Tunnel-Id 1,   LSP-Id 1
     Status:  UP    Backup LSP READY at this node.
     RSVP-TE Path Info:
       Explicit Route:  20.1.1.2       30.1.1.2
       Tspec: average rate 1m, burst rate 0, peak rate 0
       Bandwidth: 1m       Setup-priority: 7  Hold-priority: 0
```

```
    Desires LINK local protection
  RSVP-TE Resv Info:
    Record Route:   20.1.1.2      3.3.3.3      30.1.1.2      4.4.4.4
    Fspec: average rate 1m, burst rate 0, peak rate 0
    LSP Minimum MTU: 1500

Bypass LSP:
  From 2.2.2.2,   To 3.3.3.3,   Tunnel-Id 1,   LSP-Id 2
  Status:  UP
  RSVP-TE Path Info:
    Explicit Route:  40.1.1.2      50.1.1.2
    Tspec: average rate 1m, burst rate 0, peak rate 0
    Bandwidth: 1m      Setup-priority: 7  Hold-priority: 0
    Affinity: include-any 0x0, include-all 0x0, exclude-any 0x0
  RSVP-TE Resv Info:
    Record Route:
    Fspec: average rate 1m, burst rate 0, peak rate 0
    Out-Label: 24017   gigabitethernet2
    LSP Minimum MTU: 1500
```

From the details of the master tunnel, you can see that the current node is bound with the Bypass tunnel successfully, and the protect for the master tunnel is ready.

#On Device2, view the BFD session information.

```
Device2#show bfd session detail
Total session number: 1
OurAddr          NeighAddr          LD/RD          State          Holddown
interface
20.1.1.1         20.1.1.2           1/1            UP             5000
gigabitethernet1
Type:direct
Local State:UP  Remote State:UP  Up for: 1h:26m:14s  Number of times UP:1
Send Interval:1000ms  Detection time:5000ms(1000ms*5)
Local Diag:0  Demand mode:0  Poll bit:0
MinTxInt:1000  MinRxInt:1000  Multiplier:5
Remote MinTxInt:1000  Remote MinRxInt:1000  Remote Multiplier:5
Registered protocols:RSVP
```

You can see that the BFD session is set up successfully.

Step 6: Check the result.

#When the protected link between Device2 and Device3 fails, BFD fast detects the fault and informs the RSVP-TE protocol, and PLR switches the master tunnel to the Bypass tunnel at once.

#On Device1, view the details of the master tunnel.

```
Device1#show mpls traffic-eng tunnels tunnel 1

*Tunnel 1  (Device1_t1)              Destination: 4.4.4.4
  Status:
    Admin: UP      Oper: UP (Using Primary LSP)   Signalling: Connected
    path option 1, type explicit 1 (Basis for Setup)

  Config Parameters:
    Reoptimize: Enabled  interval: 3600 seconds
    Update type: Make-before-break
    Auto Route:  Disabled
    Forwarding adjacency:  Disabled
   Bandwidth: 1m       Setup-priority: 7  Hold-priority: 0
    Affinity: include-any 0x0, include-all 0x0, exclude-any 0x0
    Explicit path: None
    Record route: Enabled
    auto-bw: Disabled
    Fast-reroute:  FACILITY Enabled

  Tunnel Out-Label: 24016   gigabitethernet0


  RSVP-TE Signalling Info:
Primary LSP:
       From 1.1.1.1,   To 4.4.4.4,   Tunnel-Id 1,   LSP-Id 1
       Status:  UP
       RSVP-TE Path Info:
          Explicit Route:  10.1.1.2       20.1.1.2       30.1.1.2
          Tspec: average rate 1m, burst rate 0, peak rate 0
          Bandwidth: 1m       Setup-priority: 7  Hold-priority: 0
          Affinity: include-any 0x0, include-all 0x0, exclude-any 0x0
          Desires LINK local protection
       RSVP-TE Resv Info:
          Record Route (A: Local Protect Available):
                    10.1.1.2(AU)       2.2.2.2(AU)
                  Using backup LSP at nodes marked (U).
```

```
        Fspec: average rate 1m, burst rate 0, peak rate 0
        Out-Label: 24016   gigabitethernet0
        LSP Minimum MTU: 1500

    Other Info:
      Tunnel created:    2 hours 14 minutes 5 seconds
      Current LSP Uptime: 1 hour 57 minutes 9 seconds
```

From the Record Route information, you can see that the Bypass tunnel is enabled on PLR.

#On Device2, view the details and MPLS forwarding information on the master tunnel.

```
Device2#show mpls traffic-eng tunnels transit

*Tunnel  Device1_t1 (LSP-id 1)  Signalled from 1.1.1.1  Destination: 4.4.4.4

 In-Label:  16   gigabitethernet0   Out-Label: 17   gigabitethernet2

 RSVP-TE Signalling Info:
   Primary LSP:
     From 1.1.1.1,   To 4.4.4.4,   Tunnel-Id 1,   LSP-Id 1
     Status:  UP    Backup LSP is being USED at this node.
     RSVP-TE Path Info:
       Explicit Route:  20.1.1.2       30.1.1.2
       Tspec: average rate 1m, burst rate 0, peak rate 0
       Bandwidth: 1m       Setup-priority: 7  Hold-priority: 0
       Desires LINK local protection
     RSVP-TE Resv Info:
       Record Route:
       Fspec: average rate 1m, burst rate 0, peak rate 0
       LSP Minimum MTU:

   Bypass LSP:
     From 2.2.2.2,   To 3.3.3.3,   Tunnel-Id 1,   LSP-Id 2
     Status:  UP
     RSVP-TE Path Info:
       Explicit Route:  40.1.1.2       50.1.1.2
       Tspec: average rate 1m, burst rate 0, peak rate 0
       Bandwidth: 1m       Setup-priority: 7  Hold-priority: 0
       Affinity: include-any 0x0, include-all 0x0, exclude-any 0x0
```

```
RSVP-TE Resv Info:
  Record Route:
  Fspec: average rate 1m, burst rate 0, peak rate 0
  Out-Label: 24017   gigabitethernet2
  LSP Minimum MTU: 1500
```

On Device2, you also can see that the Bypass tunnel is enabled on the node in the details of the master tunnel.

```
Device2#show mpls forwarding-table
Pro: L - LDP, O - OSPF, B - MP-BGP, R - RSVP, M - Mapped-Route, S - Static Label,ML - mLDP (ML FEC: Root address/OT/OV), RM - RSVP P2MP (RM FEC: P2MP ID/TID)

Pro Ident       FEC             Inlabel Outlabel Outgoing          Next hop
R   -TNL-       tunnel1         /       24017    gigabitethernet2  40.1.1.2
R   global      4.4.4.4/32      24016   24016    tunnel1           40.1.1.2
```

You can see that the egress interface to the Egress node 4.4.4.4 is the Bypass tunnel Tunnel1, indicating that the data traffic is switched to the Bypass tunnel from the master tunnel.

Note:

- If there are multiple tunnels passing the protected link, and the tunnels all enable the fast re-route function, the Bypass tunnel will bind with these tunnels, that is, one Bypass tunnel can protect multiple tunnels passing the link at the same time.

4.3.4. Configure MPLS TE Fast Re-route of Node Protect Type

Network Requirements

- All devices run the OSPF protocol and enable the TE OSPF scalability.
- Use the explicit path to create one MPLS P2P TE tunnel along the link Device1→Device2→Device3→Device4, and it is required to perform the node protect for the node Device3 via the fast re-route.
- Device2 serves as the local repair point PLR, Device4 serves as the aggregation point MP, use the explicit path to create one MPLS P2P TE tunnel along the link Device2→Device5→Device4, the tunnel serves as the Bypass tunnel, protecting the node Device3.
- On the protected Device3 node and the PLR link, configure RSVP-TE to link with BFD. When the Device3 node fails, switch the master tunnel to the Bypass tunnel fast on PLR.

Network Topology

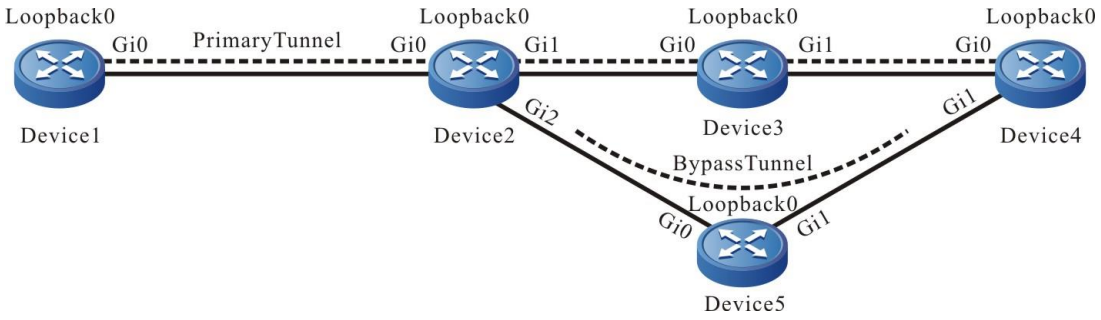

Figure 4-4 Configure the MPLS TE fast re-route of the node protect type

Device	Interface	IP Address	Device	Interface	IP Address
Device1	Gi0	10.1.1.1/24	Device3	Loopback0	3.3.3.3/32
	Loopback0	1.1.1.1/32	Device4	Gi0	30.1.1.2/24
Device2	Gi0	10.1.1.2/24		Gi1	50.1.1.2/24
	Gi1	20.1.1.1/24		Loopback0	4.4.4.4/32
	Gi2	40.1.1.1/24	Device5	Gi0	40.1.1.2/24
	Loopback0	2.2.2.2/32		Gi1	50.1.1.1/24
Device3	Gi0	20.1.1.2/24		Loopback0	5.5.5.5/32
	Gi1	30.1.1.1/24			

Configuration Steps

Step 1: Configure the IP address of the interface (omitted).

Step 2: Configure the OSPF protocol, all interfaces are covered to area 0, and area 0 enables the MPLS TE capability.

#Configure Device1.

```
Device1#configure terminal
Device1(config)#router ospf 100
Device1(config-ospf)#router-id 1.1.1.1
Device1(config-ospf)#network 10.1.1.0 0.0.0.255 area 0
Device1(config-ospf)#network 1.1.1.1 0.0.0.0 area 0
Device1(config-ospf)#mpls traffic-eng router-id 1.1.1.1
```

```
Device1(config-ospf)#mpls traffic-eng area 0
Device1(config-ospf)#exit
```

#Configure Device2.

```
Device2#configure terminal
Device2(config)#router ospf 100
Device2(config-ospf)#router-id 2.2.2.2
Device2(config-ospf)#network 10.1.1.0 0.0.0.255 area 0
Device2(config-ospf)#network 20.1.1.0 0.0.0.255 area 0
Device2(config-ospf)#network 40.1.1.0 0.0.0.255 area 0
Device2(config-ospf)#network 2.2.2.2 0.0.0.0 area 0
Device2(config-ospf)#mpls traffic-eng router-id 2.2.2.2
Device2(config-ospf)#mpls traffic-eng area 0
Device2(config-ospf)#exit
```

#Configure Device3

```
Device3#configure terminal
Device3(config)#router ospf 100
Device3(config-ospf)#router-id 3.3.3.3
Device3(config-ospf)#network 20.1.1.0 0.0.0.255 area 0
Device3(config-ospf)#network 30.1.1.0 0.0.0.255 area 0
Device3(config-ospf)#network 3.3.3.3 0.0.0.0 area 0
Device3(config-ospf)#mpls traffic-eng router-id 3.3.3.3
Device3(config-ospf)#mpls traffic-eng area 0
Device3(config-ospf)#exit
```

#Configure Device4.

```
Device4#configure terminal
Device4(config)#router ospf 100
Device4(config-ospf)#router-id 4.4.4.4
Device4(config-ospf)#network 30.1.1.0 0.0.0.255 area 0
Device4(config-ospf)#network 50.1.1.0 0.0.0.255 area 0
Device4(config-ospf)#network 4.4.4.4 0.0.0.0 area 0
Device4(config-ospf)#mpls traffic-eng router-id 4.4.4.4
Device4(config-ospf)#mpls traffic-eng area 0
Device4(config-ospf)#exit
```

#Configure Device5.

```
Device5#configure terminal
Device5(config)#router ospf 100
Device5(config-ospf)#router-id 5.5.5.5
```

```
Device5(config-ospf)#network 40.1.1.0 0.0.0.255 area 0
Device5(config-ospf)#network 50.1.1.0 0.0.0.255 area 0
Device5(config-ospf)#network 5.5.5.5 0.0.0.0 area 0
Device5(config-ospf)#mpls traffic-eng router-id 5.5.5.5
Device5(config-ospf)#mpls traffic-eng area 0
Device5(config-ospf)#exit
```

Step 3: Enable the MPLS TE function and MPLS forwarding capability. Meanwhile, configure the maximum reserved bandwidth of the link passed by the MPLS P2P TE tunnel.

#Configure Device1, enable the MPLS TE function and MPLS forwarding capability globally and on the interface gigabitethernet0, and configure the maximum reserved bandwidth of the link on the interface gigabitethernet0 as 100000 kbps.

```
Device1(config)#mpls ip
Device1(config)#mpls traffic-eng tunnels
Device1(config-rsvp-te)#router-id 1.1.1.1
Device1(config-rsvp-te)#exit
Device1(config)#interface gigabitethernet 0
Device1(config-if-gigabitethernet0)#mpls ip
Device1(config-if-gigabitethernet0)#mpls traffic-eng tunnels
Device1(config-if-gigabitethernet0)#ip rsvp bandwidth 100000
Device1(config-if-gigabitethernet0)#exit
```

#Configure Device2, enable the MPLS TE function and MPLS forwarding capability globally and on the interface gigabitethernet0, gigabitethernet1, gigabitethernet2, and configure the maximum reserved bandwidth of the link on the interface gigabitethernet0, gigabitethernet1, gigabitethernet2 as 100000 kbps.

```
Device2(config)#mpls ip
Device2(config)#mpls traffic-eng tunnels
Device2(config-rsvp-te)#router-id 2.2.2.2
Device2(config-rsvp-te)#exit
Device2(config)#interface gigabitethernet 0
Device2(config-if-gigabitethernet0)#mpls ip
Device2(config-if-gigabitethernet0)#mpls traffic-eng tunnels
Device2(config-if-gigabitethernet0)#ip rsvp bandwidth 100000
Device2(config-if-gigabitethernet0)#exit
Device2(config)#interface gigabitethernet 1
Device2(config-if-gigabitethernet1)#mpls ip
Device2(config-if-gigabitethernet1)#mpls traffic-eng tunnels
Device2(config-if-gigabitethernet1)#ip rsvp bandwidth 100000
```

```
Device2(config-if-gigabitethernet1)#exit
Device2(config)#interface gigabitethernet 2
Device2(config-if-gigabitethernet2)#mpls ip
Device2(config-if-gigabitethernet2)#mpls traffic-eng tunnels
Device2(config-if-gigabitethernet2)#ip rsvp bandwidth 100000
Device2(config-if-gigabitethernet2)#exit
```

#Configure Device3, enable the MPLS TE function and MPLS forwarding capability globally and on the interface gigabitethernet0, gigabitethernet1, and configure the maximum reserved bandwidth of the link on the interface gigabitethernet0, gigabitethernet1 as 100000 kbps.

```
Device3(config)#mpls ip
Device3(config)#mpls traffic-eng tunnels
Device3(config-rsvp-te)#router-id 3.3.3.3
Device3(config-rsvp-te)#exit
Device3(config)#interface gigabitethernet 0
Device3(config-if-gigabitethernet0)#mpls ip
Device3(config-if-gigabitethernet0)#mpls traffic-eng tunnels
Device3(config-if-gigabitethernet0)#ip rsvp bandwidth 100000
Device3(config-if-gigabitethernet0)#exit
Device3(config)#interface gigabitethernet 1
Device3(config-if-gigabitethernet1)#mpls ip
Device3(config-if-gigabitethernet1)#mpls traffic-eng tunnels
Device3(config-if-gigabitethernet1)#ip rsvp bandwidth 100000
Device3(config-if-gigabitethernet1)#exit
```

#Configure Device4, enable the MPLS TE function and MPLS forwarding capability globally and on the interface gigabitethernet0, gigabitethernet1, and configure the maximum reserved bandwidth of the link on the interface gigabitethernet0, gigabitethernet1 as 100000 kbps.

```
Device4(config)#mpls ip
Device4(config)#mpls traffic-eng tunnels
Device4(config-rsvp-te)#router-id 4.4.4.4
Device4(config-rsvp-te)#exit
Device4(config)#interface gigabitethernet 0
Device4(config-if-gigabitethernet0)#mpls ip
Device4(config-if-gigabitethernet0)#mpls traffic-eng tunnels
Device4(config-if-gigabitethernet0)#ip rsvp bandwidth 100000
Device4(config-if-gigabitethernet0)#exit
Device4(config)#interface gigabitethernet 1
Device4(config-if-gigabitethernet1)#mpls ip
Device4(config-if-gigabitethernet1)#mpls traffic-eng tunnels
```

```
Device4(config-if-gigabitethernet1)#ip rsvp bandwidth 100000
Device4(config-if-gigabitethernet1)#exit
```

#Configure Device5, enable the MPLS TE function and MPLS forwarding capability globally and on the interface gigabitethernet0, gigabitethernet1, and configure the maximum reserved bandwidth of the link on the interface gigabitethernet0, gigabitethernet1 as 100000 kbps.

```
Device5(config)#mpls ip
Device5(config)#mpls traffic-eng tunnels
Device5(config-rsvp-te)#router-id 5.5.5.5
Device5(config-rsvp-te)#exit
Device5(config)#interface gigabitethernet 0
Device5(config-if-gigabitethernet0)#mpls ip
Device5(config-if-gigabitethernet0)#mpls traffic-eng tunnels
Device5(config-if-gigabitethernet0)#ip rsvp bandwidth 100000
Device5(config-if-gigabitethernet0)#exit
Device5(config)#interface gigabitethernet 1
Device5(config-if-gigabitethernet1)#mpls ip
Device5(config-if-gigabitethernet1)#mpls traffic-eng tunnels
Device5(config-if-gigabitethernet1)#ip rsvp bandwidth 100000
Device5(config-if-gigabitethernet1)#exit
```

Step 4: Device1, Device2 configure the explicit path; the MPLS P2P TE tunnel is created along the explicit path.

#On Device1, configure the explicit path along Device1→Device2→Device3→Device4, create MPLS TE master tunnel, and configure the path option of the tunnel as the explicit path.

```
Device1(config)#ip explicit-path 1
Device1(config-ip-expl-path)#address 10.1.1.2 strict
Device1(config-ip-expl-path)#address 20.1.1.2 strict
Device1(config-ip-expl-path)#address 30.1.1.2 strict
Device1(config-ip-expl-path)#exit
Device1(config)#interface tunnel 1
Device1(config-if-tunnel1)#tunnel mode mpls traffic-eng
Device1(config-if-tunnel1)#ip unnumbered loopback 0
Device1(config-if-tunnel1)#tunnel destination 4.4.4.4
Device1(config-if-tunnel1)#tunnel mpls traffic-eng bandwidth 1000
Device1(config-if-tunnel1)#tunnel mpls traffic-eng path-option 1 explicit-path 1
Device1(config-if-tunnel1)#exit
```

#On Device2, configure the explicit path along Device2→Device5→Device4, create Bypass tunnel, and configure the path option of the tunnel as the explicit path.

```
Device2(config)#ip explicit-path 1
```

```
Device2(config-ip-expl-path)#address 40.1.1.2 strict
Device2(config-ip-expl-path)#address 50.1.1.2 strict
Device2(config-ip-expl-path)#exit
Device2(config)#interface tunnel 1
Device2(config-if-tunnel1)#tunnel mode mpls traffic-eng
Device2(config-if-tunnel1)#ip unnumbered loopback 0
Device2(config-if-tunnel1)#tunnel destination 4.4.4.4
Device2(config-if-tunnel1)#tunnel mpls traffic-eng bandwidth 1000
Device2(config-if-tunnel1)#tunnel mpls traffic-eng path-option 1 explicit-path 1
Device2(config-if-tunnel1)#exit
Device2(config)#exit
```

#View the details of the MPLS P2P TE tunnel on Device1.

```
Device1#show mpls traffic-eng tunnels tunnel 1

*Tunnel 1  (Device1_t1)              Destination: 4.4.4.4
  Status:
    Admin: UP      Oper: UP (Using Primary LSP)   Signalling: Connected
    path option 1, type explicit 1 (Basis for Setup)

  Config Parameters:
    Reoptimize: Enabled  interval: 3600 seconds
    Update type: Make-before-break
    Auto Route:  Disabled
    Forwarding adjacency:  Disabled
    Bandwidth: 1m       Setup-priority: 7  Hold-priority: 0
    Affinity: include-any 0x0, include-all 0x0, exclude-any 0x0
    Explicit path: 1
    Record route: Disabled
   auto-bw: Disabled
    Fast-reroute:  Disabled

  Tunnel Out-Label: 24016   gigabitethernet0

  RSVP-TE Signalling Info:
    Primary LSP:
      From 1.1.1.1,   To 4.4.4.4,   Tunnel-Id 1,   LSP-Id 1
      Status:  UP
```

RSVP-TE Path Info:
Explicit Route: 10.1.1.2 20.1.1.2 30.1.1.2
Tspec: average rate 1m, burst rate 1m, peak rate 0
Bandwidth: 1m Setup-priority: 7 Hold-priority: 0
Affinity: include-any 0x0, include-all 0x0, exclude-any 0x0
RSVP-TE Resv Info:
Record Route:
Fspec: average rate 1m, burst rate 1m, peak rate 0
Out-Label: 16 gigabitethernet0
LSP Minimum MTU: 1500

Other Info:
Tunnel created: 4 days 20 hours
Current LSP Uptime: 0 hour 7 minutes 47 seconds

On Device1, the tunnel is set up successfully along the specified explicit path.

#On Device2, view the details of the MPLS P2P TE tunnel.

Device2#show mpls traffic-eng tunnels tunnel 1

*Tunnel 1 (Device2_t1) Destination: 4.4.4.4
Status:
Admin: UP Oper: UP (Using Primary LSP) Signalling: Connected
path option 1, type explicit 1 (Basis for Setup)

Config Parameters:
Reoptimize: Enabled interval: 3600 seconds
Update type: Make-before-break
Auto Route: Disabled
Forwarding adjacency: Disabled
Bandwidth: 1m Setup-priority: 7 Hold-priority: 0
Affinity: include-any 0x0, include-all 0x0, exclude-any 0x0
Explicit path: 1
Record route: Disabled
auto-bw: Disabled
Fast-reroute: Disabled

Tunnel Out-Label: 24016 gigabitethernet2

```
RSVP-TE Signalling Info:
  Primary LSP:
    From 2.2.2.2,   To 4.4.4.4,   Tunnel-Id 1,   LSP-Id 1
    Status:  UP
    RSVP-TE Path Info:
      Explicit Route:  40.1.1.2        50.1.1.2
      Tspec: average rate 1m, burst rate 1m, peak rate 0
      Bandwidth: 1m       Setup-priority: 7  Hold-priority: 0
      Affinity: include-any 0x0, include-all 0x0, exclude-any 0x0
    RSVP-TE Resv Info:
      Record Route:
      Fspec: average rate 1m, burst rate 1m, peak rate 0
      Out-Label: 24016    gigabitethernet2
      LSP Minimum MTU: 1500


  Other Info:
    Tunnel created:     0 hour 1 minute 4 seconds
    Current LSP Uptime: 0 hour 1 minute 4 seconds
```

Similarly, the tunnel is set up successfully along the specified explicit path on Device2.

Step 5: Configure the binding relation of the master tunnel and the Bypass tunnel.

#Configure Device1, and the master tunnel enables the fast re-route function.

```
Device1(config)#interface tunnel 1
Device1(config-if-tunnel1)#tunnel mpls traffic-eng fast-reroute
Device1(config-if-tunnel1)#tunnel mpls traffic-eng record-route
Device1(config-if-tunnel1)#exit
```

#Configure Device2, bind the Bypass tunnel on the link of the protected node Device3, and enable RSVP-TE to link with BFD.

```
Device2(config)#interface tunnel 1
Device2(config-if-tunnel1)#tunnel mpls traffic-eng record-route
Device2(config-if-tunnel1)#exit
Device2(config)#interface gigabitethernet 1
Device2(config-if-gigabitethernet1)#mpls traffic-eng backup-path tunnel 1
Device2(config-if-gigabitethernet1)#ip rsvp bfd-signalling
Device2(config-if-gigabitethernet1)#exit
```

#Configure Device3, and enable RSVP-TE to link with BFD on the link with PLR.

```
Device3(config)#interface gigabitethernet 0
Device3(config-if-gigabitethernet0)#ip rsvp bfd-signalling
```

```
Device3(config-if-gigabitethernet0)#exit
```

#View the details of the MPLS P2P TE tunnel on Device1.

```
Device1#show mpls traffic-eng tunnels tunnel 1

*Tunnel 1  (Device1_t1)              Destination: 4.4.4.4
  Status:
    Admin: UP      Oper: UP (Using Primary LSP)   Signalling: Connected
    path option 1, type explicit 1 (Basis for Setup)

  Config Parameters:
    Reoptimize: Enabled  interval: 3600 seconds
    Update type: Make-before-break
    Auto Route:  Disabled
    Forwarding adjacency:  Disabled
    Bandwidth: 1m       Setup-priority: 7  Hold-priority: 0
    Affinity: include-any 0x0, include-all 0x0, exclude-any 0x0
    Explicit path: 1
    Record route: Enabled
    auto-bw: Disabled
    Fast-reroute:  FACILITY Enabled

  Tunnel Out-Label: 24016   gigabitethernet0


  RSVP-TE Signalling Info:
    Primary LSP:
      From 1.1.1.1,   To 4.4.4.4,   Tunnel-Id 1,   LSP-Id 1
      Status:  UP
      RSVP-TE Path Info:
        Explicit Route:  10.1.1.2       20.1.1.2       30.1.1.2
        Tspec: average rate 1m, burst rate 1m, peak rate 0
        Bandwidth: 1m       Setup-priority: 7  Hold-priority: 0
        Affinity: include-any 0x0, include-all 0x0, exclude-any 0x0
        Desires LINK local protection
      RSVP-TE Resv Info:
        Record Route (A: Local Protect Available):
                  10.1.1.2(A)       2.2.2.2(A)       20.1.1.2       3.3.3.3       30.1.1.2
```

```
                4.4.4.4
            Fspec: average rate 1m, burst rate 0, peak rate 0
            Out-Label: 24016   gigabitethernet0
            LSP Minimum MTU: 1500

        Other Info:
          Tunnel created:    4 days 20 hours
          Current LSP Uptime: 0 hour 0 minute 58 seconds
```

From the details of the master tunnel, you can see that the fast re-route function is enabled, the PLR information is recorded in the Record Route information, and the standby tunnel is available on PLR.

#On Device2, view the master tunnel and Bypass tunnel binding information.

```
Device2#show mpls traffic-eng tunnels summary
name              role   lspid  ingress      egress       ext-id       status   res-id
ref

Device2_t1        Ingress 2     2.2.2.2      4.4.4.4      2.2.2.2      up      32     1

Device1_t1        Transit 1     1.1.1.1      4.4.4.4      1.1.1.1      up      33     1
Device2_t1        Ingress 2     2.2.2.2      4.4.4.4      2.2.2.2      up      32     1
(backup)
```

You can see that the binding relation of the master tunnel and the Bypass tunnel is set up.

```
Device2#show mpls traffic-eng tunnels transit

*Tunnel  Device1_t1 (LSP-id 1)  Signalled from 1.1.1.1  Destination: 4.4.4.4

 In-Label:  24016   gigabitethernet0   Out-Label: 24016   gigabitethernet1

 RSVP-TE Signalling Info:
   Primary LSP:
     From 1.1.1.1,   To 4.4.4.4,   Tunnel-Id 1,   LSP-Id 1
     Status:  UP    Backup LSP READY at this node.
     RSVP-TE Path Info:
       Explicit Route:  20.1.1.2       30.1.1.2
       Tspec: average rate 1m, burst rate 1m, peak rate 0
       Bandwidth: 1m       Setup-priority: 7  Hold-priority: 0
       Desires LINK local protection
     RSVP-TE Resv Info:
```

```
    Record Route:   20.1.1.2      3.3.3.3      30.1.1.2      4.4.4.4
    Fspec: average rate 1m, burst rate 0, peak rate 0
    LSP Minimum MTU: 1500

  Bypass LSP:
    From 2.2.2.2,   To 4.4.4.4,   Tunnel-Id 1,   LSP-Id 2
    Status:  UP
    RSVP-TE Path Info:
      Explicit Route:  40.1.1.2      50.1.1.2
      Tspec: average rate 1m, burst rate 1m, peak rate 0
      Bandwidth: 1m      Setup-priority: 7  Hold-priority: 0
      Affinity: include-any 0x0, include-all 0x0, exclude-any 0x0
    RSVP-TE Resv Info:
      Record Route:   40.1.1.2      5.5.5.5      50.1.1.2      4.4.4.4
      Fspec: average rate 1m, burst rate 1m, peak rate 0
      Out-Label: 24016   gigabitethernet2
      LSP Minimum MTU: 1500
```

From the details of the master tunnel, you can see that the current node is bound with the Bypass tunnel successfully, and the protect for the master tunnel is ready.

#On Device2, view the BFD session information.

```
Device2#show bfd session
OurAddr          NeighAddr          LD/RD          State          Holddown
interface
20.1.1.1         20.1.1.2           6/1            UP             5000
gigabitethernet1
```

You can see that the BFD session is set uo successfully.

Step 6: Check the result.

#When the protected node Device3 fails, BFD fast detects the fault and informs the RSVP-TE protocol, and PLR switches the master tunnel to the Bypass tunnel at once.

#On Device1, view the details of the master tunnel.

```
Device1#show mpls traffic-eng tunnels tunnel 1

*Tunnel 1  (Device1_t1)              Destination: 4.4.4.4
  Status:
    Admin: UP      Oper: UP (Using Primary LSP)   Signalling: Connected
    path option 1, type explicit 1 (Basis for Setup)

  Config Parameters:
```

Reoptimize: Enabled interval: 3600 seconds
Update type: Make-before-break
Auto Route: Disabled
Forwarding adjacency: Disabled
Bandwidth: 1m Setup-priority: 7 Hold-priority: 0
Affinity: include-any 0x0, include-all 0x0, exclude-any 0x0
Explicit path: None
Record route: Enabled
auto-bw: Disabled
Fast-reroute: FACILITY Enabled

Tunnel Out-Label: 24016 gigabitethernet0

RSVP-TE Signalling Info:
Primary LSP:
From 1.1.1.1, To 4.4.4.4, Tunnel-Id 1, LSP-Id 1
Status: UP
RSVP-TE Path Info:
Explicit Route: 10.1.1.2 20.1.1.2 30.1.1.2
Tspec: average rate 1m, burst rate 1m, peak rate 0
Bandwidth: 1m Setup-priority: 7 Hold-priority: 0
Affinity: include-any 0x0, include-all 0x0, exclude-any 0x0
Desires LINK local protection
RSVP-TE Resv Info:
Record Route (A: Local Protect Available):
10.1.1.2(AU) 2.2.2.2(AU)
Using backup LSP at nodes marked (U).
Fspec: average rate 1m, burst rate 0, peak rate 0
Out-Label: 16 gigabitethernet0
LSP Minimum MTU: 1500

Last Error Info:
Notify Error(25), Tunnel locally repaired(3)
Node where Error originated: 10.1.1.2

Other Info:

```
    Tunnel created:     4 days 20 hours
    Current LSP Uptime: 0 hour 9 minutes 6 seconds
```

From the Record Route information, you can see that the Bypass tunnel is enabled on PLR.

#On Device2, view the master tunnel information and MPLS forwarding table information.

```
Device2#show mpls traffic-eng tunnels transit

*Tunnel  Device1_t1 (LSP-id 1)  Signalled from 1.1.1.1  Destination: 4.4.4.4

 In-Label:  24016   gigabitethernet0    Out-Label: 24016   gigabitethernet2

 RSVP-TE Signalling Info:
   Primary LSP:
     From 1.1.1.1,   To 4.4.4.4,   Tunnel-Id 1,   LSP-Id 1
     Status:  UP    Backup LSP is being USED at this node.
     RSVP-TE Path Info:
       Explicit Route:  20.1.1.2       30.1.1.2
       Tspec: average rate 1m, burst rate 1m, peak rate 0
       Bandwidth: 1m       Setup-priority: 7  Hold-priority: 0
       Desires LINK local protection
     RSVP-TE Resv Info:
       Record Route:    40.1.1.2       5.5.5.5       50.1.1.2       4.4.4.4
       Fspec: average rate 1m, burst rate 0, peak rate 0
       LSP Minimum MTU:

   Bypass LSP:
     From 2.2.2.2,   To 4.4.4.4,   Tunnel-Id 1,   LSP-Id 2
     Status:  UP
     RSVP-TE Path Info:
       Explicit Route:  40.1.1.2       50.1.1.2
       Tspec: average rate 1m, burst rate 1m, peak rate 0
       Bandwidth: 1m       Setup-priority: 7  Hold-priority: 0
       Affinity: include-any 0x0, include-all 0x0, exclude-any 0x0
     RSVP-TE Resv Info:
       Record Route:    40.1.1.2       5.5.5.5       50.1.1.2       4.4.4.4
       Fspec: average rate 1m, burst rate 1m, peak rate 0
       Out-Label: 16   gigabitethernet2
       LSP Minimum MTU: 1500
```

On Device2, you also can see that the Bypass tunnel is enabled on the node in the details of the master tunnel.

```
Device2#show mpls forwarding-table

Pro: L - LDP, O - OSPF, B - MP-BGP, R - RSVP, M - Mapped-Route, S - Static
Label,ML - mLDP (ML FEC: Root address/OT/OV), RM - RSVP P2MP (RM FEC: P2MP
ID/TID)


Pro Ident      FEC           Inlabel Outlabel Outgoing        Next hop
R   -TNL-      tunnel1       /       24016    gigabitethernet2 40.1.1.2
R   global     4.4.4.4/32    24016   3        tunnel1         40.1.1.2
```

You can see that the egress interface to the Egress node 4.4.4.4 is the Bypass tunnel Tunnel1, indicating that the data traffic is switched to the Bypass tunnel from the master tunnel.

4.3.5. Configure MPLS L3VPN over MPLS TE

Network Requirements

- PE1 and PE2 set up L3VPN; CE1 and CE2 communicate with each other via the VPN set up by PE1 and PE2.
- PE1, P, PE2 use the RSVP-TE protocol to distribute the global label, making the VPN data traffic be forwarded along the MPLS P2P TE tunnel.
- The required bandwidth of the MPLS P2P TE tunnel from PE1 to PE2, PE2 to PE1 is 1000kbps; the reserved bandwidth of the TE tunnel is 100000kbps.

Network Topology

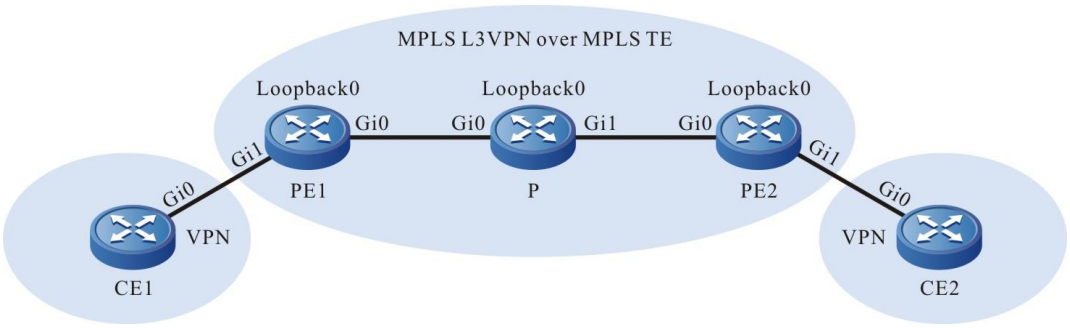

Figure 4-5 Configure MPLS L3VPN over MPLS TE

Device	Interface	IP Address	Device	Interface	IP Address
PE1	Gi0	10.1.1.1/24	PE2	Gi0	20.1.1.2/24
	Gi1	100.1.1.1/24		Gi1	110.1.1.1/24
	Loopback0	1.1.1.1/32		Loopback0	3.3.3.3/32
P	Gi0	10.1.1.2/24	CE1	Gi0	100.1.1.2/24

Device	Interface	IP Address	Device	Interface	IP Address
	Gi1	20.1.1.1/24	CE2	Gi0	110.1.1.2/24
	Loopback0	2.2.2.2/32			

Configuration Steps

Step 1: Configure the IP address of the interface (omitted).

Step 2: Configure the global OSPF protocol, cover the interfaces of PE, P, and PE2 to area 0, and area 0 of PE1, P, and PE2 enable the MPLS TE capability.

#Configure PE1.

```
PE1#configure terminal
PE1(config)#router ospf 100
PE1(config-ospf)#router-id 1.1.1.1
PE1(config-ospf)#network 10.1.1.0 0.0.0.255 area 0
PE1(config-ospf)#network 1.1.1.1 0.0.0.0 area 0
PE1(config-ospf)#mpls traffic-eng router-id 1.1.1.1
PE1(config-ospf)#mpls traffic-eng area 0
PE1(config-ospf)#exit
```

#Configure P.

```
P#configure terminal
P(config)#router ospf 100
P(config-ospf)#router-id 2.2.2.2
P(config-ospf)#network 10.1.1.0 0.0.0.255 area 0
P(config-ospf)#network 20.1.1.0 0.0.0.255 area 0
P(config-ospf)#network 2.2.2.2 0.0.0.0 area 0
P(config-ospf)#mpls traffic-eng router-id 2.2.2.2
P(config-ospf)#mpls traffic-eng area 0
P(config-ospf)#exit
```

#Configure PE2.

```
PE2#configure terminal
PE2(config)#router ospf 100
PE2(config-ospf)#router-id 3.3.3.3
PE2(config-ospf)#network 20.1.1.0 0.0.0.255 area 0
PE2(config-ospf)#network 3.3.3.3 0.0.0.0 area 0
PE2(config-ospf)#mpls traffic-eng router-id 3.3.3.3
PE2(config-ospf)#mpls traffic-eng area 0
```

```
PE2(config-ospf)#exit
```

Step 3: Enable the MPLS TE function and MPLS forwarding capability. Meanwhile, configure the maximum reserved bandwidth of the link passed by the MPLS P2P TE tunnel.

#Configure PE1, enable the MPLS TE function and MPLS forwarding capability globally and on the interface gigabitethernet0, and configure the maximum reserved bandwidth of the link on the interface gigabitethernet0 as 100000 kbps.

```
PE1(config)#mpls ip
PE1(config)#mpls traffic-eng tunnels
PE1(config-rsvp-te)#router-id 1.1.1.1
PE1(config-rsvp-te)#exit
PE1(config)#interface gigabitethernet 0
PE1(config-if-gigabitethernet0)#mpls ip
PE1(config-if-gigabitethernet0)#mpls traffic-eng tunnels
PE1(config-if-gigabitethernet0)#ip rsvp bandwidth 100000
PE1(config-if-gigabitethernet0)#exit
```

#Configure P, enable the MPLS TE function and MPLS forwarding capability globally and on the interface gigabitethernet0, gigabitethernet1, and configure the maximum reserved bandwidth of the link on the interface gigabitethernet0, gigabitethernet1 as 100000 kbps.

```
P(config)#mpls ip
P(config)#mpls traffic-eng tunnels
P(config-rsvp-te)#router-id 2.2.2.2
P(config-rsvp-te)#exit
P(config)#interface gigabitethernet 0
P(config-if-gigabitethernet0)#mpls ip
P(config-if-gigabitethernet0)#mpls traffic-eng tunnels
P(config-if-gigabitethernet0)#ip rsvp bandwidth 100000
P(config-if-gigabitethernet0)#exit
P(config)#interface gigabitethernet 1
P(config-if-gigabitethernet1)#mpls ip
P(config-if-gigabitethernet1)#mpls traffic-eng tunnels
P(config-if-gigabitethernet1)#ip rsvp bandwidth 100000
P(config-if-gigabitethernet1)#exit
```

#Configure PE2, enable the MPLS TE function and MPLS forwarding capability globally and on the interface gigabitethernet0, and configure the maximum reserved bandwidth of the link on the interface gigabitethernet0 as 100000 kbps.

```
PE2(config)#mpls ip
PE2(config)#mpls traffic-eng tunnels
```

```
PE2(config-rsvp-te)#router-id 3.3.3.3
PE2(config-rsvp-te)#exit
PE2(config)#interface gigabitethernet 0
PE2(config-if-gigabitethernet0)#mpls ip
PE2(config-if-gigabitethernet0)#mpls traffic-eng tunnels
PE2(config-if-gigabitethernet0)#ip rsvp bandwidth 100000
PE2(config-if-gigabitethernet0)#exit
```

Step 4: Create one MPLS P2P TE tunnel and configure the MPLS TE auto route.

#Configure PE1, create one MPLS P2P TE tunnel Tunnel1, and configure the required bandwidth of the tunnel as 1000kbps.

```
PE1(config)#interface tunnel 1
PE1(config-if-tunnel1)#tunnel mode mpls traffic-eng
PE1(config-if-tunnel1)#ip unnumbered loopback 0
PE1(config-if-tunnel1)#tunnel destination 3.3.3.3
PE1(config-if-tunnel1)#tunnel mpls traffic-eng bandwidth 1000
PE1(config-if-tunnel1)#tunnel mpls traffic-eng autoroute announce
PE1(config-if-tunnel1)#exit
```

#Configure PE2, create one MPLS P2P TE tunnel Tunnel1, and configure the required bandwidth of the tunnel as 1000kbps.

```
PE2(config)#interface tunnel 1
PE2(config-if-tunnel1)#tunnel mode mpls traffic-eng
PE2(config-if-tunnel1)#ip unnumbered loopback 0
PE2(config-if-tunnel1)#tunnel destination 1.1.1.1
PE2(config-if-tunnel1)#tunnel mpls traffic-eng bandwidth 1000
PE2(config-if-tunnel1)#tunnel mpls traffic-eng autoroute announce
PE2(config-if-tunnel1)#exit
```

#On PE1, view the MPLS P2P TE tunnel information.

```
PE1#show mpls traffic-eng tunnels summary
name                role   lspid  ingress      egress       ext-id       status  res-id
ref

PE1_t1              Ingress 1     1.1.1.1      3.3.3.3      1.1.1.1      up      8       1

PE2_t1              Egress  1     3.3.3.3      1.1.1.1      3.3.3.3      up      0       1
```

You can see that the tunnel PE1_t1 from PE1 to PE2 is set up normally and the status is UP; similarly, the tunnel PE2_t1 from PE2 to PE1 is also set up successfully.

Step 5: Configure the VPN instance; CE and PE advertise the route via the OSPF protocol.

#Configure PE1.

```
PE1(config)#ip vrf 1
PE1(config-vrf)#rd 100:1
PE1(config-vrf)#route-target export 100:1
PE1(config-vrf)#route-target import 100:1
PE1(config-vrf)#exit
PE1(config)#interface gigabitethernet 1
PE1(config-if-gigabitethernet1)#ip vrf forwarding 1
PE1(config-if-gigabitethernet1)#ip address 100.1.1.1 255.255.255.0
PE1(config-if-gigabitethernet1)#exit
PE1(config)#router ospf 200 vrf 1
PE1(config-ospf)#network 100.1.1.0 0.0.0.255 area 0
PE1(config-ospf)#exit
```

#Configure CE1.

```
CE1#configure terminal
CE1(config)#router ospf 100
CE1(config-ospf)#network 100.1.1.0 0.0.0.255 area 0
CE1(config-ospf)#exit
```

#Configure PE2.

```
PE2(config)#ip vrf 1
PE2(config-vrf)#rd 100:1
PE2(config-vrf)#route-target export 100:1
PE2(config-vrf)#route-target import 100:1
PE2(config-vrf)#exit
PE2(config)#interface gigabitethernet 1
PE2(config-if-gigabitethernet1)#ip vrf forwarding 1
PE2(config-if-gigabitethernet1)#ip address 110.1.1.1 255.255.255.0
PE2(config-if-gigabitethernet1)#exit
PE2(config)#router ospf 200 vrf 1
PE2(config-ospf)#network 110.1.1.0 0.0.0.255 area 0
PE2(config-ospf)#exit
```

#Configure CE2.

```
CE2#configure terminal
CE2(config)#router ospf 100
CE2(config-ospf)#network 110.1.1.0 0.0.0.255 area 0
CE2(config-ospf)#exit
```

Step 6: Configure MP-IBGP, use the Loopback0 address of PE as the peer address, and re-distribute the route with the IGP protocol in the VPN instance.

#Configure PE1.

```
PE1(config)#router bgp 100
PE1(config-bgp)#neighbor 3.3.3.3 remote-as 100
PE1(config-bgp)#neighbor 3.3.3.3 update-source loopback 0
PE1(config-bgp)#address-family vpnv4
PE1(config-bgp-af)#neighbor 3.3.3.3 activate
PE1(config-bgp-af)#neighbor 3.3.3.3 send-community extended
PE1(config-bgp-af)#exit-address-family
PE1(config-bgp)#address-family ipv4 vrf 1
PE1(config-bgp-af)#redistribute ospf 200
PE1(config-bgp-af)#exit-address-family
PE1(config-bgp)#exit
PE1(config)#router ospf 200 vrf 1
PE1(config-ospf)#redistribute bgp 100
PE1(config-ospf)#exit
```

#Configure PE2.

```
PE2(config)#router bgp 100
PE2(config-bgp)#neighbor 1.1.1.1 remote-as 100
PE2(config-bgp)#neighbor 1.1.1.1 update-source loopback 0
PE2(config-bgp)#address-family vpnv4
PE2(config-bgp-af)#neighbor 1.1.1.1 activate
PE2(config-bgp-af)#neighbor 1.1.1.1 send-community extended
PE2(config-bgp-af)#exit-address-family
PE2(config-bgp)#address-family ipv4 vrf 1
PE2(config-bgp-af)#redistribute ospf 200
PE2(config-bgp-af)#exit-address-family
PE2(config-bgp)#exit
PE2(config)#router ospf 200 vrf 1
PE2(config-ospf)#redistribute bgp 100
PE2(config-ospf)#exit
```

#On the PE, view the BGP neighbor information.

Take PE1 as an example:

```
PE1#show ip bgp vpnv4 all summary
BGP router identifier 1.1.1.1, local AS number 100
```

```
BGP table version is 6
1 BGP AS-PATH entries
0 BGP community entries

Neighbor        V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
3.3.3.3         4   100      92      93        6    0    0 01:18:23        1

Total number of neighbors 1
```

You can see that the BGP neighbor is already set up.

#On the PE, view the BGP VPNv4 route information and the VPN route information.

Take PE1 as an example:

```
PE1#show ip bgp vpnv4 all
BGP table version is 3, local router ID is 1.1.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network          Next Hop            Metric LocPrf Weight Path
Route Distinguisher: 100:1 (Default for VRF 1)
[0]*> 100.1.1.0/24     0.0.0.0                  1         32768 ?
[B]*>i110.1.1.0/24     3.3.3.3                  1    100      0 ?

PE1#show ip route vrf 1
Codes: C - Connected, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external



C   100.1.1.0/24 is directly connected, 00:50:09, gigabitethernet1
B   110.1.1.0/24 [200/1] via 3.3.3.3, 00:43:00, tunnel1
```

In the BGP VPNv4 route information and VPN route information of PE1, there is the route 110.1.1.0/24, and the egress interface points to Tunnel1.

#On the PE, view the MPLS forwarding information.

Take PE1 as an example:

```
PE1#show mpls forwarding-table

Pro: L - LDP, O - OSPF, B - MP-BGP, R - RSVP, M - Mapped-Route, S - Static
Label,ML - mLDP (ML FEC: Root address/OT/OV), RM - RSVP P2MP (RM FEC: P2MP
ID/TID)
```

```
Pro Ident       FEC              Inlabel Outlabel Outgoing          Next hop
B  1            110.1.1.0/24[V]  /       24240    tunnel1           3.3.3.3
R  -TNL-        tunnel1          /       24017    gigabitethernet0  10.1.1.2
B  1            100.1.1.0/24     24240   /        /
```

In the MPLS forwarding information of PE1, the egress interface of the VPN route is Tunnel1, indicating that the VPN data traffic is forwarded along the MPLS P2P TE tunnel.

Step7: Check the result.

#On CE1, use the ping command to check the connectivity with CE2.

```
CE1#ping 110.1.1.2

Press key (ctrl + shift + 6) interrupt it.
Sending 5, 76-byte ICMP Echos to 100.1.1.2 , timeout is 2 seconds:
!!!!!
Success rate is 100% (5/5). Round-trip min/avg/max = 0/0/0 ms.
```

CE1 can communicate with CE2 normally.

5. MPLS OAM

5.1. Overview

The MPLS OAM function is used to detect and maintain the fault in the MPLS network, including MPLS LSP Ping/Traceroute and MPLS BFD two sub function. The MPLS LSP Ping/Traceroute function is common detection tool and can detect the end-to-end LSP connectivity and the consistency of the control plane and data plane.

5.2. MPLS OAM Function Configuration

Table 5-1 MPLS OAM function configuration list

Configuration Task	
Configure MPLS OAM function	Enable the MPLS OAM function
Use MPLS LSP Ping/Traceroute to detect LSP	MPLS LSP Ping function
	MPLS LSP Traceroute function
	Interactive MPLS LSP Ping function
	Interactive MPLS LSP Traceroute function
Configure LSP Ping to detect LSP periodically	Configure LSP Ping to detect the connectivity of the static SR LSP periodically

5.2.1. Configure MPLS OAM Functions

Configuration Condition

Before configuring the MPLS OAM function, first complete the following task:

- Configure the MPLS basic functions, ensuring that the MPLS packet can be received and sent normally.

Enable MPLS OAM Function

Table 5-2 Enable the MPLS OAM function

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enable the MPLS OAM function and enter the MPLS OAM configuration mode	**mpls oam**	Mandatory By default, do not enable the MPLS OAM function.

5.2.2. Use MPLS LSP Ping/Traceroute to Detect LSP

Configuration Condition

To detect the validity of the detection result, complete the following task before using MPLS LSP Ping/Traceroute to detect the LSP:

- When using MPLS LSP Ping detection, it is necessary to enable the MPLS OAM function on the Ingress node and Egress node of LSP.
- When using MPLS LSP Traceroute detection, it is necessary to enable the MPLS OAM function on all nodes of the LSP path.

MPLS LSP Ping Function

MPLS LSP Ping detects the LSP connectivity by receiving and sending the echo request and echo reply packet, The echo request packet sent by the Ingress node carries the label to the specified FEC. The detected LSP sends the packet to the Egress node, and the Egress node processes and returns the echo reply packet. If the the echo reply packet received by the Ingress node does not have error information, it indicates that the detected LSP is reachable. If not receiving the echo reply packet or the received echo reply packet carries the error TLV, it indicates that the detected LSP is unreachable.

Table 5-3 MPLS LSP Ping function

Step	Command	Description
Use the ping command to detect the LSP connectivity	**ping mpls** [{ **ipv4** *prefix-address prefix-mask-length* [**destination** *address-start address-end address-increment*] | **vrf** *vrf-name* **ipv4** *prefix-address prefix-mask-length* [**destination** *address-start address-end address-increment*] | **traffic-eng tunnel** *tunnel-unit* } [**ttl** *time-to-live* / **source** *source-address* / **repeat** *count* / **timeout** *seconds* / **size** *packet-size* / **sweep** *minimum-size maximum-size size-increment* / **pad** *pattern* / **reply-pad-tlv** / **reply-mode** { **ipv4** | **router-alert** } / **interval** *msec* / **exp** *exp-bits* / **verbose**]]	Mandatory

MPLS LSP Traceroute Function

MPLS LSP Traceroute is used to detect the reachability of each hop and the label consistency on the LSP path. The Ingress node sends the echo request packet by adding the TTL, and receives the echo reply packet returned by each hop on the LSP path, so as to discover the information of each hop on the LSP path until reaching Egress.

Table 5-4 MPLS LSP Traceroute function

Step	Command	Description
Detect the reachability of each hop and the label consistency on the LSP path	**traceroute mpls** [{ **ipv4** *prefix-address prefix-mask-length* [**destination** *address-start address-end address-increment*] | **vrf** *vrf-name* **ipv4** *prefix-address prefix-mask-length* [**destination** *address-start address-end address-increment*] | **traffic-eng tunnel** *tunnel-unit* } [**ttl** *time-to-live* / **source** *source-address* / **timeout** *seconds* / **reply-pad-tlv** / **reply-mode** { **ipv4** | **router-alert** } / **exp** *exp-bits*]]	Mandatory

Interactive MPLS LSP Ping Function

Table 5-5 Interactive MPLS LSP Ping function

Step	Command	Description
Enter the ping mpls interactive mode	**ping mpls**	-
Specify the detected FEC type	**Target ipv4, traffic-eng, or vrf** [**ipv4**]**:** [**ipv4** | **traffic-eng** | **vrf**]	Mandatory By default, the FEC type is ipv4.
Specify the IPv4 address of the detected FEC	**Target IPv4 address:** { *prefix-address* }	Mandatory
Specify the IPv4 mask length of the detected FEC	**Target mask length** [**32**]**:** [*prefix-mask-length*]	Optional By default, the IPv4 mask length is 32.
Specify the times of sending the same MPLS echo request packet repeatedly	**Repeat count** [**5**]**:** [*count*]	Optional By default, the times of sending the packet repeatedly is 5.
Specify the length of the MPLS echo request packet	**Datagram size** [**150**]**:** [*packet-size*]	Optional By default, the packet length is 150 bytes.
Specify the timeout of the MPLS echo request packet	**Timeout in seconds** [**2**]**:** [*seconds*]	Optional By default, the timeout is 2s.
Specify the interval of sending the MPLS echo request packet	**Send interval in msec** [**0**]**:** [*msec*]	Optional By default, the interval of sending the MPLS echo request packet is 0ms.
Select whether to enable the MPLS OAM function extended option	**Extended command?** [**no**]**:** [**yes** | **no**]	Optional By default, the extended option is not enabled.

Step	Command	Description
Specify the start address of the MPLS echo request packets sent by increasing the destination IPv4 address	**Destination address or destination start address** [**127.0.0.1**]**:** [*address-start*]	Optional By default, the destination address of the sent MPLS echo request packet does not increase, but is fixed as 127.0.0.1.
Specify the end address of the MPLS echo request packets sent by increasing the destination IPv4 address	**Destination end address:** [*address-end*]	Optional
Specify the address increment of the MPLS echo request packets sent by increasing the destination IPv4 address	**Destination address increment** [**0.0.0.1**]**:** [*address-increment*]	Optional By default, the increment value is 0.0.0.1.
Specify the IPv4 source address of the MPLS echo request packet	**Source address:** [*source-address*]	Optional
Specify the value of the EXP field in the MPLS label of the MPLS echo request packet	**EXP bits in mpls header** [**0**]**:** [*exp-bits*]	Optional By default, the value of the EXP field in the label is 0.
Specify the filling value in the pad TLV of the MPLS echo request packet	**Pad TLV pattern** [**0xABCD**]**:** [*pattern*]	Optional By default, the filling value in pad TLV is 0xABCD.
Specify whether to contain pad TLV in the MPLS echo reply packet	**Reply Pad TLV?** [**no**]**:** [**yes** | **no**]	Optional By default, do not contain pad TLV in the MPLS echo reply packet.
Set the TTL of the outermost label of the MPLS echo request packet	**Time To Live** [**255**]**:** [*time-to-live*]	Optional By default, the TTL value of the outermost label is 255.

Step	Command	Description
Specify the reply mode of the MPLS echo reply packet	**Reply mode** (**2-ipv4 via udp, 3-ipv4 via udp with router alert**) [**2**]**:**	Optional By default, the reply mode is 2, that is, return by the IPv4 UDP packet.
Select whether to display the result of the MPLS LSP Ping operation in the detail mode	**Verbose mode?** [**no**]**:** [**yes** | **no**]	Optional By default, display the result of the MPLS LSP Ping operation in the simple mode.
Select whether to send the MPLS echo request packet by increasing the length	**Sweep range of sizes?** [**no**]**:** [**yes** | **no**]	Optional By default, send the MPLS echo request packet by the fixed packet length.
Specify the start value of the sent MPLS echo request packet length	**Sweep min size** [**150**]**:** [*minimum-size*]	Optional By default, the start value of the packet length is 150 bytes.
Specify the maximum value of the sent MPLS echo request packet length	**Sweep max size** [**18024**]**:** [*maximum-size*]	Optional By default, the maximum value of the increment of the packet length is 18024 bytes.
Specify the length increment of the sent MPLS echo request packet	**Sweep interval** [**100**]**:** [*size-increment*]	Optional By default, the length increment is 100 bytes.

Interactive MPLS LSP Traceroute Function

Table 5-6 Interactive MPLS LSP Traceroute function

Step	Command	Description
Enter the traceroute mpls interactive mode	**traceroute mpls**	-
Specify the type of the detected FEC	**Target ipv4, traffic-eng, or vrf** [**ipv4**]**:** [**ipv4** | **traffic-eng** | **vrf**]	Mandatory By default, the FEC type is ipv4.
Specify the IPv4 address of the detected FEC	**Target IPv4 address:** { *prefix-address* }	Mandatory
Specify the IPv4 mask length of the detected FEC	**Target mask length** [**32**]**:** [*prefix-mask-length*]	Optional By default, the IPv4 mask length is 32.
Specify the timeout of the MPLS echo request packet	**Timeout in seconds** [**2**]**:** [*seconds*]	Optional By default, the timeout is 2s.
Select whether to enable the MPLS OAM function extended option	**Extended command?** [**no**]**:** [**yes** | **no**]	Optional By default, the extended option is not enabled.
Specify the start address of sending the MPLS echo request packet by increasing the destination IPv4 address	**Destination address or destination start address** [**127.0.0.1**]**:** [*address-start*]	Optional By default, the destination address of sending the MPLS echo request packet does not increase, but is fixed as 127.0.0.1.
Specify the end address of sending the MPLS echo request packet by increasing the destination IPv4 address	**Destination end address:** [*address-end*]	Optional
Specify the address increment of sending the MPLS echo request packet by increasing the destination IPv4 address	**Destination address increment** [**0.0.0.1**]**:** [*address-increment*]	Optional By default, the increment is 0.0.0.1.

Step	Command	Description
Specify the IPv4 source packet of the MPLS echo request packet	**Source address:** [*source-address*]	Optional
Specify the value of the EXP field in the MPLS label of the MPLS echo request packet	**EXP bits in mpls header [0]:** [*exp-bits*]	Optional By default, the value of the EXP field in the MPLS label of the MPLS echo request packet is 0.
Specify whether to contain pad TLV in the MPLS echo reply packet	**Reply Pad TLV?** [**no**]**:** [**yes** | **no**]	Optional By default, the MPLS echo reply packet does not contain pad TLV.
Set the TTL incremental maximum value of the outermost label of the MPLS echo request packet	**Time To Live** [**30**]**:** [*time-to-live*]	By default, the TTL incremental maximum value of the outermost label of the MPLS echo request packet is 30.
Specify the reply mode of the MPLS echo request packet	**Reply mode** (**2-ipv4 via udp, 3-ipv4 via udp with router alert**) [**2**]**:**	Optional

5.2.3. Configure MPLS BFD to Detect LSP

Configuration Condition

None

Configure MPLS BFD Global Parameters

Table 5-7 Configure MPLS BFD global parameters

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enable the MPLS OAM function and enter the MPLS OAM configuration mode	**mpls oam**	-
Enable MPLS OAM to link with BFD	**bfd enable**	Mandatory By default, do not enable MPLS OAM to link with BFD.
Configure the global minimum receive interval of the MPLS BFD control packet	**bfd min-receive-interval** *receive-interval-value*	Optional By default, the global minimum receive interval of the MPLS BFD control packet is 1000ms.
Configure the global minimum transmit interval of the MPLS BFD control packet	**bfd min-transmit-interval** *transmit-interval-value*	Optional By default, the global minimum transmit interval of the MPLS BFD control packet is 1000ms.
Configure the global detection timeout multiplier of the MPLS BFD control packet	**bfd multiplier** *multiplier-value*	Optional By default, the global detection timeout multiplier of the MPLS BFD control packet is 5.

Note:

- To use BFD to detect the LSP connectivity, it is necessary to enable MPLS OAM to link with BFD on the Ingress node and Egress node of the detected LSP.
- To configure the global detection timeout multiplier of the MPLS BFD control packet, first enable MPLS OAM to link with BFD.
- The detection parameters of the MPLS BFD session can be configured globally in a unified manner, and also can be configured based on the session. If the two modes are configured at the same time, the session-based configuration is prior.
- If disabling MPLS OAM from linking with BFD, all configurations of the MPLS BFD function will be deleted.

Configure MPLS BFD to Detect the Connectivity of LDP IPv4 FEC LSP

Table 5-8 Configure MPLS BFD to detect the connectivity of the LDP IPv4 FEC LSP

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enable the MPLS OAM function and enter the MPLS OAM configuration mode	**mpls oam**	-
Enable MPLS OAM to link with BFD	**bfd enable**	Mandatory By default, do not enable MPLS OAM to link with BFD.
Configure MPLS BFD to detect the connectivity of the LDP IPv4 FEC LSP	**bfd ipv4** *prefix-address prefix-mask-length* [**nexthop** *nexthop-address* **[discriminator-local** *local-discriminator* **discriminator-remote** *remote-discriminator*]] [**min-receive-interval** *receive-interval-value* **min-transmit-interval** *transmit-interval-value* **multiplier** *multiplier-value*]	Mandatory By default, do not configure MPLS BFD to detect the connectivity of the LDP IPv4 FEC LSP.

Note:

- To configure BFD to detect the connectivity of LDP IPv4 FEC LSP successfully, first enable MPLS OAM to link with BFD.
- The detection parameters of the MPLS BFD session can be configured globally in a unified manner, and also can be configured based on the session. If the two modes are configured at the same time, the session-based configuration is prior.
- When configuring the static MPLS BFD session, the configured authentication values on two sides of devices must match, that is, the configured local authentication value of the local device is the same as the remote authentication value on the remote device, the configured remote authentication value on the local device is the same as the local authentication value on the remote device.
- When configuring BFD to detect the connectivity of LDP IPv4 FEC LSP, you can specify the next hop. If not specifying the next hop, automatically create one MPLS BFD session for each next hop respectively. The two modes cannot be configured at the same time. When configuring the static mode, you must specify the next hop.

Configure MPLS BFD to Detect the Connectivity of MPLS TE FEC LSP

Table 5-9 Configure MPLS BFD to detect the connectivity of the MPLS TE FEC LSP

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enable the MPLS OAM function and enter the MPLS OAM configuration mode	**mpls oam**	-
Enable MPLS OAM to link with BFD	**bfd enable**	Mandatory By default, do not enable MPLS OAM to link with BFD.
Configure MPLS BFD to detect the connectivity of the MPLS TE FEC LSP	**bfd traffic-eng tunnel** *tunnel-unit* [**discriminator-local** *local-discriminator* **discriminator-remote** *remote-discriminator*] [**min-receive-interval** *receive-interval-value* **min-transmit-interval** *transmit-interval-value* **multiplier** *multiplier-value*]	Mandatory By default, do not configure MPLS BFD to detect the connectivity of the MPLS TE FEC LSP

Note:

- To configure BFD to detect the connectivity of MPLS TE FEC LSP successfully, first enable MPLS OAM to link with BFD.
- The detection parameters of the MPLS BFD session can be configured globally in a unified manner, and also can be configured based on the session. If the two modes are configured at the same time, the session-based configuration is prior.
- When configuring the static MPLS BFD session, the configured authentication values on two sides of devices must match, that is, the configured local authentication value of the local device is the same as the remote authentication value on the remote device, the configured remote authentication value on the local device is the same as the local authentication value on the remote device.

Configure MPLS BFD to Detect Connectivity of Static SR LSP

Table 5-10 Configure MPLS BFD to detect the connectivity of the static SR LSP

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enable the MPLS OAM function and enter the MPLS OAM configuration mode	**mpls oam**	-
Enable MPLS OAM to link with BFD	**bfd enable**	Mandatory By default, do not enable MPLS OAM to link with BFD.
Configure MPLS BFD to detect the connectivity of the static SR LSP	**bfd static-sr lsp** *lsp-name* **discriminator-local** *local-discr-value* **discriminator-remote** *remote-discr-value* [**min-receive-interval** *recv-interval-value* **min-transmit-interval** *trans-interval-value* **multiplier** *mult-value*]	Mandatory By default, do not configure MPLS BFD to detect the connectivity of the static SR LSP.

Note:

- The linkage function between MPLS OAM and BFD must be enabled before BFD can be successfully configured to detect the connectivity of static SR LSP.
- The detection parameters of MPLS BFD session can be configured globally or based on the session. If they are configured at the same time, the session-based configuration takes precedence.
- Only the static MPLS BFD session detection can be configured to detect the connectivity of the static SR LSP. The authentication values configured on the devices at both ends must match, that is, the local authentication value configured on the local device is the same as the remote authentication value configured on the remote device, and the remote authentication value configured on the local device is the same as the local authentication value configured on the remote device.
- BFD static session and periodic LSP Ping cannot be configured simultaneously for a static SR LSP for connectivity detection.

5.2.4. Configure Periodic LSP Ping to Detect LSP

Configuration Conditions

None

Configure Periodic LSP Ping to Detect Static SR LSP Connectivity

Table 5-11 Configure the periodic LSP Ping to detect the static SR LSP connectivity

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enable the MPLS OAM function and enter the MPLS OAM configuration mode	**mpls oam**	-
Configure the periodic LSP Ping to detect the static SR LSP connectivity	**periodic-ping static-sr lsp** *lsp-name*	Mandatory By default, do not Configure the periodic LSP Ping to detect the static SR LSP connectivity.

Note:

- Periodic LSP Ping and BFD static sessions cannot be configured simultaneously for a static SR LSP for connectivity detection.

5.2.5. MPLS OAM Monitoring and Maintaining

Table 5-12 MPLS OAM monitoring and maintaining

Command	Description
show mpls oam client [*client-name* | **target-fec** { **ipv4** *prefix-address prefix-mask-length* [**nexthop** *nexthop-address*] | **static-sr lsp** *lsp-name* | **traffic-eng tunnel** *tunnel-unit* }]**show mpls oam bfd client** [*client-name* | **target-fec** { **ipv4** *prefix-address prefix-mask-length* [**nexthop** *nexthop-address*] | **traffic-eng tunnel** *tunnel-unit* }]	Display the MPLS BFDOAM client registration information
show mpls oam periodic-ping entity [**static-sr lsp** [*lsp-name*]] [**detail**]	Display periodic LSP ping entity information
show mpls oam periodic-ping unit [**static-sr lsp** [*lsp-name*]] [**detail**]	Display periodic LSP Ping unit information

5.3. MPLS OAM Typical Configuration Example

5.3.1. Configure Using MPLS LSP Ping to Detect LSP

Network Requirements

- In the MPLS L3VPN network, use the LSP Ping to detect the connectivity of MPLS LSP and the consistency of the control plane and data plane.

Network Topology

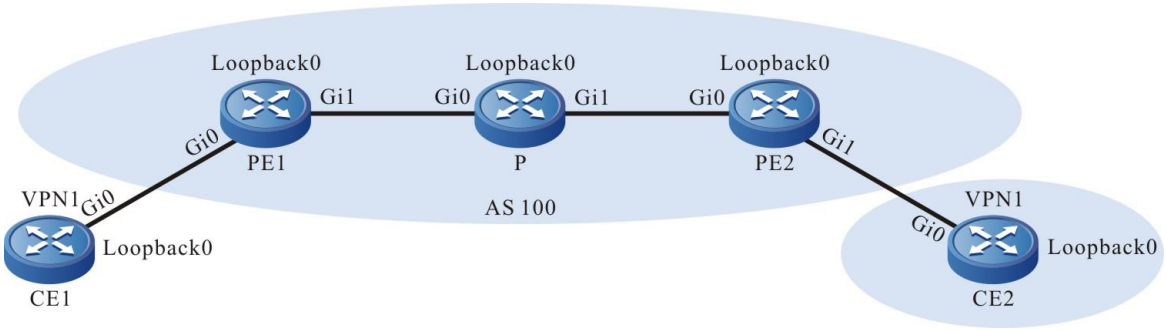

Figure 5-1 Use MPLS LSP Ping to detect LSP

Device	Interface	IP Address	Device	Interface	IP Address
CE1	Gi0	10.1.1.1/24	P	Loopback0	22.22.22.22/32
	Loopback0	1.1.1.1/32	PE2	Gi0	10.1.3.2/24
PE1	Gi0	10.1.1.2/24		Gi1	10.1.4.1/24
	Gi1	10.1.2.1/24		Loopback0	33.33.33.33/32
	Loopback0	11.11.11.11/32	CE2	Gi0	10.1.4.2/24
P	Gi0	10.1.2.2/24		Loopback0	2.2.2.2/32
	Gi1	10.1.3.1/24			

Configuration Steps

Step 1: Configure the interface IP address; CE1, PE1, P and PE2, CE2 form the MPLS L3VPN network; CE1 and CE2 can communicate with each other; VRF on PE1 is 1 (omitted, refer to the configuration manual-the MPLS L3VPN chapter).

Step 2: On the Ingress node and Egress node of the detected LSP, configure MPLS OAM.

#On PE1, configure MPLS OAM.

```
PE1#configure terminal
PE1(config)#mpls oam
```

#On PE2, configure MPLS OAM.

```
PE2#configure terminal
PE2(config)#mpls oam
```

Step 3: Check the result.

#On the PE, perform the LSP ping operation.

Take PE1 as an example:

```
PE1#ping mpls ipv4 33.33.33.33 32

Sending 5, 120-byte MPLS Echos to 33.33.33.33/32, TTL is 255, timeout is 2 seconds:

Codes: '!' - success, 'Q' - request not transmitted,
    '.' - timeout, 'U' - unreachable,
    'R' - downstream router but not destination,
    'M' - malformed request,
    'MR' - malformed reply

Press key (ctrl + shift + 6) to abort.
!!!!!
Success rate is 100% percent (5/5), round-trip min/avg/max = 0/0/0 ms.
```

You can see that when PE1 pings the Loopback0 interface of PE2, PE1 sends five echo request packets to the egress LSR PE2 successively, and receives the echo reply packet from PE2.

```
PE1#ping mpls vrf 1 ipv4 2.2.2.2 32

Sending 5, 120-byte MPLS Echos to vrf 1 2.2.2.2/32, TTL is 255, timeout is 2 seconds:

Codes: '!' - success, 'Q' - request not transmitted,
    '.' - timeout, 'U' - unreachable,
    'R' - downstream router but not destination,
    'M' - malformed request,
    'MR' - malformed reply

Press key (ctrl + shift + 6) to abort.
!!!!!
Success rate is 100% percent (5/5), round-trip min/avg/max = 0/3/16 ms.
```

You can see that when PE1 pings the Loopback0 interface of CE2, PE1 sends five echo request packets to CE2 successively, and receives the echo reply packet from CE2.

Note:

- For the checking method of PE2, refer to PE1.

5.3.2. Configure Using MPLS LSP Traceroute to Detect LSP

Network Requirements

- In the MPLS L3VPN network, use LSP Traceroute to detect the connectivity of MPLS LSP and the consistency of the control plane and data plane, and discover each hop on LSP.

Network Topology

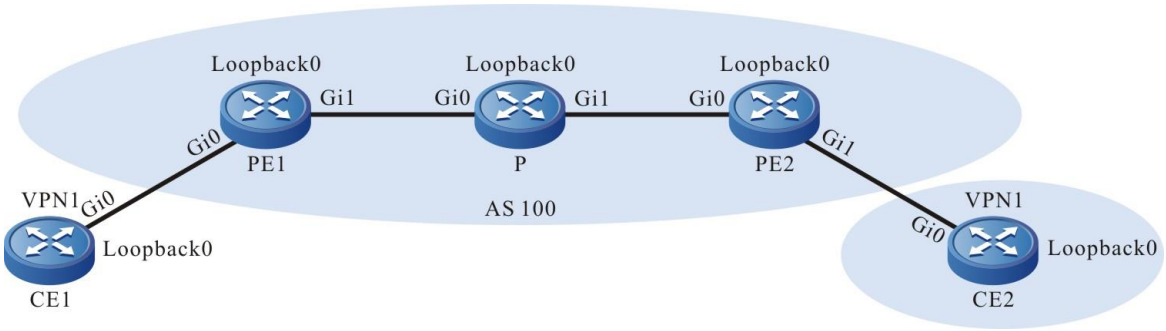

Figure 5-2 Use LSP Traceroute to detect LSP

Device	Interface	IP Address	Device	Interface	IP Address
CE1	Gi0	10.1.1.1/24	P	Loopback0	22.22.22.22/32
	Loopback0	1.1.1.1/32	PE2	Gi0	10.1.3.2/24
PE1	Gi0	10.1.1.2/24		Gi1	10.1.4.1/24
	Gi1	10.1.2.1/24		Loopback0	33.33.33.33/32
	Loopback0	11.11.11.11/32	CE2	Gi0	10.1.4.2/24
P	Gi0	10.1.2.2/24		Loopback0	2.2.2.2/32
	Gi1	10.1.3.1/24			

Configuration Steps

Step 1: Configure the interface IP address; CE1, PE1, P and PE2, CE2 form the MPLS L3VPN network; CE1 and CE2 can communicate with each other; VRF on PE1 is 1 (omitted, refer to the configuration manual-the MPLS L3VPN chapter).

Step 2: On all nodes passed by the detected LSP, configure MPLS OAM.

#On PE1, configure MPLS OAM.

```
PE1#configure terminal
PE1(config)#mpls oam
```

#On P, configure MPLS OAM.

```
P#configure terminal
P(config)#mpls oam
```

#On PE2, configure MPLS OAM.

```
PE2#configure terminal
PE2(config)#mpls oam
```

Step 3: Check the result.

#On PE, CE, perform the LSP Traceroute operation.

Take PE1 as an example:

```
PE1#traceroute mpls ipv4 33.33.33.33 32

Tracing MPLS Label Switched Path to 33.33.33.33/32, timeout is 2 seconds:

Codes: '!' - success, 'Q' - request not transmitted,
    '.' - timeout, 'U' - unreachable,
    'R' - downstream router but not destination,
    'M' - malformed request,
    'MR' - malformed reply

Press key (ctrl + shift + 6) to abort.

  0 10.1.2.1 mtu 1500 [Labels: 24001 EXP: 0]
R 1 10.1.2.2 mtu 1500 [Labels: 3 EXP: 0] 0 ms
! 2 10.1.3.2 0 ms
```

You can see the path of the packet forwarded from PE1 to PE2 Loopback0 address and the label information of each hop.

```
PE1#traceroute mpls vrf 1 ipv4 2.2.2.2 32

Tracing MPLS Label Switched Path to vrf 1 2.2.2.2/32, timeout is 2 seconds:

Codes: '!' - success, 'Q' - request not transmitted,
    '.' - timeout, 'U' - unreachable,
    'R' - downstream router but not destination,
    'M' - malformed request,
```

```
'MR' - malformed reply

Press key (ctrl + shift + 6) to abort.

 0 10.1.2.1 mtu 1500 [Labels: 24001/24000 EXP: 0/0]
R 1 10.1.2.2 mtu 1500 [Labels: 3/24000 EXP: 0/0] 0 ms
! 2 10.1.3.2 0 ms
```

You can see the path of the packet forwarded from PE1 to CE2 Loopback0 address and the label information of each hop.

Note:

- For the checking method of PE2, refer to PE1.

5.3.3. Configure Dynamic MPLS BFD to Detect the Connectivity of LDP IPv4 FEC LSP

Network Requirements

- Configure the dynamic MPLS BFD to detect the connectivity of the LSP with the FEC type as LDP IPv4 FEC and the destination address as Device3 on Device1.

Network Topology

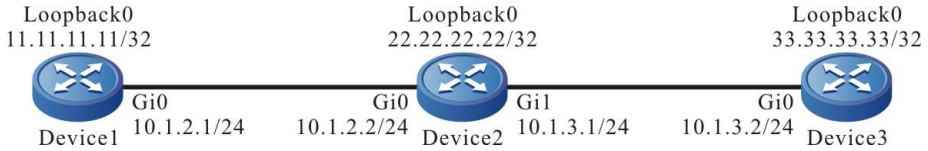

Figure 5-3 Configure the dynamic MPLS BFD to detect the connectivity of LDP IPv4 FEC LSP

Configuration Steps

Step 1: Configure the IP address of the interface, and set up the LDP IPv4 LSP from Device1 to Device3 (omitted, refer to “MPLS LDP Function Configuration” of the configuration manual).

Step 2: Enable MPLS OAM BFD on Device1.

```
Device1#configure terminal
Device1(config)#mpls oam
Device1(config-mpls-oam)#bfd enable
```

Step 3: On Device1, configure the dynamic BFD to detect the connectivity of the LSP with the FEC destination address as 33.33.33.33/32 and the next hop as 10.1.2.2.

```
Device1#configure terminal
Device1(config)#mpls oam
Device1(config-mpls-oam)#bfd ipv4 33.33.33.33 32 nexthop 10.1.2.2
```

Step 4: Enable MPLS BFD on Device3.

```
Device3#configure terminal
Device3(config)#mpls oam
Device3(config-mpls-oam)#bfd enable
```

Step 5: On Device1, query whether MPLS BFD session is up.

```
Device1#show mpls oam bfd session active ipv4 33.33.33.33 32 nexthop 10.1.2.2
session type [Ldp_Ipv4] [active|dynamic] , prefix [33.33.33.33] nexthop [10.1.2.2]
src addr(out_int_addr) : 10.1.2.1
 nexthop addr : 10.1.2.2
 dst addr : 127.0.0.1
state [UP]
 oif : gigabitethernet0
 vrf: [global]
 local_discr : 1981
 remote_discr : 1834
 multiplier : 5
 min-transmit-interval : 1000
 min-receive-interval : 1000
 client: no client registed
 label-stack: 24000
```

On Device1, you can see that the status of the MPLS BFD session with the FEC type as LDP IPv4, destination address as 33.33.33.33/32, and the next hop as 10.1.2.2 is up. The configuration is complete.

5.3.4. Configure Dynamic MPLS BFD to Detect the Connectivity of MPLS TE FEC LSP

Network Requirements

- Configure the dynamic MPLS BFD to detect the connectivity of the LSP with the FEC type as MPLS TE and tunnel interface No. as 1 on Device1.

Network Topology

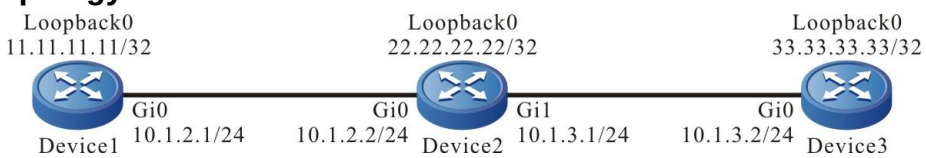

Figure 5-4 Configure the dynamic MPLS BFD to detect the connectivity of MPLS TE FEC LSP

Configuration Steps

Step 1: Configure the IP address of the interface, and set up the MPLS TE tunnel with the tunnel interface No. 1 from Device1 to Device3 (omitted, refer to “MPLS TE Function Configuration” of the configuration manual).

Step 2: Enable MPLS BFD on Device1.

```
Device1#configure terminal
Device1(config)#mpls oam
Device1(config-mpls-oam)#bfd enable
```

Step 3: On Device1, configure the dynamic BFD to detect the connectivity of the LSP with the FEC type as MPLS TE, and tunnel interface No. as 1.

```
Device1#configure terminal
Device1(config)#mpls oam
Device1(config-mpls-oam)#bfd traffic-eng tunnel 1
```

Step 4: Enable MPLS BFD on Device3.

```
Device3#configure terminal
Device3(config)#mpls oam
Device3(config-mpls-oam)#bfd enable
```

Step 5: On Device1, query whether the created MPLS BFD session is up.

```
Device3#show mpls oam bfd session active traffic tunnel 1 detail
session type [Tunnel] [active|dynamic] , tunnel [1] nexthop [10.1.3.1]
src addr(out_int_addr) : 10.1.3.2
 nexthop addr : 10.1.3.1
 dst addr : 127.0.0.1
state [UP]
 oif : gigabitethernet0
 vrf: [global]
 local-discr : 37
 remote-discr : 27
 multiplier : 5
 min-transmit-interval : 1000
 min-receive-interval : 1000
 client: no client registed
 label-stack: 24000
```

On Device1, you can see that the status of the MPLS BFD session with the FEC type as MPLS TE, and the tunnel interface No. as 10.1.2.2 is up. The configuration is complete.

5.3.5. Configure Static MPLS BFD to Detect the Connectivity of LDP IPv4 FEC LSP

Network Requirements

- Configure the static MPLS BFD to detect the connectivity of the LDP IPv4 FEC LSP, that is, LDP IPv4 LSP from Device1 to Device3, and LDP IPv4 LSP from Device3 to Device1.

Network Topology

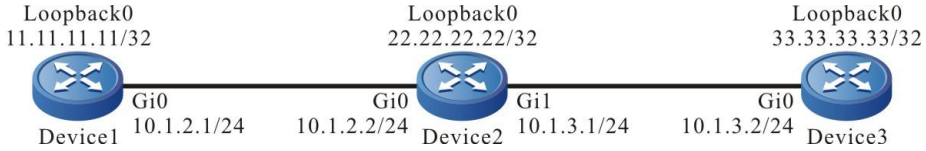

Figure 5-5 Configure the static MPLS BFD to detect the connectivity of LDP IPv4 FEC LSP

Configuration Steps

Step 1: Configure the IP address of the interface, and set up the LDP IPv4 LSP from Device1 to Device3 and the LDP IPv4 LSP from Device3 to Device1 (omitted, refer to “MPLS LDP Function Configuration” of the configuration manual).

Step 2: Enable MPLS OAM BFD on Device1.

```
Device1#configure terminal
Device1(config)#mpls oam
Device1(config-mpls-oam)#bfd enable
```

Step 3: On Device1, configure the static BFD to detect the connectivity of the LSP with the FEC destination address as 33.33.33.33/32 and the next hop as 10.1.2.2.

```
Device1#configure terminal
Device1(config)#mpls oam
Device1(config-mpls-oam)#bfd ipv4 33.33.33.33 32 nexthop 10.1.2.2 discriminator-local 27 discriminator-remote 37
```

Step 4: Enable MPLS BFD on Device3.

```
Device3#configure terminal
Device3(config)#mpls oam
Device3(config-mpls-oam)#bfd enable
```

Step 5: On Device3, configure the static BFD to detect the connectivity of the LSP with the FEC destination address as 11.11.11.11/32 and the next hop as 10.1.3.1. Here, the local authentication value and the peer authentication value correspond to the local and peer authentication values on Device1.

```
Device3#configure terminal
Device3(config)#mpls oam
```

```
Device3(config-mpls-oam)#bfd ipv4 11.11.11.11 32 nexthop 10.1.3.1 discriminator-local
37 discriminator-remote 27
```

Step 6: On Device1, query whether the corresponding MPLS BFD session is up.

```
Device1#show mpls oam bfd session active ipv4 33.33.33.33 32 nexthop 10.1.2.2
session type [Ldp_Ipv4] [active|static] , prefix [33.33.33.33] nexthop [10.1.2.2]
src addr(out_int_addr) : 10.1.2.1
 nexthop addr : 10.1.2.2
 dst addr : 127.0.0.1
 state [UP]
 oif : gigabitethernet0
 vrf: [global]
 local-discr : 27
 remote-discr : 37
 multiplier : 5
 min-transmit-interval : 1000
 min-receive-interval : 1000
 client: no client registed
 label-stack: 24000
```

Step 7: On Device3, query whether the corresponding MPLS BFD session is up.

```
Device3#show mpls oam bfd session active ipv4 11.11.11.11 32 nexthop 10.1.3.1
session type [Ldp_Ipv4] [active|static] , prefix [11.11.11.11] nexthop [10.1.3.1]
src addr(out_int_addr) : 10.1.3.2
 nexthop addr : 10.1.3.1
 dst addr : 127.0.0.1
state [UP]
 oif : gigabitethernet0
 vrf: [global]
 local-discr : 37
 remote-discr : 27
 multiplier : 5
 min-transmit-interval : 1000
 min-receive-interval : 1000
 client: no client registed
 label-stack: 24000
```

5.3.6. Configure Static MPLS BFD to Detect the Connectivity of MPLS TE FEC LSP

Network Requirements

- Use the static MPLS BFD to detect the connectivity of the MPLS TE FEC LSP, that is, the MPLS TE tunnel 1 from Device1 to Device3 and the MPLS TE tunnel 2 from Device3 to Device1.

Network Topology

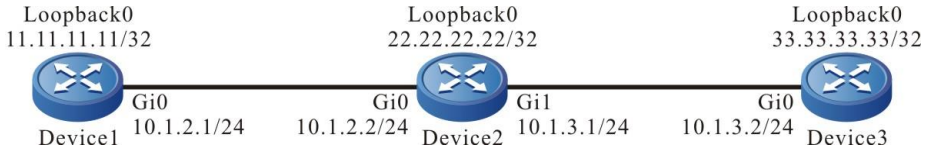

Figure 5-6 Configure the static MPLS BFD to detect the connectivity of MPLS TE FEC LSP

Configuration Steps

Step 1: Configure the IP address of the interface, and set up the MPLS TE tunnel from Device1 to Device3 and the MPLS TE tunnel from Device3 to Device1 (omitted, refer to “MPLS TE Function Configuration” of the configuration manual).

Step 2: Enable MPLS OAM BFD on Device1.

```
Device1#configure terminal
Device1(config)#mpls oam
Device1(config-mpls-oam)#bfd enable
```

Step 3: On Device1, configure the static BFD to detect the connectivity of the LSP with the FEC type as MPLS TE, and tunnel interface No. as 1.

```
Device1#configure terminal
Device1(config)#mpls oam
Device1(config-mpls-oam)#bfd traffic-eng tunnel 1 discriminator-local 27 discriminator-remote 37
```

Step 4: Enable MPLS BFD on Device3.

```
Device3#configure terminal
Device3(config)#mpls oam
Device3(config-mpls-oam)#bfd enable
```

Step 5: On Device3, configure the static BFD to detect the connectivity of the LSP with the FEC type as MPLS TE and the tunnel interface No. as 2. Here, the local authentication value and the peer authentication value correspond to the local and peer authentication values on Device1.

```
Device3#configure terminal
Device3(config)#mpls oam
```

```
Device3(config-mpls-oam)#bfd traffic-eng tunnel 2 discriminator-local 37
discriminator-remote 27
```

Step 6: On Device1, query whether the corresponding MPLS BFD session is up.

```
Device1#show mpls oam bfd session active traffic-eng tunnel 1
session type [tunnel] [active|static] , tunnel [1] nexthop [10.1.2.2]
src addr(out_int_addr) : 10.1.2.1
 nexthop addr : 10.1.2.2
 dst addr : 127.0.0.1
 state [UP]
 oif : gigabitethernet0
 vrf: [global]
 local_discr : 27
 remote_discr : 37
 multiplier : 5
 min-transmit-interval : 1000
 min-receive-interval : 1000
 client: no client registed
 label-stack: 24000
```

Step 7: On Device3, query whether the corresponding MPLS BFD session is up.

```
Device3#show mpls oam bfd session active traffic-eng tunnel 2
session type [tunnel] [active|static] , tunnel [2] nexthop [10.1.3.1]
 src addr(out_int_addr) : 10.1.3.2
 nexthop addr : 10.1.3.1
 dst addr : 127.0.0.1
state [UP]
 oif : gigabitethernet0
 vrf: [global]
 local_discr : 37
 remote_discr : 27
 multiplier : 5
 min-transmit-interval : 1000
 min-receive-interval: 1000
 client: no client registed
 label-stack: 24000
```

6. 6PE

6.1. Overview

6PE (IPv6 Provider Edge) is one tunnel technology of transiting IPv4 to IPv6, connecting the IPv6 island. Different from other tunnel technology, the 6PE tunnel can make full use of the existing dynamic setup IPv4 MPLS tunnel, but does not need to add the explicit tunnel configuration. Therefore, you do not need to do any change for the backbone network core, but just need to upgrade the PE device to support the dual-protocol stack. The PE device is called 6PE device.

The 6PE architecture is shown in the following figure:

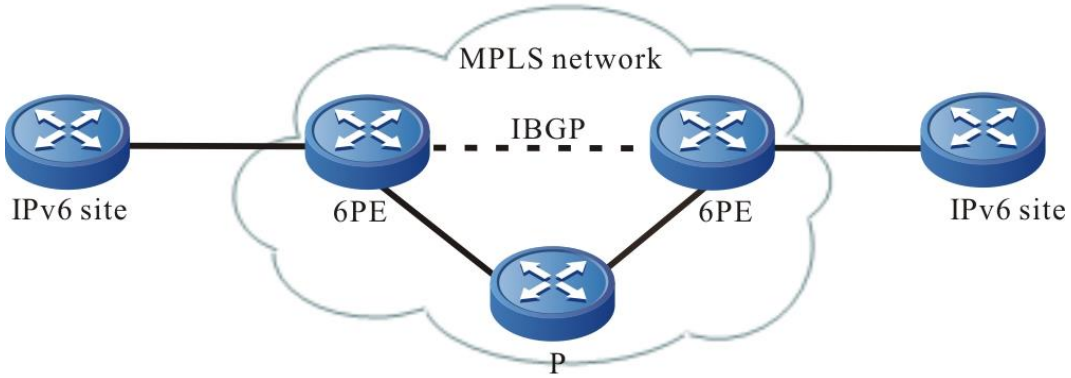

Figure 6-1 6PE networking

In the above figure, the IPv4 backbone network runs MPLS and all P devices do not perceive the existing of the IPv6 network. The 6PE device is at the edge of the IPv4 network and IPv6 network and run the IPv4/IPv6 dual-protocol stack. The IPv6 site (CE) device runs the IPv6 protocol stack.

6PE makes use of the BGP/MPLS VPN theory and regards the IPv6 island as the VPN access site. The 6PE devices distribute the IPv6 routes and the used labels for the sites via MP-BGP, but the interface connected to the CE device on the 6PE is not the VRF interface. All IPv6 islands connected to the IPv4 MPLS backbone network can communicate with each other, and their address spaces cannot overlap and all run in the IPv6 global address space.

The 6PE and CE devices can run the static route, BGP4+, IGP protocol to transmit the IPv6 route. The 6PE devices run the BGP/MPLS protocol to distribute the label for the IPv6 route to the CE.

6.2. 6PE Function Configuration

Table 6-1 6PE function configuration list

Configuration tasks	
Configure 6PE basic functions	Configure PE-PE route exchange
	Configure PE-CE route exchange
Configure 6PE route label distributing	Configure the 6PE route label distributing
Configure 6PE cross-domain	Configure the Option-A cross-domain
	Configure the Option-B cross-domain

6.2.1. Configure 6PE Basic Functions

Configuration Condition

Before configuring the 6PE basic functions, first complete the following tasks:

- Configure the IGP of the MPLS backbone network, making the IP between the PE devices reachable
- Configure the MPLS basic capability and LDP of the MPLS backbone network, and set up LSP between PE devices
- Enable the IPv6 capability on the connected interface of the CE and PE, and configure the global unicast address

Configure PE-PE Route Exchange

In the 6PE network, the PEs use the IPv4 address to set up the BGP neighbor and exchange the VPNv6 route via MP-IBGP. The configuration modes of the two PEs are the same.

Table 6-2 Configure PE-PE route exchange

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enable the BGP protocol and enter the BGP configuration mode	**router bgp** *autonomous-system*	-
Configure the PE neighbor	**neighbor** { *ipv4-address* | *peer-group-name* } **remote-as** *as-number*	Mandatory By default, do not configure any PE neighbor.
Configure the source address used by setting up the PE neighbor	**neighbor** { *ipv4-address* | *peer-group-name* } **update-source** { *interface* | *ip-address* }	Mandatory By default, use the egress interface address to the PE neighbor route as the source address.
Enter the BGP IPv6 unicast configuration mode	**address-family ipv6** [**unicast**]	-
Activate the IPv6 address family of the PE neighbor	**neighbor** { *ipv4-address* | *peer-group-name* } **activate**	Mandatory By default, the BGP neighbors can only receive and send the IPv4 unicast route.
Configure carrying the label when distributing the IPv6 route to the PE neighbor	**neighbor** *ipv4-address* **send-label** [**explicit-null**]	Mandatory By default, do not carry the label when advertising the route to the PE.

Configure PE-CE Route Exchange

PE and CE can use the IPv6 static route, RIPng, OSPFv3, ISIS IPv6 and BGP4+ route protocol to exchange the route. Which protocol is adopted depends on the actual network environment. The PE configuration is the same as the CE configuration mode.

1. **Configure PE-CE to use static route**

Table 6-3 Configure PE-CE to use the static route

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Configure the static route to the CE	**ipv6 route** [**vrf** *vrf-name1*] *ipv6-prefix/mask-length* { *interface-name* | [*nexthop-ipv6-address* [**vrf** *vrf-name2*]]} [**name** *nexthop-name*] [**tag** *tag-value*] [**track** *track-id*] [*administrative-distance*]	Mandatory By default, do not configure the static route to the CE.
Enable the BGP protocol and enter the BGP configuration mode	**router bgp** *autonomous-system*	-
Enter the BGP IPv6 unicast configuration mode	**address-family ipv6** [**unicast**]	Mandatory By default, it is in the BGP IPv4 unicast configuration mode.
Configure BGP to re-distribute the static route	**redistribute static** [**route-map** *map-name* / **metric** *value*]	Mandatory By default, do not configure BGP to re-distribute the static route.

2. Configure PE-CE to use RIPng

Table 6-4 Configure PE-CE to use RIPng

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enable the RIPng protocol and enter the RIPng configuration mode	**ipv6 router rip** *process-id*	Mandatory By default, do not enable RIPng.
Return to the global configuration mode	**exit**	-
Enter the interface configuration mode	**interface** *interface-name*	-
Enable the RIPng protocol on the connected interface of PE and CE	**ipv6 rip enable** *process-id*	Mandatory By default, the interface does not enable the RIPng protocol.
Return to the global configuration mode	**exit**	
Enable the BGP protocol and enter the BGP configuration mode	**router bgp** *autonomous-system*	-
Enter the BGP IPv6 unicast configuration mode	**address-family ipv6** [**unicast**]	Mandatory By default, it is in the BGP IPv4 unicast configuration mode.
Configure the BGP to re-distribute RIPng	**redistribute rip** *process-id* [**route-map** *map-name* / **metric** *value*]	Mandatory By default, do not re-distribute the RIPng protocol route.

3. Configure PE-CE to use OSPFv3

Table 6-5 Configure PE-CE to use OSPFv3

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Create one OSPFv3 process and enter the OSPFv3 configuration mode	**ipv6 router ospf** *process-id* **vrf** *vrf-name*	Mandatory By default, the system does not enable the OSPFv3 protocol.
Configure OSPFv3 router-id	**router-id** *router-id*	Mandatory By default, OSPFv3 does not configure router-id.
Return to the global configuration mode	**exit**	-
Enter the interface configuration mode	**interface** *interface-name*	-
Enable the OSPFv3 protocol on the connected interface of PE and CE	**ipv6 router ospf** *process-id* **area** *area-id* [**instance-id** *instance-id*]	Mandatory By default, the interface does not enable the OSPFv3 protocol.
Return to the global configuration mode	**exit**	-
Enable the BGP protocol and enter the BGP configuration mode	**router bgp** *autonomous-system*	-
Enter the BGP IPv6 unicast configuration mode	**address-family ipv6** [**unicast**]	Mandatory By default, it is in the BGP IPv4 unicast configuration mode.

Step	Command	Description
Configure BGP to re-distribute OSPF	**redistribute ospf** *process-tag* [**route-map** *map-name* / **metric** *value* / **match** *level*]	Mandatory By default, do not re-distribute the OSPFv3 protocol route.

4. Configure PE-CE to use ISIS IPv6

Table 6-6 Configure PE-CE to use ISIS IPv6

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the IS-IS configuration mode	**router isis** [*instance-name*]	-
Configure the network entity title for ISIS	**net** *entry-title*	Mandatory By default, ISIS does not have the network entity title.
Return to the global configuration mode	**exit**	-
Enter the interface configuration mode	**interface** *interface-name*	-
The interface enables the IS-IS protocol	**ipv6 router isis** [*instance-name*]	Mandatory By default, the interface does not enable the IS-IS protocol.
Return to the global configuration mode	**exit**	-
Enable the BGP protocol and enter the BGP configuration mode	**router bgp** *autonomous-system*	-

Step	Command	Description
Enter the BGP IPv6 unicast configuration mode	**address-family ipv6** [**unicast]**	Mandatory By default, it is in the BGP IPv4 unicast configuration mode.
Configure BGP to re-distribute ISIS	**redistribute isis** [*instance-name*] [**route-map** *map-name* / **metric** *value* / **match** *level*]	Optional By default, do not re-distribute the IS-IS protocol route.

5. Configure PE-CE to use BGP4+

Table 6-7 Configure PE-CE to use BGP4+

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enable the BGP protocol and enter the BGP configuration mode	**router bgp** *autonomous-system*	-
Enter the BGP IPv6 unicast configuration mode	**address-family ipv6** [**unicast]**	Mandatory By default, it is in the BGP IPv4 unicast configuration mode.
Configure the CE as the EBGP neighbor	**neighbor** { *ipv6-address* | *peer-group-name* } **remote-as** *as-number*	Mandatory By default, do not configure any CE neighbor.

6.2.2. Configure 6PE Route Label Distributing

Configuration Condition

Before configuring the 6PE route label distributing mode, first complete the following task:

- Configure 6PE basic functions

Configure 6PE Route Label Distributing

BGP has two modes of distributing the label for the IPv6 route: explicit null label distributing mode and non-explicit null label distributing mode. When adopting the non-explicit null mode, BGP distributes different labels for each IPv6 route. When adopting the explicit null mode, BGP

distributes the same label for the local route and the label value is 2, while the routes from the PE and CE still adopt the non-explicit null mode.

By default, BGP adopts the non-explicit null label distributing mode.

Table 6-8 Configure the 6PE route label distributing

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enable the BGP protocol and enter the BGP configuration mode	**router bgp** *autonomous-system*	-
Enter the BGP IPv6 unicast configuration mode	**address-family ipv6** [**unicast**]	-
Configure the explicit null label distributing mode	**neighbor** *ipv4-address* **send-label explicit-null**	Mandatory By default, enable the non-explicit null label distributing mode.

6.2.3. Configure 6PE Cross-Domain

Configuration Condition

Before configuring the 6PE cross-domain, first complete the following task:

- Configure 6PE basic functions

Configure Option-A Cross-Domain

Option-A cross-domain is similar to the Option-A cross-domain mode in L3VPN, and the difference is that ASBR of the 6PE runs in the global route table and L3VPN runs in the VRF route table. Option-A cross-domain mode is the simplest mode of realizing the 6PE inter-access between ASs. Take the other ASBR as the CE device to process the 6PE connectivity between ASs. The following figure describes one Option-A cross-domain instance.

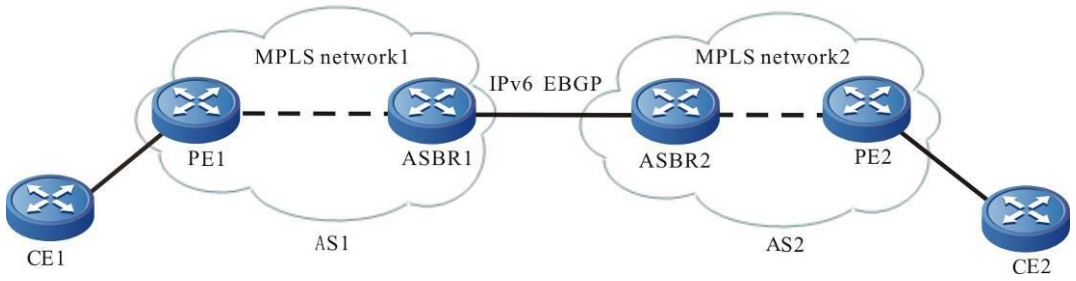

Figure 6-2 Configure Option-A cross-domain

In the above figure IPv6 site (CE1) and IPv6 site 2 (CE2) are connected to two different service providers respectively: AS1 and AS2. The service providers are connected via ASBR. Two AS areas configure the MPLS network. The sites crossing the AS need the local ASBR to serve as

the PE device and the peer ASBR serve as the CE device. The PE and ASBR devices need to have the IPv4 and IPv6 dual-protocol stack capability. Configure BGP4+ between two ASBR and transmit the IPv6 route, so as to realize the interconnection of CE1 and CE2.

The advantage of the Option-A mode is that it is not necessary to run MPLS between ASBR. The disadvantage is that ASBR needs to maintain all IPv6 routes. Therefore, the expansibility is poor.

For the configuration of the Option-A cross-domain mode, refer to the part of “Configure 6PE basic functions”.

Configure Option-B Cross-Domain

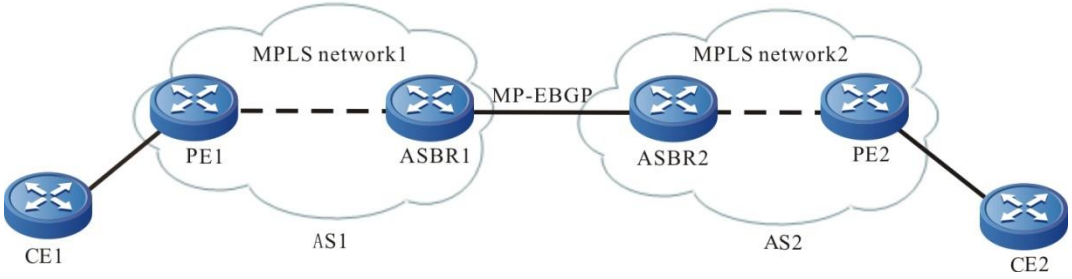

Figure 6-3 Configure Option-B cross-domain (MP-EBGP carries the 6PE route)

Option-B cross-domain needs to run MP-EBGP between ASBR. After ASBR learns all 6PE routes of the local AS PE, distribute the new label for the 6PE route, and then advertise the route information and new label to the peer ASBR. ASBR needs to maintain all 6PE routes received from the local PE and the peer ASBR.

In the Option-B cross-domain mode, the interfaces between ASBR do not need to enable the IPv6 capability, but need to enable the MPLS forwarding capability; ASBR still needs to maintain all 6PE routes and distribute new label for each label. Install the ILM entry of the old and new label translation at the local. Therefore, ASBR has the good load capability.

Table 6-9 Configure Option-B cross-domain

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enable the MPLS forwarding globally	**mpls ip**	Mandatory By default, do not enable the MPLS forwarding.
Enter the interface configuration mode	**interface** *interface_name*	-

Step	Command	Description
Enable the MPLS forwarding on the interface	**mpls ip**	Mandatory Configure on the interconnecting interfaces of the two ASBR. By default, do not enable the MPLS forwarding on the interface.
Return to the global configuration mode	**exit**	-
Enable the BGP protocol and enter the BGP configuration mode	**router bgp** *autonomous-system*	-
Configure the peer ASBR as the EBGP neighbor	**neighbor** { *ipv4-address* | *peer-group-name* } **remote-as** *as-number*	Mandatory By default, do not configure any EBGP neighbor.
Enter the BGP IPv4 unicast configuration mode	**address-family ipv6** [**unicast**]	Mandatory By default, it is in the BGP IPv4 unicast configuration mode.
Activate the MP-EBGP neighbor to advertise the IPv6 route	**neighbor** { *ipv4-address* | *peer-group-name* } **activate**	Mandatory By default, BGP only advertises the IPv4 unicast route.
Configure the capability of the neighbor carrying the label when transmitting the IPv6 route	**neighbor** *ipv4-address* **send-label** [**explicit-null**]	Mandatory By default, do not carry the label.
Configure changing the next hop when advertising the route to the PE	**neighbor** { *neighbor-address* | *peer-group-name* } **next-hop-self**	Mandatory By default, do not configure changing the next hop when advertising the route to the PE.

Note:

The above just lists the basic configuration of the Option-B cross-domain on ASBR. For the configuration of the ASBR and the PE, P devices in the AS, refer to the part of “Configure 6PE Basic Functions”.

6.2.4. 6PE Monitoring and Maintaining

Table 6-10 6PE monitoring and maintaining

Command	Description
clear bgp ipv6 { ***** | *as-number* | **peer-group** *peer-group-name* | **external** } **in prefix-filter**	Advertise ORF to the neighbor
clear bgp ipv6 { * | *as-number* **| peer-group** *peer-group-name* | **external** | *neighbor-address*} **unicast** { [**soft**] [**in** | **out**] }	Soft-reset the neighbor
show bgp ipv6 unicast [*ipv6-address* | *ipv6-address/mask-length*]	Display the route database information in the BGP VPNv6 unicast address family
show bgp ipv6 unicast labels	Display the label information of the IPv6 unicast route
show bgp ipv6 unicast neighbors *ipv4-adress*	Display the neighbor details in the BGP VPNv6 unicast address family
show bgp ipv6 unicast summary	Display all neighbor summary information in the BGP IPv6 unicast address family
show mpls forwarding-table [**detail**]	Display the MPLS forwarding table information
show mpls forwarding-table ilm ipv6	Display the MPLS IPv6 forwarding table information
show mpls forwarding-table ilm [**detail**]	Display the MPLS ILM forwarding table information

6.3. 6PE Typical Configuration Example

6.3.1. Configure Intra-Domain 6PE

Network Requirements

- PE1, P, and PE2 belong to the IPv4 MPLS network.
- CE1 and CE2 belong to the IPv6 network.
- CE and PE use IPv6 BGP to exchange the route information.
- PEs adopt OSPF as IGP to make PEs communicate with each other. Configure MP-IBGP to exchange the IPv6 route information with the label.

Network Topology

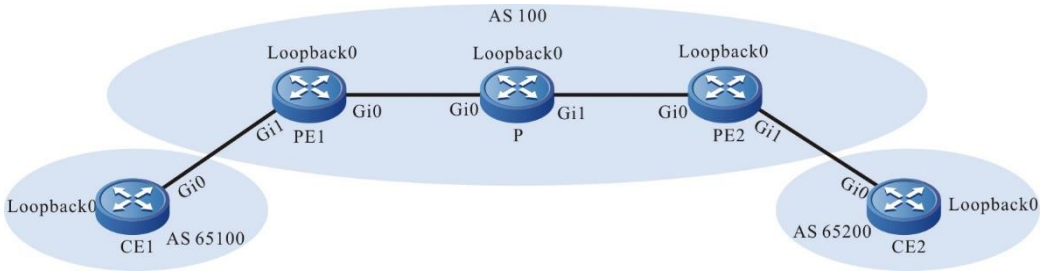

Figure 6-4Networking of configuring the intra-domain 6PE

Device	Interface	IP Address	Device	Interface	IP Address
CE1	Gi0	2001:1::2/64	P	Gi0	10.1.1.1/24
	Loopback0	3000::1/128		Gi1	10.1.2.2/24
PE1	Gi0	10.1.1.2/24		Loopback0	22.22.22.22/32
	Gi1	2001:1::1/64	PE2	Gi0	10.1.2.1/24
	Loopback0	11.11.11.11/32		Gi1	2001:2::1/64
CE2	Gi0	2001:2::2/64		Loopback0	33.33.33.33/32
	Loopback0	4000::1/128			

Configuration Steps

Step 1: Configure the IP address of the interface (omitted).

Step 2: Configure the global OSPF and advertise the global route.

#Configure the global OSPF on PE1.

```
PE1#configure terminal
PE1(config)#router ospf 100
```

```
PE1(config-ospf)#network 10.1.1.0 0.0.0.255 area 0
PE1(config-ospf)#network 11.11.11.11 0.0.0.0 area 0
PE1(config-ospf)#exit
```

#Configure the global OSPF on P.

```
P#configure terminal
P(config)#router ospf 100
P(config-ospf)#network 10.1.1.0 0.0.0.255 area 0
P(config-ospf)#network 10.1.2.0 0.0.0.255 area 0
P(config-ospf)#network 22.22.22.22 0.0.0.0 area 0
P(config-ospf)#exit
```

#Configure the global OSPF on PE2.

```
PE2#configure terminal
PE2(config)#router ospf 100
PE2(config-ospf)#network 10.1.2.0 0.0.0.255 area 0
PE2(config-ospf)#network 33.33.33.33 0.0.0.0 area 0
PE2(config-ospf)#exit
```

#After the configuration is complete, view the global route table on the device.

Take PE1 as an example:

```
PE1#show ip route
Codes: C - Connected, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external

C   10.1.1.0/24 is directly connected, 00:10:59, gigabitethernet0
O   10.1.2.0/24 [110/2] via 10.1.1.1, 00:05:29, gigabitethernet0
C   127.0.0.0/8 is directly connected, 1w3d:00:43:58, lo0
C   11.11.11.11/32 is directly connected, 00:10:40, loopback0
O   22.22.22.22/32 [110/2] via 10.1.1.1, 00:05:19, gigabitethernet0
O   33.33.33.33/32 [110/3] via 10.1.1.1, 00:02:47, gigabitethernet0
```

You can see that there is the route information of P and PE2 loopback ports in the global route table of PE1.

Note:

- For the checking method of P and PE2, refer to PE1.

Step 3: Enable MPLS IP and MPLS LDP.

#On PE1, enable the global MPLS IP and MPLS LDP. Meanwhile, enable MPLS IP and MPLS LDP on the interface.

```
PE1(config)#mpls ip
PE1(config)#mpls ldp
PE1(config-ldp)#router-id 11.11.11.11
PE1(config-ldp)#address-family ipv4
PE1(config-ldp-af4)#transport-address 11.11.11.11
PE1(config-ldp-af4)#exit
PE1(config-ldp)#exit
PE1(config)#interface gigabitethernet0
PE1(config-if-gigabitethernet0)#mpls ip
PE1(config-if-gigabitethernet0)#mpls ldp
PE1(config-if-gigabitethernet0)#exit
```

#On P, enable the global MPLS IP and MPLS LDP. Meanwhile, enable MPLS IP and MPLS LDP on the interface.

```
P(config)#mpls ip
P(config)#mpls ldp
P(config-ldp)#router-id 22.22.22.22
P(config-ldp)#address-family ipv4
P(config-ldp-af4)#transport-address 22.22.22.22
P(config-ldp-af4)#exit
P(config-ldp)#exit
P(config)#interface gigabitethernet0
P(config-if-gigabitethernet0)#mpls ip
P(config-if-gigabitethernet0)#mpls ldp
P(config-if-gigabitethernet0)#exit
P(config)#interface gigabitethernet1
P(config-if-gigabitethernet1)#mpls ip
P(config-if-gigabitethernet1)#mpls ldp
P(config-if-gigabitethernet1)#exit
```

#On PE2, enable the global MPLS IP and MPLS LDP. Meanwhile, enable MPLS IP and MPLS LDP on the interface.

```
PE2(config)#mpls ip
PE2(config)#mpls ldp
PE2(config-ldp)#router-id 33.33.33.33
PE2(config-ldp)#address-family ipv4
```

```
PE2(config-ldp-af4)#transport-address 33.33.33.33
PE2(config-ldp-af4)#exit
PE2(config-ldp)#exit
PE2(config)#interface gigabitethernet0
PE2(config-if-gigabitethernet0)#mpls ip
PE2(config-if-gigabitethernet0)#mpls ldp
PE2(config-if-gigabitethernet0)#exit
```

Note:

- router-id and transport-address can be configured manually and also can be generated automatically. Usually, they are configured the same. If not configuring router-id and transport-address manually, the device will select automatically. From the up interfaces, first select the Loopback interface with the maximum IP address. If the device does not configure the Loopback interface address, select the common interface with the maximum IP address.

#After the configuration is complete, view the LDP session information on the device.

Take PE1 as an example:

```
PE1#show mpls ldp session
Peer IP Address    Peer Type    My Role   State        DS Cap   DeadTime
22.22.22.22        Multicast    Active    OPERATIONAL  Disabled 00:02:34
Statistics for ldp sessions:
    Multicast sessions: 1
    Targeted sessions: 0
```

You can see that PE1 and P set up the LDP session successfully.

#View the MPLS forwarding table on the device.

Take PE1 as an example:

```
PE1#show ip route 22.22.22.22 detail
Codes: C - Connected, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
    U - Per-user Static route
    O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external




O   22.22.22.22/32 [110/2] via 10.1.1.1, label 3, 00:05:12, gigabitethernet0
                           10.1.1.1 [0], gigabitethernet0

PE1#show ip route 33.33.33.33 detail
Codes: C - Connected, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
    U - Per-user Static route
```

O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external

O 33.33.33.33/32 [110/2] via 10.1.1.1, label 24017, 00:06:03, gigabitethernet0
10.1.1.1 [0], gigabitethernet0

You can see that the loopback port route from PE1 to P and PE2 has the label information.

Note:

- For the checking method of P and PE2, refer to PE1.

Step 4: Configure IPv6 BGP to advertise the route on the CE and PE.

#On PE1, configure IPv6 BGP.

```
PE1(config)#router bgp 100
PE1(config-bgp)#address-family ipv6
PE1(config-bgp-af)#neighbor 2001:1::2 remote-as 65100
PE1(config-bgp-af)#exit-address-family
PE1(config-bgp)#exit
```

#Configure IPv6 BGP on CE1.

```
CE1#configure terminal
CE1(config)#router bgp 65100
CE1(config-bgp)#bgp router-id 10.10.10.10
CE1(config-bgp)#address-family ipv6
CE1(config-bgp-af)#neighbor 2001:1::1 remote-as 100
CE1(config-bgp-af)#network 3000::1/128
CE1(config-bgp-af)#exit-address-family
CE1(config-bgp)#exit
```

#Configure IPv6 BGP on PE2.

```
PE2(config)#router bgp 100
PE2(config-bgp)#address-family ipv6
PE2(config-bgp-af)#neighbor 2001:2::2 remote-as 65200
PE2(config-bgp-af)#exit-address-family
PE2(config-bgp)#exit
```

#Configure IPv6 BGP on CE2.

```
CE2#configure terminal
CE2(config)#router bgp 65200
CE2(config-bgp)#bgp router-id 20.20.20.20
```

```
CE2(config-bgp)#address-family ipv6
CE2(config-bgp-af)#neighbor 2001:2::1 remote-as 100
CE2(config-bgp-af)#network 4000::1/128
CE2(config-bgp-af)#exit-address-family
CE2(config-bgp)#exit
```

#On PE1, view the global IPv6 route table.

```
PE1#show ipv6 route
Codes: C - Connected, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management



L   ::1/128 [0/0]
    via ::, 1w3d:01:28:30, lo0
C   2001:1::/64 [0/0]
    via ::, 00:55:45, gigabitethernet1
L   2001:1::1/128 [0/0]
    via ::, 00:55:45, gigabitethernet1
B   3000::1/128 [20/0]
    via 2001:1::2, 00:05:06, gigabitethernet1
```

You can see that there is the route information of CE1 in the global IPv6 route table of PE1.

Note:

- For the checking method of PE2, refer to PE1.

Step 5: Configure MP-IBGP, and use the loopback interface as the peer address.

#On PE1, configure MP-IBGP, activate the neighbor in the IPv6 address family, and configure the label sending capability.

```
PE1(config)#router bgp 100
PE1(config-bgp)#neighbor 33.33.33.33 remote-as 100
PE1(config-bgp)#neighbor 33.33.33.33 update-source loopback 0
PE1(config-bgp)#address-family ipv6
PE1(config-bgp-af)#neighbor 33.33.33.33 activate
PE1(config-bgp-af)#neighbor 33.33.33.33 send-label
PE1(config-bgp-af)#exit-address-family
PE1(config-bgp)#exit
```

#On PE1, configure MP-IBGP, activate the neighbor in the IPv6 address family, and configure the label sending capability.

```
PE2(config)#router bgp 100
PE2(config-bgp)#neighbor 11.11.11.11 remote-as 100
PE2(config-bgp)#neighbor 11.11.11.11 update-source loopback 0
PE2(config-bgp)#address-family ipv6
PE2(config-bgp-af)#neighbor 11.11.11.11 activate
PE2(config-bgp-af)#neighbor 11.11.11.11 send-label
PE2(config-bgp-af)#exit-address-family
PE2(config-bgp)#exit
```

Step 6: Check the result.

#After the configuration is complete, view the BGP neighbor information on the PE.

Take PE1 as an example:

```
PE1#show bgp ipv6 unicast summary
BGP router identifier 11.11.11.11, local AS number 100
BGP table version is 4
3 BGP AS-PATH entries
0 BGP community entries

Neighbor        V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
33.33.33.33     4   100      10       9        4    0    0 00:06:21        1
2001:1::2       4 65100      32      31        4    0    0 00:25:23        1

Total number of neighbors 2
```

The content of the State/PfxRcd list is displayed as number (the number of the route prefixes received from the neighbor), and you can see that PE1 and PE2 set up the BGP neighbor successfully.

#View the BGP IPv6 route table and global IPv6 route table on the PE.

Take PE1 as an example:

```
PE1#show bgp ipv6 unicast
BGP table version is 4, local router ID is 11.11.11.11
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network          Next Hop            Metric     LocPrf Weight Path
[B]*> 3000::1/128     1000::2                  0             0 65100 i
[B]*>i4000::1/128     ::ffff:33.33.33.33
                                               0      100      0 65200 i
```

```
PE1#show ipv6 route
Codes: C - Connected, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management

L   ::1/128 [0/0]
    via ::, 1w3d:01:51:03, lo0
C   2001:1::/64 [0/0]
    via ::, 01:18:18, gigabitethernet1
L   2001:1::1/128 [0/0]
    via ::, 01:18:18, gigabitethernet1
B   3000::1/128 [20/0]
    via 2001:1::2, 00:27:38, gigabitethernet1
B   4000::1/128 [200/0]
    via ::ffff:33.33.33.33, 00:08:13, gigabitethernet0
```

You can see that there is the route information to the peer CE2 in the IPv6 BGP route table of PE1 and the global IPv6 route table.

#View the MPLS forwarding table on the PE.

Take PE1 as an example:

```
PE1#show mpls forwarding-table
Pro: L - LDP, O - OSPF, B - MP-BGP, R - RSVP, M - Mapped-Route, S - Static
Label,ML - mLDP (ML FEC: Root address/OT/OV), RM - RSVP P2MP (RM FEC: P2MP
ID/TID)

Pro Ident      FEC            Inlabel Outlabel Outgoing          Next hop
B   global     3000::1/128     25120   /      gigabitethernet1   2001:1::2
```

You can see that there is the route label information of CE1 in the MPLS forwarding table of PE1.

#On the PE, view the route detail information.

Take PE1 as an example:

```
PE1#show ipv6 route 4000::1/128
Codes: C - Connected, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management
```

```
B   4000::1/128 [200/0]
    via ::ffff:33.33.33.33 [0], label 25120, 00:12:18, gigabitethernet0
        ::ffff:10.1.1.1 [3], label 24017, gigabitethernet0
```

You can see that there is the route information of CE2 in the route table of PE1, the private network label of the route is 25120, and the global label is 24017.

Note:

- For the checking method of PE2, refer to PE1.

#Ping the loopback port of CE2 at CE1 and view whether the ping can be connected.

```
CE1#ping 4000::1 -s 3000::1

Press key (ctrl + shift + 6) interrupt it.
Reply from  4000::1: bytes = 76  time < 16 ms
Reply from  4000::1: bytes = 76  time < 16 ms
Reply from  4000::1: bytes = 76  time < 16 ms
Reply from  4000::1: bytes = 76  time < 16 ms
Reply from  4000::1: bytes = 76  time < 16 ms
Success rate is 100% (5/5). Round-trip min/avg/max = 0/0/0 ms.
```

You can see that CE1 and CE2 can communicate with each other.

6.3.2. Configure Cross-Domain OptionA

Network Requirements

- The whole MPLS network includes two AS domains. CE1 in AS100 needs to communicate with CE2 in AS200.
- CE and PE use IPv6 BGP to exchange the route information.
- Use IPv6 BGP to exchange the route information between ASBRs.
- ASBR and PE use MP-IBGP to exchange the IPv6 route with the label.

Network Topology

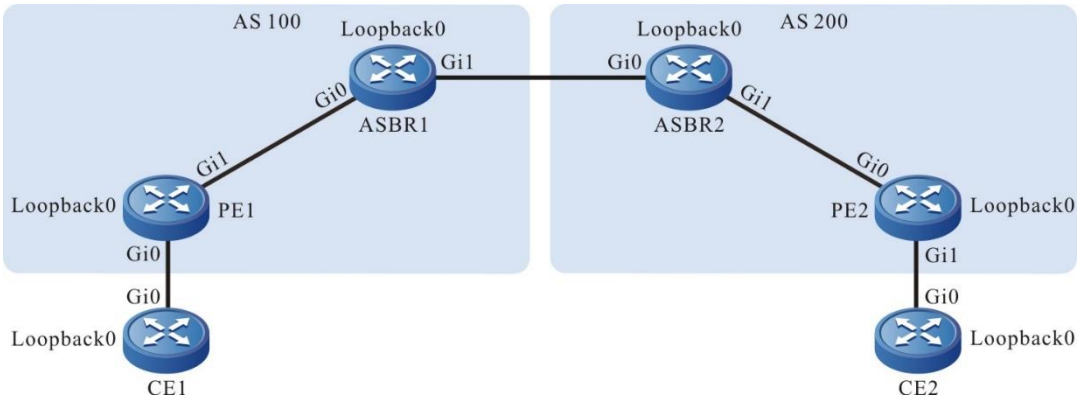

Figure 6-5 Networking of configuring the cross-domain OptionA

Device	Interface	IP Address	Device	Interface	IP Address
CE1	Gi0	2001:1::2/64	ASBR2	Gi0	2001:2::1/64
	Loopback0	3000::1/128		Gi1	10.1.2.2/24
PE1	Gi0	2001:1::1/64		Loopback0	33.33.33.33/32
	Gi1	10.1.1.2/24	PE2	Gi0	10.1.2.1/24
	Loopback0	11.11.11.11/32		Gi1	2001:3::1/64
ASBR1	Gi0	10.1.1.1/24		Loopback0	44.44.44.44/32
	Gi1	2001:2::2/64	CE2	Gi0	2001:3::2/64
	Loopback0	22.22.22.22/32		Loopback0	4000::1/128

Configuration Steps

Step 1: Configure the IP address of the interface (omitted).

Step 2: Configure the global OSPF and advertise the global route.

#Configure the global OSPF on PE1.

```
PE1#configure terminal
PE1(config)#router ospf 100
PE1(config-ospf)#network 10.1.1.0 0.0.0.255 area 0
PE1(config-ospf)#network 11.11.11.11 0.0.0.0 area 0
PE1(config-ospf)#exit
```

#Configure the global OSPF on ASBR1.

```
ASBR1#configure terminal
ASBR1(config)#router ospf 100
ASBR1(config-ospf)#network 10.1.1.0 0.0.0.255 area 0
ASBR1(config-ospf)#network 22.22.22.22 0.0.0.0 area 0
ASBR1(config-ospf)#exit
```

#Configure the global OSPF on ASBR2.

```
ASBR2#configure terminal
ASBR2(config)#router ospf 100
ASBR2(config-ospf)#network 10.1.2.0 0.0.0.255 area 0
ASBR2(config-ospf)#network 33.33.33.33 0.0.0.0 area 0
ASBR2(config-ospf)#exit
```

#Configure the global OSPF on PE2.

```
PE2#configure terminal
PE2(config)#router ospf 100
PE2(config-ospf)#network 10.1.2.0 0.0.0.255 area 0
PE2(config-ospf)#network 44.44.44.44 0.0.0.0 area 0
PE2(config-ospf)#exit
```

#After the configuration is complete, view the global route table on the device.

Take PE1 as an example:

```
PE1#show ip route
Codes: C - Connected, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external




C   10.1.1.0/24 is directly connected, 04:49:02, gigabitethernet1
C   127.0.0.0/8 is directly connected, 1w3d:05:22:00, lo0
C   11.11.11.11/32 is directly connected, 04:48:43, loopback0
O   22.22.22.22/32 [110/2] via 10.1.1.1, 04:43:21, gigabitethernet1
```

You can see that there is the route information of ASBR1 loopback port in the global route table of PE1.

Note:

- For the checking method of PE2 and ASBR, refer to PE1.

Step 3: Enable MPLS IP and MPLS LDP.

#On PE1, enable the global MPLS IP and MPLS LDP. Meanwhile, enable MPLS IP and MPLS LDP on the interface.

```
PE1(config)#mpls ip
PE1(config)#mpls ldp
PE1(config-ldp)#router-id 11.11.11.11
PE1(config-ldp)#address-family ipv4
PE1(config-ldp-af4)#transport-address 11.11.11.11
PE1(config-ldp-af4)#exit
```

```
PE1(config-ldp)#exit
PE1(config)#interface gigabitethernet1
PE1(config-if-gigabitethernet1)#mpls ip
PE1(config-if-gigabitethernet1)#mpls ldp
PE1(config-if-gigabitethernet1)#exit
```

#On ASBR1, enable the global MPLS IP and MPLS LDP. Meanwhile, enable MPLS IP and MPLS LDP on the interface.

```
ASBR1(config)#mpls ip
ASBR1(config)#mpls ldp
ASBR1(config-ldp)#router-id 22.22.22.22
ASBR1(config-ldp)#address-family ipv4
ASBR1(config-ldp-af4)#transport-address 22.22.22.22
ASBR1(config-ldp-af4)#exit
ASBR1(config-ldp)#exit
ASBR1(config)#interface gigabitethernet0
ASBR1(config-if-gigabitethernet0)#mpls ip
ASBR1(config-if-gigabitethernet0)#mpls ldp
ASBR1(config-if-gigabitethernet0)#exit
```

#On ASBR2, enable the global MPLS IP and MPLS LDP. Meanwhile, enable MPLS IP and MPLS LDP on the interface.

```
ASBR2(config)#mpls ip
ASBR2(config)#mpls ldp
ASBR2(config-ldp)#router-id 33.33.33.33
ASBR2(config-ldp)#address-family ipv4
ASBR2(config-ldp-af4)#transport-address 33.33.33.33
ASBR2(config-ldp-af4)#exit
ASBR2(config-ldp)#exit
ASBR2(config)#interface gigabitethernet1
ASBR2(config-if-gigabitethernet1)#mpls ip
ASBR2(config-if-gigabitethernet1)#mpls ldp
ASBR2(config-if-gigabitethernet1)#exit
```

#On PE2, enable the global MPLS IP and MPLS LDP. Meanwhile, enable MPLS IP and MPLS LDP on the interface.

```
PE2(config)#mpls ip
PE2(config)#mpls ldp
PE2(config-ldp)#router-id 44.44.44.44
PE2(config-ldp)#address-family ipv4
PE2(config-ldp-af4)#transport-address 44.44.44.44
```

```
PE2(config-ldp-af4)#exit
PE2(config-ldp)#exit
PE2(config)#interface gigabitethernet0
PE2(config-if-gigabitethernet0)#mpls ip
PE2(config-if-gigabitethernet0)#mpls ldp
PE2(config-if-gigabitethernet0)#exit
```

#After the configuration is complete, view the LDP session information on the device.

Take PE1 as an example:

```
PE1#show mpls ldp session
Peer IP Address    Peer Type    My Role   State        DS Cap   DeadTime
22.22.22.22        Multicast    Active    OPERATIONAL  Disabled 00:02:20
Statistics for ldp sessions:
    Multicast sessions: 1
    Targeted sessions: 0
```

You can see that PE1 and ASBR1 set up the LDP session successfully.

#View the route label information on the device.

Take PE1 as an example:

```
PE1#show ip route 22.22.22.22 detail
Codes: C - Connected, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
    U - Per-user Static route
    O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external



O   22.22.22.22/32 [110/2] via 10.1.1.1, label 3, 03:19:45, gigabitethernet1
                           10.1.1.1 [0], gigabitethernet1
```

You can see that the loopback port route from PE1 to ASBR1 has the label information.

Note:

- For the checking method of PE2 and ASBR, refer to PE1.

Step 4: Configure IPv6 BGP to advertise the route on the CE and PE.

#Configure IPv6 BGP on PE1.

```
PE1(config)#router bgp 100
PE1(config-bgp)#address-family ipv6
PE1(config-bgp-af)#neighbor 2001:1::2 remote-as 65100
PE1(config-bgp-af)#exit-address-family
PE1(config-bgp)#exit
```

#Configure IPv6 BGP on CE1.

```
CE1#configure terminal
CE1(config)#router bgp 65100
CE1(config-bgp)#bgp router-id 10.10.10.10
CE1(config-bgp)#address-family ipv6
CE1(config-bgp-af)#neighbor 2001:1::1 remote-as 100
CE1(config-bgp-af)#network 3000::1/128
CE1(config-bgp-af)#exit-address-family
CE1(config-bgp)#exit
```

#Configure IPv6 BGP on PE2.

```
PE2#configure terminal
PE2(config)#router bgp 200
PE2(config-bgp)#address-family ipv6
PE2(config-bgp-af)#neighbor 2001:3::2 remote-as 65200
PE2(config-bgp-af)#exit-address-family
PE2(config-bgp)#exit
```

#Configure IPv6 BGP on CE2.

```
CE2#configure terminal
CE2(config)#router bgp 65200
CE2(config-bgp)#bgp router-id 20.20.20.20
CE2(config-bgp)#address-family ipv6 unicast
CE2(config-bgp-af)#neighbor 2001:3::1 remote-as 200
CE2(config-bgp-af)#network 4000::1/128
CE2(config-bgp-af)#exit-address-family
CE2(config-bgp)#exit
```

#On PE1, view the global IPv6 route table.

```
PE1#show ipv6 route
Codes: C - Connected, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management


L   ::1/128 [0/0]
    via ::, 1w3d:01:28:30, lo0
C   2001:1::/64 [0/0]
    via ::, 00:55:45, gigabitethernet1
L   2001:1::1/128 [0/0]
```

```
    via ::, 00:55:45, gigabitethernet1
B   3000::1/128 [20/0]
    via 2001:1::2, 00:05:06, gigabitethernet1
```

You can see that there is the route information of CE1 loopback port in the global IPv6 route table of PE1.

Note:

- For the checking method of PE2, refer to PE1.

Step 5: Configure MP-IBGP between PE and ASBR, and use the loopback interface as the peer address; configure IPv6 BGP between ASBR, and use the direct-connected interface as the peer address.

#On PE1, configure MP-IBGP, activate the neighbor in the IPv6 address family, and configure the label sending capability.

```
PE1(config)#router bgp 100
PE1(config-bgp)#neighbor 22.22.22.22 remote-as 100
PE1(config-bgp)#neighbor 22.22.22.22 update-source loopback 0
PE1(config-bgp)#address-family ipv6
PE1(config-bgp-af)#neighbor 22.22.22.22 activate
PE1(config-bgp-af)#neighbor 22.22.22.22 send-label
PE1(config-bgp-af)#exit-address-family
PE1(config-bgp)#exit
```

#On ASBR1, configure MP-IBGP, activate the neighbor in the IPv6 address family, and configure the label sending capability.

```
ASBR1(config)#router bgp 100
ASBR1(config-bgp)#neighbor 11.11.11.11 remote-as 100
ASBR1(config-bgp)#neighbor 11.11.11.11 update-source loopback 0
ASBR1(config-bgp)#address-family ipv6
ASBR1(config-bgp-af)#neighbor 11.11.11.11 activate
ASBR1(config-bgp-af)#neighbor 11.11.11.11 send-label
ASBR1(config-bgp-af)#neighbor 2001:2::1 remote-as 200
ASBR1(config-bgp-af)#exit-address-family
ASBR1(config-bgp)#exit
```

#On ASBR2, configure MP-IBGP, activate the neighbor in the IPv6 address family, and configure the label sending capability.

```
ASBR2(config)#router bgp 200
ASBR2(config-bgp)#neighbor 44.44.44.44 remote-as 200
ASBR2(config-bgp)#neighbor 44.44.44.44 update-source loopback 0
ASBR2(config-bgp)#address-family ipv6
```

```
ASBR2(config-bgp-af)#neighbor 44.44.44.44 activate
ASBR2(config-bgp-af)#neighbor 44.44.44.44 send-label
ASBR2(config-bgp-af)#neighbor 2001:2::2 remote-as 100
ASBR2(config-bgp-af)#exit-address-family
ASBR2(config-bgp)#exit
```

#On PE2, configure MP-IBGP, activate the neighbor in the IPv6 address family, and configure the label sending capability.

```
PE2(config)#router bgp 200
PE2(config-bgp)#neighbor 33.33.33.33 remote-as 200
PE2(config-bgp)#neighbor 33.33.33.33 update-source loopback 0
PE2(config-bgp)#address-family ipv6
PE2(config-bgp-af)#neighbor 33.33.33.33 activate
PE2(config-bgp-af)#neighbor 33.33.33.33 send-label
PE2(config-bgp-af)#exit-address-family
PE2(config-bgp)#exit
```

Step 6: Check the result.

#After the configuration is complete, view the BGP neighbor information on the PE and ASBR.

Take PE1, ASBR1 as an example:

```
PE1#show bgp ipv6 unicast summary
BGP router identifier 11.11.11.11, local AS number 100
BGP table version is 4
3 BGP AS-PATH entries
0 BGP community entries

Neighbor        V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
22.22.22.22     4   100      10       9        4    0    0 00:06:21        1
2001:1::2       4 65100      32      31        4    0    0 00:25:23        1

Total number of neighbors 2
```

The content of the State/PfxRcd list is displayed as number (the number of the route prefixes received from the neighbor), and you can see that PE1 and ASBR1 set up the BGP neighbor successfully.

```
ASBR1#show bgp ipv6 unicast summary
BGP router identifier 22.22.22.22, local AS number 100
BGP table version is 4
3 BGP AS-PATH entries
0 BGP community entries
```

```
Neighbor        V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
11.11.11.11     4   100      25      25        4    0    0 00:19:40        1
2001:2::1       4   200      11      12        4    0    0 00:08:04        1

Total number of neighbors 2
```

The content of the State/PfxRcd list is displayed as number (the number of the route prefixes received from the neighbor), and you can see that ASBR1 and PE1, ASBR2 set up the BGP neighbor successfully.

#View the IPv6 BGP route table on the PE and ASBR.

Take PE1, ASBR1 as an example:

```
PE1#show bgp ipv6 unicast
BGP table version is 4, local router ID is 11.11.11.11
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network          Next Hop            Metric     LocPrf Weight Path
[B]*> 3000::1/128     2001:1::2                0             0 65100 i
[B]*>i4000::1/128     ::ffff:22.22.22.22
                                    0      100      0 200 65200 i

ASBR1#sh bgp ipv6 unicast
BGP table version is 4, local router ID is 22.22.22.22
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network          Next Hop            Metric     LocPrf Weight Path
[B]*>i3000::1/128     ::ffff:11.11.11.11
                                    0      100      0 65100 i
[B]*> 4000::1/128     2001:2::1                0             0 200 65200 i
```

You can see that there is the IPv6 BGP route information to the peer CE2 in the IPv6 BGP route table of PE1 and ASBR1.

#View the MPLS forwarding table on the PE and ASBR.

Take PE1, ASBR1 as an example

```
PE1#show mpls forwarding-table
```

Pro: L - LDP, O - OSPF, B - MP-BGP, R - RSVP, M - Mapped-Route, S - Static Label,ML - mLDP (ML FEC: Root address/OT/OV), RM - RSVP P2MP (RM FEC: P2MP ID/TID)

Pro Ident FEC Inlabel Outlabel Outgoing Next hop

B global 3000::1/128 24016 / gigabitethernet0 2001:1::2

You can see the there is the route label information of CE1 in the MPLS forwarding table of PE1.

ASBR1#show mpls forwarding-table

Pro: L - LDP, O - OSPF, B - MP-BGP, R - RSVP, M - Mapped-Route, S - Static Label,ML - mLDP (ML FEC: Root address/OT/OV), RM - RSVP P2MP (RM FEC: P2MP ID/TID)

Pro Ident FEC Inlabel Outlabel Outgoing Next hop

B global 4000::1/128 24016 / gigabitethernet1 2001:2::1

You can see that there is CE2 route label information in the MPLS forwarding table of ASBR1.

#On the PE and ASBR, view the route detail information.

Take PE1 and ASBR1 as an example:

PE1#show ipv6 route 4000::1/128

Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS

U - Per-user Static route

O - OSPF, OE-OSPF External, M - Management

B 4000::1/128 [200/0]

via ::ffff:22.22.22.22 [0], label 24016, 00:21:37, gigabitethernet1

::ffff:10.1.1.1 [2], label 3, gigabitethernet1

You can see that there is the route information of CE2 in the route table of PE1, the private network label is 16, and the global label is 3.

ASBR1#show ipv6 route 4000::1/128

Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS

U - Per-user Static route

O - OSPF, OE-OSPF External, M - Management

B 4000::1/128 [20/0]

```
via 2001:2::1 [0], 00:23:12, gigabitethernet1
    2001:2::1 [0], gigabitethernet1
```

You can see that there is the route information of CE2 in the route table of ASBR1.

Note:

- For the checking method of PE2, ASBR2 , refer to PE1, ASBR1.

#On CE1, ping the loopback port of CE2 and view whether the ping can be connected.

```
CE1#ping 4000::1 -s 3000::1

Press key (ctrl + shift + 6) interrupt it.
Reply from  4000::1: bytes = 76  time < 16 ms
Reply from  4000::1: bytes = 76  time < 16 ms
Reply from  4000::1: bytes = 76  time < 16 ms
Reply from  4000::1: bytes = 76  time < 16 ms
Reply from  4000::1: bytes = 76  time < 16 ms
Success rate is 100% (5/5). Round-trip min/avg/max = 0/0/0 ms.
```

You can see that CE1 and CE2 can communicate with each other normally.

6.3.3. Configure Cross-Domain OptionB

Network Requirements

- The whole MPLS network includes two AS domains. CE1 in AS100 needs to communicate with CE2 in AS200.
- CE and PE use IPv6 BGP to exchange the route information.
- Use MP-EBGP to exchange the IPv6 route between ASBRs.
- ASBR and PE use MP-IBGP to exchange the IPv6 route with the label.

Network Topology

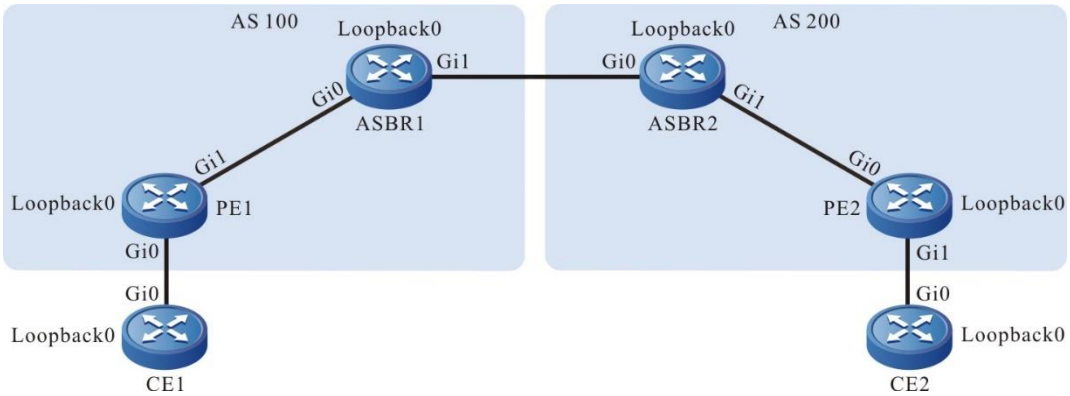

Figure 6-6 Networking of configuring the cross-domain OptionB

Device	Interface	IP Address	Device	Interface	IP Address
CE1	Gi0	2001:1::2/64	ASBR2	Gi0	10.1.3.1/24
	Loopback0	3000::1/128		Gi1	10.1.2.2/24
PE1	Gi0	2001:1::1/64		Loopback0	33.33.33.33/32
	Gi1	10.1.1.2/24	PE2	Gi0	10.1.2.1/24
	Loopback0	11.11.11.11/32		Gi1	2001:2::1/64
ASBR1	Gi0	10.1.1.1/24		Loopback0	44.44.44.44/32
	Gi1	10.1.3.2/24	CE2	Gi0	2001:2::2/64
ASBR1	Loopback0	22.22.22.22/32	CE2	Loopback0	4000::1/128

Configuration Steps

Step 1: Configure the IP address of the interface (omitted).

Step 2: Configure the global OSPF and advertise the global route.

#Configure the global OSPF on PE1.

```
PE1#configure terminal
PE1(config)#router ospf 100
PE1(config-ospf)#network 10.1.1.0 0.0.0.255 area 0
PE1(config-ospf)#network 11.11.11.11 0.0.0.0 area 0
PE1(config-ospf)#exit
```

#Configure the global OSPF on ASBR1.

```
ASBR1#configure terminal
ASBR1(config)#router ospf 100
ASBR1(config-ospf)#network 10.1.1.0 0.0.0.255 area 0
ASBR1(config-ospf)#network 22.22.22.22 0.0.0.0 area 0
ASBR1(config-ospf)#exit
```

#Configure the global OSPF on ASBR2.

```
ASBR2#configure terminal
ASBR2(config)#router ospf 100
ASBR2(config-ospf)#network 10.1.2.0 0.0.0.255 area 0
ASBR2(config-ospf)#network 33.33.33.33 0.0.0.0 area 0
ASBR2(config-ospf)#exit
```

#Configure the global OSPF on PE2.

```
PE2#configure terminal
PE2(config)#router ospf 100
PE2(config-ospf)#network 10.1.2.0 0.0.0.255 area 0
PE2(config-ospf)#network 44.44.44.44 0.0.0.0 area 0
PE2(config-ospf)#exit
```

#After the configuration is complete, view the global route table on the device.

Take PE1 as an example:

```
PE1#show ip route
Codes: C - Connected, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
    U - Per-user Static route
    O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external




C   10.1.1.0/24 is directly connected, 04:49:02, gigabitethernet1
C   127.0.0.0/8 is directly connected, 1w3d:05:22:00, lo0
C   11.11.11.11/32 is directly connected, 04:48:43, loopback0
O   22.22.22.22/32 [110/2] via 10.1.1.1, 04:43:21, gigabitethernet1
```

You can see that there is the route information of the ASBR1 loopback port in the global route table of PE1.

Step 3: Enable MPLS IP and MPLS LDP.

#On PE1, enable the global MPLS IP and MPLS LDP. Meanwhile, enable MPLS IP and MPLS LDP on the interface.

```
PE1(config)#mpls ip
PE1(config)#mpls ldp
PE1(config-ldp)#router-id 11.11.11.11
PE1(config-ldp)#address-family ipv4
PE1(config-ldp-af4)#transport-address 11.11.11.11
PE1(config-ldp-af4)#exit
PE1(config-ldp)#exit
PE1(config)#interface gigabitethernet1
```

```
PE1(config-if-gigabitethernet1)#mpls ip
PE1(config-if-gigabitethernet1)#mpls ldp
PE1(config-if-gigabitethernet1)#exit
```

#On ASBR1, enable the global MPLS IP and MPLS LDP. Meanwhile, enable MPLS IP and MPLS LDP on the interface.

```
ASBR1(config)#mpls ip
ASBR1(config)#mpls ldp
ASBR1(config-ldp)#router-id 22.22.22.22
ASBR1(config-ldp)#address-family ipv4
ASBR1(config-ldp-af4)#transport-address 22.22.22.22
ASBR1(config-ldp-af4)#exit
ASBR1(config-ldp)#exit
ASBR1(config)#interface gigabitethernet0
ASBR1(config-if-gigabitethernet0)#mpls ip
ASBR1(config-if-gigabitethernet0)#mpls ldp
ASBR1(config-if-gigabitethernet0)#exit
ASBR1(config)#interface gigabitethernet1
ASBR1(config-if-gigabitethernet1)#mpls ip
ASBR1(config-if-gigabitethernet1)#exit
```

#On ASBR2, enable the global MPLS IP and MPLS LDP. Meanwhile, enable MPLS IP and MPLS LDP on the interface.

```
ASBR2(config)#mpls ip
ASBR2(config)#mpls ldp
ASBR2(config-ldp)#router-id 33.33.33.33
ASBR2(config-ldp)#address-family ipv4
ASBR2(config-ldp-af4)#transport-address 33.33.33.33
ASBR2(config-ldp-af4)#exit
ASBR2(config-ldp)#exit
ASBR2(config)#interface gigabitethernet1
ASBR2(config-if-gigabitethernet1)#mpls ip
ASBR2(config-if-gigabitethernet1)#mpls ldp
ASBR2(config-if-gigabitethernet1)#exit
ASBR2(config)#interface gigabitethernet0
ASBR2(config-if-gigabitethernet0)#mpls ip
ASBR2(config-if-gigabitethernet0)#exit
```

#On PE2, enable the global MPLS IP and MPLS LDP. Meanwhile, enable MPLS IP and MPLS LDP on the interface.

```
PE2(config)#mpls ip
```

```
PE2(config)#mpls ldp
PE2(config-ldp)#router-id 44.44.44.44
PE2(config-ldp)#address-family ipv4
PE2(config-ldp-af4)#transport-address 44.44.44.44
PE2(config-ldp-af4)#exit
PE2(config-ldp)#exit
PE2(config)#interface gigabitethernet0
PE2(config-if-gigabitethernet0)#mpls ip
PE2(config-if-gigabitethernet0)#mpls ldp
PE2(config-if-gigabitethernet0)#exit
```

#After the configuration is complete, view the LDP session information on the device.

Take PE1 as an example:

```
PE1#show mpls ldp session
Peer IP Address    Peer Type    My Role   State        DS Cap    DeadTime
22.22.22.22        Multicast    Active    OPERATIONAL  Disabled  00:02:20
Statistics for ldp sessions:
    Multicast sessions: 1
    Targeted sessions: 0
```

You can see that PE1 and ASBR1 set up the LDP session successfully.

#View the route label information on the device.

Take PE1 as an example:

```
PE1#show ip route 22.22.22.22 detail
Codes: C - Connected, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
    U - Per-user Static route
    O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external




O   22.22.22.22/32 [110/2] via 10.1.1.1, label 3, 00:5:23, gigabitethernet1
                           10.1.1.1 [0], gigabitethernet1
```

You can see that the loopback port route from PE1 to ASBR1 has the label information.

Note:

For the checking method of ASBR and PE2, refer to PE1.

Step 4: Configure IPv6 BGP to advertise the route on the CE and PE.

#On PE1, configure IPv6 BGP.

```
PE1(config)#router bgp 100
```

```
PE1(config-bgp)#address-family ipv6
PE1(config-bgp-af)#neighbor 2001:1::2 remote-as 65100
PE1(config-bgp-af)#exit-address-family
PE1(config-bgp)#exit
```

#On CE1, configure IPv6 BGP.

```
CE1#configure terminal
CE1(config)#router bgp 65100
CE1(config-bgp)#bgp router-id 10.10.10.10
CE1(config-bgp)#address-family ipv6
CE1(config-bgp-af)#neighbor 2001:1::1 remote-as 100
CE1(config-bgp-af)#network 3000::1/128
CE1(config-bgp-af)#exit-address-family
CE1(config-bgp)#exit
```

#On PE2, configure IPv6 BGP.

```
PE2(config)#router bgp 200
PE2(config-bgp)#address-family ipv6
PE2(config-bgp-af)#neighbor 2001:2::2 remote-as 65200
PE2(config-bgp-af)#exit-address-family
PE2(config-bgp)#exit
```

#On CE2, configure IPv6 BGP.

```
CE2#configure terminal
CE2(config)#router bgp 65200
CE2(config-bgp)#bgp router-id 20.20.20.20
CE2(config-bgp)#address-family ipv6
CE2(config-bgp-af)#neighbor 2001:2::1 remote-as 200
CE2(config-bgp-af)#network 4000::1/128
CE2(config-bgp-af)#exit-address-family
CE2(config-bgp)#exit
```

#On PE1, view the global IPv6 route table.

```
PE1#show ipv6 route
Codes: C - Connected, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management



L   ::1/128 [0/0]
    via ::, 1w3d:01:28:30, lo0
```

```
C   2001:1::/64 [0/0]
    via ::, 00:55:45, gigabitethernet0
L   2001:1::1/128 [0/0]
    via ::, 00:55:45, gigabitethernet0
B   3000::1/128 [20/0]
    via 2001:1::2, 00:05:06, gigabitethernet0
```

You can see that there is the route information of CE1 loopback port in the global IPv6 route table of PE1.

Note:

- For the checking method of PE2, refer to PE1.

Step 5: Configure MP-IBGP between PE and ASBR, and use the loopback interface as the peer address; configure MP-EBGP between ASBR, and use the direct-connected interface as the peer address.

#On PE1, configure MP-IBGP, activate the neighbor in the IPv6 address family, and configure the label sending capability.

```
PE1(config)#router bgp 100
PE1(config-bgp)#neighbor 22.22.22.22 remote-as 100
PE1(config-bgp)#neighbor 22.22.22.22 update-source loopback 0
PE1(config-bgp)#address-family ipv6
PE1(config-bgp-af)#neighbor 22.22.22.22 activate
PE1(config-bgp-af)#neighbor 22.22.22.22 send-label
PE1(config-bgp-af)#exit-address-family
PE1(config-bgp)#exit
```

#On ASBR1, configure MP-IBGP, activate the neighbor in the IPv6 address family, and configure the label sending capability.

```
ASBR1(config)#router bgp 100
ASBR1(config-bgp)#neighbor 11.11.11.11 remote-as 100
ASBR1(config-bgp)#neighbor 11.11.11.11 update-source loopback 0
ASBR1(config-bgp)#neighbor 10.1.3.1 remote-as 200
ASBR1(config-bgp)#address-family ipv6
ASBR1(config-bgp-af)#neighbor 11.11.11.11 activate
ASBR1(config-bgp-af)#neighbor 11.11.11.11 send-label
ASBR1(config-bgp-af)#neighbor 11.11.11.11 next-hop-self
ASBR1(config-bgp-af)#neighbor 10.1.3.1 activate
ASBR1(config-bgp-af)#neighbor 10.1.3.1 send-label
ASBR1(config-bgp-af)#exit-address-family
ASBR1(config-bgp)#exit
```

#On ASBR2, configure MP-IBGP, activate the neighbor in the IPv6 address family, and configure the label sending capability.

```
ASBR2(config)#router bgp 200
ASBR2(config-bgp)#neighbor 44.44.44.44 remote-as 200
ASBR2(config-bgp)#neighbor 44.44.44.44 update-source loopback 0
ASBR2(config-bgp)#neighbor 10.1.3.2 remote-as 100
ASBR2(config-bgp)#address-family ipv6
ASBR2(config-bgp-af)#neighbor 44.44.44.44 activate
ASBR2(config-bgp-af)#neighbor 44.44.44.44 send-label
ASBR2(config-bgp-af)#neighbor 44.44.44.44 next-hop-self
ASBR2(config-bgp-af)#neighbor 10.1.3.2 activate
ASBR2(config-bgp-af)#neighbor 10.1.3.2 send-label
ASBR2(config-bgp-af)#exit-address-family
ASBR2(config-bgp)#exit
```

#On PE2, configure MP-IBGP, activate the neighbor in the IPv6 address family, and configure the label sending capability.

```
PE2(config)#router bgp 200
PE2(config-bgp)#neighbor 33.33.33.33 remote-as 200
PE2(config-bgp)#neighbor 33.33.33.33 update-source loopback 0
PE2(config-bgp)#address-family ipv6
PE2(config-bgp-af)#neighbor 33.33.33.33 activate
PE2(config-bgp-af)#neighbor 33.33.33.33 send-label
PE2(config-bgp-af)#exit-address-family
PE2(config-bgp)#exit
```

Step 6: Check the result.

#After the configuration is complete, view the BGP neighbor information on the PE and ASBR.

Take PE1, ASBR1 as an example:

```
PE1#show bgp ipv6 unicast summary
BGP router identifier 11.11.11.11, local AS number 100
BGP table version is 4
3 BGP AS-PATH entries
0 BGP community entries

Neighbor        V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
22.22.22.22     4   100      10       9        4    0    0 00:06:21        1
2001:1::2       4 65100      32      31        4    0    0 00:25:23        1
```

```
Total number of neighbors 2
```

The content of the State/PfxRcd list is displayed as number (the number of the route prefixes received from the neighbor), and you can see that PE1 and ASBR1, CE1 set up the BGP neighbor successfully.

```
ASBR1#show bgp ipv6 unicast summary
BGP router identifier 22.22.22.22, local AS number 100
BGP table version is 8
3 BGP AS-PATH entries
0 BGP community entries

Neighbor        V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
10.1.3.1        4   200      13      14        8    0    0 00:09:42        1
11.11.11.11     4   100      88      89        8    0    0 01:14:12        1

Total number of neighbors 2
```

The content of the State/PfxRcd list is displayed as number (the number of the route prefixes received from the neighbor), and you can see that ASBR1 and PE1, ASBR2 set up the BGP neighbor successfully.

#View the IPv6 BGP route table on the PE and ASBR.

Take PE1, ASBR1 as an example:

```
PE1#show bgp ipv6 unicast
BGP table version is 4, local router ID is 11.11.11.11
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network          Next Hop            Metric     LocPrf Weight Path
[B]*> 3000::1/128     2001:1::2                0             0 65100 i
[B]*>i4000::1/128     ::ffff:22.22.22.22
                                       0      100      0 200 65200 i

ASBR1#show bgp ipv6 unicast
BGP table version is 8, local router ID is 22.22.22.22
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network          Next Hop            Metric     LocPrf Weight Path
[B]*>i3000::1/128     ::ffff:11.11.11.11
                                       0      100      0 65100 i
```

```
[B]*> 4000::1/128        ::ffff:10.1.3.1        0              0 200 65200 i
```

You can see that there is the IPv6 BGP route information to the peer CE2 in the IPv6 BGP route table of PE1 and ASBR1.

#View the MPLS forwarding table on the PE and ASBR.

Take PE1, ASBR1 as an example

PE1#show mpls forwarding-table

```
Pro: L - LDP, O - OSPF, B - MP-BGP, R - RSVP, M - Mapped-Route, S - Static
Label,ML - mLDP (ML FEC: Root address/OT/OV), RM - RSVP P2MP (RM FEC: P2MP
ID/TID)

Pro Ident        FEC              Inlabel Outlabel Outgoing          Next hop
B   global       3000::1/128        24016   /      gigabitethernet0     2001:1::2
```

You can see that there is the route label information of CE1 in the MPLS forwarding table of PE1.

```
ASBR1#show mpls forwarding-table
Pro: L - LDP, O - OSPF, B - MP-BGP, R - RSVP, M - Mapped-Route, S - Static
Label,ML - mLDP (ML FEC: Root address/OT/OV), RM - RSVP P2MP (RM FEC: P2MP
ID/TID)

Pro Ident        FEC              Inlabel Outlabel Outgoing          Next hop
B   global       3000::1/128        24016   24016    gigabitethernet0     11.11.11.11
B   global       4000::1/128        24017   24016    gigabitethernet1     10.1.3.1
```

You can see that there is the route label information of CE1, CE2 in the MPLS forwarding table of ASBR1.

#On the PE and ASBR, view the route detail information.

Take PE1 and ASBR1 as an example:

```
PE1#show ipv6 route 4000::1/128
Codes: C - Connected, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management

B   4000::1/128 [200/0]
    via ::ffff:22.22.22.22 [0], label 24017, 00:21:37, gigabitethernet1
        ::ffff:10.1.1.1 [2], label 3, gigabitethernet1
```

```
ASBR1#show ipv6 route 4000::1/128
Codes: C - Connected, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management



B   4000::1/128 [20/0]
    via ::ffff:10.1.3.1 [0], label 24016, 00:06:01, gigabitethernet1
        ::ffff:10.1.3.1 [10], gigabitethernet1
```

You can see that there is the route information of CE2 in the route table of PE1, the private network label is 24017, and the global label is 3. There is the route information of CE2 in the route table of ASBR1 and the private network label of the route is 24016.

Note:

For the checking method of PE2, ASBR2, refer to PE1.

#On CE1, ping the loopback port of CE2 and view whether the ping can be connected.

```
CE1#ping 4000::1 -s 3000::1

Press key (ctrl + shift + 6) interrupt it.
Reply from  4000::1: bytes = 76  time < 16 ms
Reply from  4000::1: bytes = 76  time < 16 ms
Reply from  4000::1: bytes = 76  time < 16 ms
Reply from  4000::1: bytes = 76  time < 16 ms
Reply from  4000::1: bytes = 76  time < 16 ms
Success rate is 100% (5/5). Round-trip min/avg/max = 0/0/0 ms.
```

You can see that CE1 and CE2 can communicate with each other.

6.3.4. Configure 6PE Route Reflector

Network Requirements

- CE and PE use IPv6 BGP to exchange the IPv6 route information.
- PE1, PE2 and RR use MP-IBGP to exchange the IPv6 route information with the label.
- On the RR, configure PE1 and PE2 as the reflector client.

Network Topology

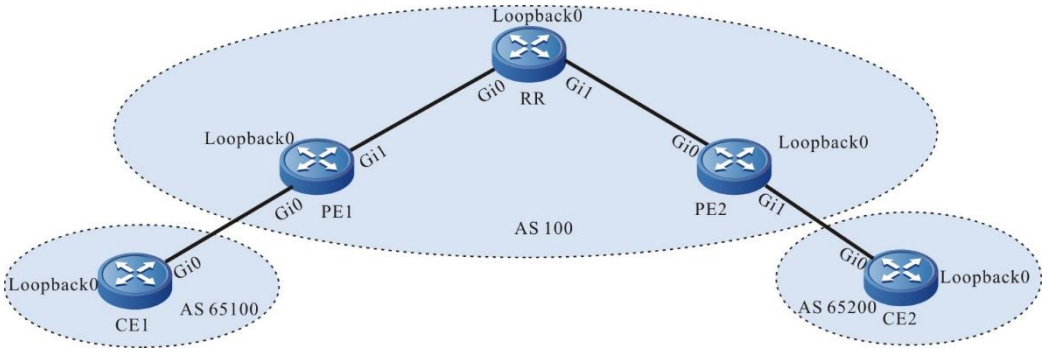

Figure 6-7 Networking of configuring 6PE route reflector

Device	Interface	IP Address	Device	Interface	IP Address
CE1	Gi0	2001:1::2/64	RR	Loopback0	22.22.22.22/32
	Loopback0	3000::1/128	PE2	Gi0	10.1.2.1/24
PE1	Gi0	2001:1::1/64		Gi1	2001:2::1/64
PE1	Gi1	10.1.1.2/24	PE2	Loopback0	33.33.33.33/32
	Loopback0	11.11.11.11/32	CE2	Gi0	2001:2::2/64
RR	Gi0	10.1.1.2/24		Loopback0	4000::1/128
	Gi1	10.1.2.2/24			

Configuration Steps

Step 1: Configure the IP address of the interface (omitted).

Step 2: Configure the global OSPF and advertise the global route.

#Configure the global OSPF on PE1.

```
PE1#configure terminal
PE1(config)#router ospf 100
PE1(config-ospf)#network 10.1.1.0 0.0.0.255 area 0
PE1(config-ospf)#network 11.11.11.11 0.0.0.0 area 0
PE1(config-ospf)#exit
```

#Configure the global OSPF on RR.

```
RR#configure terminal
RR(config)#router ospf 100
RR(config-ospf)#network 10.1.1.0 0.0.0.255 area 0
RR(config-ospf)#network 10.1.2.0 0.0.0.255 area 0
RR(config-ospf)#network 22.22.22.22 0.0.0.0 area 0
RR(config-ospf)#exit
```

#Configure the global OSPF on PE2.

```
PE2#configure terminal
PE2(config)#router ospf 100
PE2(config-ospf)#network 10.1.2.0 0.0.0.255 area 0
PE2(config-ospf)#network 33.33.33.33 0.0.0.0 area 0
PE2(config-ospf)#exit
```

#After the configuration is complete, view the global route table on the device.

Take PE1 as an example:

```
PE1#show ip route
Codes: C - Connected, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
    U - Per-user Static route
    O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external



C   10.1.1.0/24 is directly connected, 00:10:59, gigabitethernet1
O   10.1.2.0/24 [110/2] via 10.1.1.1, 00:05:29, gigabitethernet1
C   127.0.0.0/8 is directly connected, 1w3d:00:43:58, lo0
C   11.11.11.11/32 is directly connected, 00:10:40, loopback0
O   22.22.22.22/32 [110/2] via 10.1.1.1, 00:04:19, gigabitethernet1
O   33.33.33.33/32 [110/3] via 10.1.1.1, 00:01:47, gigabitethernet1
```

You can see that there is the route information of RR, PE2 loopback ports in the global route table of PE1.

Note:

- For the checking method of RR, PE2, refer to PE1.

Step 3: Enable MPLS IP and MPLS LDP.

#On PE1, enable the global MPLS IP and MPLS LDP. Meanwhile, enable MPLS IP and MPLS LDP on the interface.

```
PE1(config)#mpls ip
PE1(config)#mpls ldp
```

```
PE1(config-ldp)#router-id 11.11.11.11
PE1(config-ldp)#address-family ipv4
PE1(config-ldp-af4)#transport-address 11.11.11.11
PE1(config-ldp-af4)#exit
PE1(config-ldp)#exit
PE1(config)#interface gigabitethernet1
PE1(config-if-gigabitethernet1)#mpls ip
PE1(config-if-gigabitethernet1)#mpls ldp
PE1(config-if-gigabitethernet1)#exit
```

#On RR, enable the global MPLS IP and MPLS LDP. Meanwhile, enable MPLS IP and MPLS LDP on the interface.

```
RR(config)#mpls ip
RR(config)#mpls ldp
RR(config-ldp)#router-id 22.22.22.22
RR(config-ldp)#address-family ipv4
RR(config-ldp-af4)#transport-address 22.22.22.22
RR(config-ldp-af4)#exit
RR(config-ldp)#exit
RR(config)#interface gigabitethernet0
RR(config-if-gigabitethernet0)#mpls ip
RR(config-if-gigabitethernet0)#mpls ldp
RR(config-if-gigabitethernet0)#exit
RR(config)#interface gigabitethernet1
RR(config-if-gigabitethernet1)#mpls ip
RR(config-if-gigabitethernet1)#mpls ldp
RR(config-if-gigabitethernet1)#exit
```

#On PE2, enable the global MPLS IP and MPLS LDP. Meanwhile, enable MPLS IP and MPLS LDP on the interface.

```
PE2(config)#mpls ip
PE2(config)#mpls ldp
PE2(config-ldp)#router-id 33.33.33.33
PE2(config-ldp)#address-family ipv4
PE2(config-ldp-af4)#transport-address 33.33.33.33
PE2(config-ldp-af4)#exit
PE2(config-ldp)#exit
PE2(config)#interface gigabitethernet0
PE2(config-if-gigabitethernet0)#mpls ip
PE2(config-if-gigabitethernet0)#mpls ldp
```

```
PE2(config-if-gigabitethernet0)#exit
```

Note:

- router-id and transport-address can be configured manually and also can be generated automatically. Usually, they are configured the same. If not configuring router-id and transport-address manually, the device will select automatically. From the up interfaces, first select the Loopback interface with the maximum IP address. If the device does not configure the Loopback interface address, select the common interface with the maximum IP address.

#After the configuration is complete, view the LDP session information on the device.

Take PE1 as an example:

```
PE1#show mpls ldp session
Peer IP Address    Peer Type    My Role   State        DS Cap   DeadTime
22.22.22.22        Multicast    Active    OPERATIONAL  Disabled 00:02:20
Statistics for ldp sessions:
    Multicast sessions: 1
    Targeted sessions: 0
```

You can see that PE1 and RR set up the LDP session successfully.

#View the route label information on the device.

Take PE1 as an example:

```
PE1#show ip route 22.22.22.22 detail
Codes: C - Connected, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
    U - Per-user Static route
    O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external



O   22.22.22.22/32 [110/2] via 10.1.1.1, label 3, 00:5:23, gigabitethernet1
                   10.1.1.1 [0], gigabitethernet1

PE1#show ip route 33.33.33.33 detail
Codes: C - Connected, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
    U - Per-user Static route
    O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external



O  33.33.33.33/32 [110/2] via 10.1.1.1, label 24017, 00:5:23, gigabitethernet1
                  10.1.1.1 [0], gigabitethernet1
```

You can see that the loopback port route from PE1 to RP and PE2 has the label information.

Note:

- For the checking method of RR, PE2, refer to PE1.

Step 4: On CE and PE, configure IPv6 BGP to advertise the route.

#On PE1, configure IPv6 BGP.

```
PE1(config)#router bgp 100
PE1(config-bgp)#address-family ipv6
PE1(config-bgp-af)#neighbor 2001:1::2 remote-as 65100
PE1(config-bgp-af)#exit-address-family
PE1(config-bgp)#exit
```

#On CE1, configure IPv6 BGP.

```
CE1#configure terminal
CE1(config)#router bgp 65100
CE1(config-bgp)#bgp router-id 10.10.10.10
CE1(config-bgp)#address-family ipv6
CE1(config-bgp-af)#neighbor 2001:1::1 remote-as 100
CE1(config-bgp-af)#network 3000::1/128
CE1(config-bgp-af)#exit-address-family
CE1(config-bgp)#exit
```

#On PE2, configure IPv6 BGP.

```
PE2(config)#router bgp 100
PE2(config-bgp)#address-family ipv6
PE2(config-bgp-af)#neighbor 2001:2::2 remote-as 65200
PE2(config-bgp-af)#exit-address-family
PE2(config-bgp)#exit
```

#On CE2, configure IPv6 BGP.

```
CE2#configure terminal
CE2(config)#router bgp 65200
CE2(config-bgp)#bgp router-id 20.20.20.20
CE2(config-bgp)#address-family ipv6
CE2(config-bgp-af)#neighbor 2001:2::1 remote-as 100
CE2(config-bgp-af)#network 4000::1/128
CE2(config-bgp-af)#exit-address-family
CE2(config-bgp)#exit
```

#On PE1, view the global IPv6 route table.

```
PE1#show ipv6 route
Codes: C - Connected, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management


L   ::1/128 [0/0]
    via ::, 1w3d:01:28:30, lo0
C   2001:1::/64 [0/0]
    via ::, 00:55:45, gigabitethernet0
L   2001:1::1/128 [0/0]
    via ::, 00:55:45, gigabitethernet0
B   3000::1/128 [20/0]
    via 2001:1::2, 00:05:06, gigabitethernet0
```

You can see that there is the route information of CE1 loopback port in the global IPv6 route table of PE1.

Note:

- For the checking method of PE2, refer to PE1.

Step 5: Configure MP-IBGP, use the loopback port interface as the peer address, and configure RR as the route reflector.

#On PE1, configure MP-IBGP, activate the neighbor in the IPv6 address family, and configure the label sending capability.

```
PE1(config)#router bgp 100
PE1(config-bgp)#neighbor 22.22.22.22 remote-as 100
PE1(config-bgp)#neighbor 22.22.22.22 update-source loopback 0
PE1(config-bgp)#address-family ipv6
PE1(config-bgp-af)#neighbor 22.22.22.22 activate
PE1(config-bgp-af)#neighbor 22.22.22.22 send-label
PE1(config-bgp-af)#exit-address-family
PE1(config-bgp)#exit
```

#On RR, configure MP-IBGP, activate the neighbor in the IPv6 address family, and configure the label sending capability. Configure PE1 and PE2 as the reflector client.

```
RR(config)#router bgp 100
RR(config-bgp)#neighbor 11.11.11.11 remote-as 100
RR(config-bgp)#neighbor 11.11.11.11 update-source loopback 0
RR(config-bgp)#neighbor 33.33.33.33 remote-as 100
RR(config-bgp)#neighbor 33.33.33.33 update-source loopback 0
RR(config-bgp)#address-family ipv6
```

```
RR(config-bgp-af)#neighbor 11.11.11.11 activate
RR(config-bgp-af)#neighbor 11.11.11.11 send-label
RR(config-bgp-af)#neighbor 11.11.11.11 route-reflector-client
RR(config-bgp-af)#neighbor 33.33.33.33 activate
RR(config-bgp-af)#neighbor 33.33.33.33 send-label
RR(config-bgp-af)#neighbor 33.33.33.33 route-reflector-client
RR(config-bgp-af)#exit-address-family
RR(config-bgp)#exit
```

#On PE2, configure MP-IBGP, activate the neighbor in the IPv6 address family, and configure the label sending capability.

```
PE2(config)#router bgp 100
PE2(config-bgp)#neighbor 22.22.22.22 remote-as 100
PE2(config-bgp)#neighbor 22.22.22.22 update-source loopback 0
PE2(config-bgp)#address-family ipv6
PE2(config-bgp-af)#neighbor 22.22.22.22 activate
PE2(config-bgp-af)#neighbor 22.22.22.22 send-label
PE2(config-bgp-af)#exit-address-family
PE2(config-bgp)#exit
```

Step 6: Check the result.

#After the configuration is complete, view the BGP neighbor information on the PE.

Take PE1 as an example:

```
PE1#show bgp ipv6 unicast summary
BGP router identifier 11.11.11.11, local AS number 100
BGP table version is 4
3 BGP AS-PATH entries
0 BGP community entries

Neighbor        V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
22.22.22.22     4   100      10       9        5    0    0 00:06:21        1
2001:1::2       4 65100      32      31        5    0    0 00:25:23        1

Total number of neighbors 2
```

The content of the State/PfxRcd list is displayed as number (the number of the route prefixes received from the neighbor), and you can see that PE1 and RR, CE1 set up the BGP neighbor successfully.

#View the BGP IPv6 route table and the global IPv6 route table on the PE.

Take PE1 as an example:

```
PE1#show bgp ipv6 unicast
BGP table version is 4, local router ID is 11.11.11.11
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network          Next Hop            Metric     LocPrf Weight Path
[B]*> 3000::1/128     2001:1::2              0              0 65100 i
[B]*>i4000::1/128     ::ffff:33.33.33.33
                                     0      100      0  i

PE1#show ipv6 route
Codes: C - Connected, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management

L   ::1/128 [0/0]
     via ::, 1w3d:01:51:03, lo0
C   2001:1::/64 [0/0]
     via ::, 01:18:18, gigabitethernet0
L   2001:1::1/128 [0/0]
     via ::, 01:18:18, gigabitethernet0
B   3000::1/128 [20/0]
     via 2001:1::2, 00:27:38, gigabitethernet0
B   4000::1/128 [200/0]
     via ::ffff:33.33.33.33, 00:08:13, gigabitethernet1
```

You can see that there is the route information to the peer CE2 in the BGP IPv6 route table of PE1 and global IPv6 route table.

#On the PE, view the MPLS forwarding table.

Take PE1 as an example:

```
PE1#show mpls forwarding-table
Pro: L - LDP, O - OSPF, B - MP-BGP, R - RSVP, M - Mapped-Route, S - Static
Label,ML - mLDP (ML FEC: Root address/OT/OV), RM - RSVP P2MP (RM FEC: P2MP
ID/TID)

Pro Ident       FEC             Inlabel Outlabel Outgoing       Next hop
```

B global 3000::1/128 25120 / gigabitethernet0 2001:1::2 You can see that there is the route label information of CE1 in the MPLS forwarding table of PE1.

#On the PE, view the route detail information.

Take PE1 as an example:

```
PE1#show ipv6 route 4000::1/128
Codes: C - Connected, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management



B   4000::1/128 [200/0]
      via ::ffff:33.33.33.33 [0], label 25120, 00:12:18, gigabitethernet1
        ::ffff:10.1.1.1 [3], label 24017, gigabitethernet1
```

You can see that there is the route information of CE2 in the route table of PE1, the private network label of the route is 25120, and the global label is 24017.

Note:

- For the checking method of RR, PE2, refer to PE1.

#On CE1, ping the loopback port of CE2 and view whether the ping can be connected.

```
CE1#ping 4000::1 -s 3000::1

Press key (ctrl + shift + 6) interrupt it.
Reply from  4000::1: bytes = 76  time < 16 ms
Reply from  4000::1: bytes = 76  time < 16 ms
Reply from  4000::1: bytes = 76  time < 16 ms
Reply from  4000::1: bytes = 76  time < 16 ms
Reply from  4000::1: bytes = 76  time < 16 ms
Success rate is 100% (5/5). Round-trip min/avg/max = 0/0/0 ms.
```

You can see that CE1 and CE2 can communicate with each other normally.

7. IPV6 MPLS L3VPN

7.1. Overview

IPv6 MPLS L3VPN is one network technology of permitting the service provider to use its IP backbone network to provide the L3 VPN service for the user. In the IPv6 MPLS L3VPN network, BGP is used to release the VPNv6 route information in the backbone network of the service provider. MPLS is used to forward the VPN service from one VPN site to another site.

VRF (VPN Routing/Forwarding Instance) is one basic concept in the IPv6 MPLS L3VPN network technology. Each VRF can be seen as one virtual router and owns one separate route table. Meanwhile, VRF has the separate address space, one group of interface set belonging to the VRF, and one group of route protocol only used by the VRF. The VRF technology can be used to separate different VPN users and solve the problem of the network address overlapping.

The following figure is the diagram of the IPv6 MPLS L3VPN network architecture.

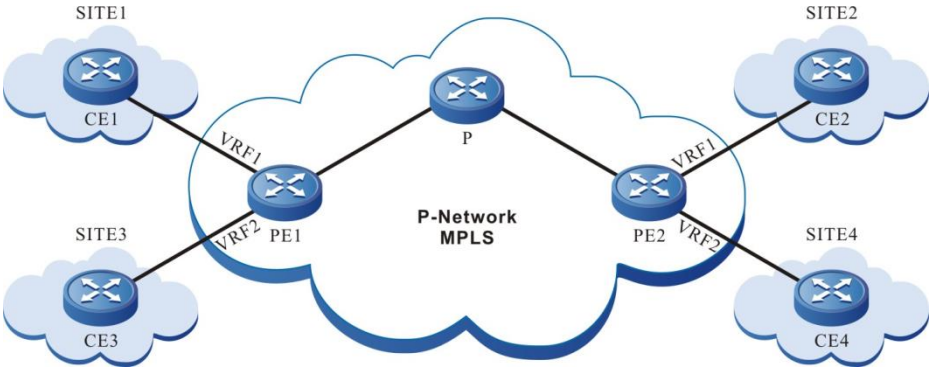

Figure 7-1 IPv6 MPLS L3VPN networking

In the above figure, each PE contains two VRFs, connecting two sites. The two interfaces connecting the sites belong to two VRFs respectively. Site 1 and site 2 belong to one VPN. Site 3 and site 4 belong to the other VPN. According to the above figure, you can see that IPv6 MPLS L3VPN theory is the same as MPLS L3VPN theory. The difference is that in the IPv6 MPLS L3VPN network, all P devices do not perceive the existing of the IPv6 network, the PE device is at the edge of the IPv4 network and IPv6 network and runs the IPv4 and IPv6 dual-protocol stack, the CE device only runs the IPv6 protocol stack, and the PE devices use MP-BGP to exchange the VPNv6 route and the distributed label.

7.2. IPv6 MPLS L3VPN Function Configuration

Table 7-1 IPv6 MPLS L3VPN function configuration list

Configuration Task	
Configure the VPN basic functions	Configure the VPN instance
	Configure PE-PE route exchange
	Configure PE-CE route exchange
Configure M-VRF	Configure M-VRF
Configure the VPN route label distributing	Configure the VPN route label distributing
Configure the VPN cross-domain	Configure the Option-A cross-domain
	Configure the Option-B cross-domain
Configure the VPN user to access Internet	Configure CE to access Internet
Configure the AS covering	Configure the AS covering
Configure the OSPF sham link	Configure the OSPF sham link
Configure VPN ORF	Configure VPN ORF

7.2.1. Configure VPN Basic Functions

Configuration Condition

Before configuring the VPN basic functions, first complete the following tasks:

- Configure the IGP of the MPLS backbone network, making the IP between the PE devices reachable.
- Configure the MPLS basic capability and LDP of the MPLS backbone network, and set up LSP between PE devices.

Configure a VPN Instance

VRF can separate the routes between different VPNs, between VPN and public network. When configuring IPv6 MPLS L3VPN, it is necessary to configure the VPN instance on the PE device and associate the Site in the VPN instance.

1. Configure VRF

VRF is used to separate different VPN users. In different VRFs, permit the address overlapping. When the VRF route is transmitted in the service provider network, it is sure to solve the problem of address overlapping. This requires that each VRF needs one local unique RD. When PE sends the VRF route to the remote PE, add RD to the front of each IPv6 prefix, forming the unique VPNv6 address.

Table 7-2 Configure VRF

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Create one VRF and enter the VRF configuration mode	**ip vrf** *vrf-name*	Mandatory By default, do not configure any VRF.
Configure the VRF RD	**rd** *route-distinguisher*	Mandatory By default, do not configure the RD of the VRF.

Note:

- After configuring VRF, you should configure RD at the same time so that VRF can be used.
- After configuring the VRF RD, you cannot directly delete or modify it. When it is necessary to delete or modify, use the **no ip vrf** command to delete VRF, and then configure RD. The RD cannot be the same as the other VRF RD of the device.

2. Configure VRF to associate with the interface

The PE device connects with the CE via the local configured VRF. The interface connected with the CE needs to associate with the corresponding VRF.

Table 7-3 Configure the VRF to associate with the interface

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the interface configuration mode	**interface** *interface-name*	-
Configure the interface to associate with VRF	**ip vrf forwarding** *vrf-name*	Mandatory By default, the interface does not associate with any VRF.
Configure the interface IPv6 address	**ipv6 address** *ipv6-address/mask-len*	Mandatory By default, the interface is not configured with the IPv6 address.

Note:

- After configuring the **ip vrf forwarding** command in the interface, the existing IPv6 address of the interface will be deleted automatically and needs to be configured again.

3. Configure the VRF attribute

When the local PE receives the VPNv6 route information sent by the remote PE device, the local PE device needs to confirm in which local VRF the VPNv6 route is placed. To control the distributing of the VPNv6 route, each VRF needs one or multiple RT attributes. There are two kinds of RT attributes: Export RT and Import RT. When the PE initiates the VPNv6 route, carry the Export RT attribute. When the PE decides which VRF the VPNv6 route is imported to, use the Export RT attribute carried by the route to match with the Import RT of the local VRF.

Besides that the VRF RT attribute can control the distributing of the VPNv6 route, the route policy on VRF also can control the route distributing. Two route policies can be configured: Import map and Import map. Import map uses the route map to control whether the route can import the VRF. Export map uses the route map to change the attributes of the route initiated from the VRF.

Table 7-4 Configure the VRF attributes

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Create one VRF and enter the VRF configuration mode	**ip vrf** *vrf-name*	Mandatory By default, do not configure any VRF.
Enter the VRF IPv6 configuration mode	**address-family ipv6**	-
Configure the VRF RT	**route-target** [**both** | **export** | **import**] { *ASN:nn* | *IP-address:nn* }	Optional By default, do not configure the Export, Import RT attributes of the VRF.
Configure the VRF ingress route policy	**import map** *rtmap-name*	Optional By default, do not configure the VRF ingress route policy.
Configure the VRF egress route policy	**export map** *rtmap-name*	Optional By default, do not configure the VRF egress route policy.

Note:

- The Import map policy is valid for the local route and the remote VPN route.
- The Export map policy is valid only for the local route.
- Export map cannot perform the route filter, but can only modify the attributes of the VPN route released by the VRF. The attributes that can be modified include: community, extcommunity, and local-preference.
- When the PE imports the VPNv6 to the VRF, the RT match rule has higher priority than Import map, that is, first match the RT rule, and then match the Import map.

Configure PE-PE Route Exchange

In the IPv6 MPLS L3VPN network, set up the IPv4 or IPv6 connection and exchange the VPNv6 route via MP-IBGP between PEs. The configuration modes of the two PEs are the same.

Table 7-5 Configure PE-PE route exchange

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enable the BGP protocol and enter the BGP configuration mode	**router bgp** *autonomous-system*	-
Configure the PE neighbor	**neighbor** { *ipv4-address* | *ipv6-address* | *peer-group-name* } **remote-as** *as-number*	Mandatory By default, do not configure any PE neighbor.
Configure the source address used by setting up the PE neighbor	**neighbor** { *ipv4-address* | *ipv6-address* | *peer-group-name* } **update-source** { *interface* | *ip-address* }	Mandatory By default, use the egress interface address to the PE neighbor route as the source address.
Enter the BGP VPNv6 configuration mode	**address-family vpnv6** [**unicast**]	-
Activate the VPNv6 address family of the PE neighbor	**neighbor** { *ipv4-address* | *ipv6-address* | *peer-group-name* } **activate**	Mandatory By default, the BGP neighbors can only receive and send the IPv4 unicast route.
Configure sending the extended community attributes to the PE neighbor	**neighbor** { *ipv4-address* | *ipv6-address* | *peer-group-name* } **send-community** [**both** | **extended** | **standard**]	Optional By default, the VPNv6 address family of the activated neighbor will automatically configure sending the extended community attribute.
Configure the VPNv6 route suppression function	**bgp dampening** [*reach-half-life* [*reuse-value suppress-value max-suppress-time* [*unreach-half-life*]] | **route-map** *rtmap-name*]	Optional By default, do not enable the VPNv6 route suppression function.

Note:

- Many route features in the BGP VPNv6 address family are the same as the route features in the BGP IPv6 unicast address family. Whether to select the features is decided by the networking demands. For details, refer to the IPv6 MPLS L3VPN chapter of the technical manual.
- IPv4 LDP is deployed in the backbone network, and IPv4 connection is established between PE and PE; IPv6 LDP is deployed in the backbone network, and the IPv6 connection is established between PE and PE.

Configure PE-CE Route Exchange

PE and CE can use the IPv6 static route, OSPFv3 and BGP4+ route protocol to exchange the route. Which protocol is adopted depends on the actual network environment. The PE configuration is the same as the CE configuration mode.

1. Configure PE-CE to use IPv6 static route

Table 7-6 Configure PE-CE to use the IPv6 static route

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Configure the static route to the CE	**ipv6 route vrf** *vrf-name1 ipv6-prefix/mask-length* { *interface-name* | [*nexthop-ipv6-address* [**vrf** *vrf-name2*]]} [**name** *nexthop-name*] [**tag** *tag-value*] [**track** *track-id*] [*administrative-distance*]	Mandatory By default, do not configure the static route to the CE.
Enable the BGP protocol and enter the BGP configuration mode	**router bgp** *autonomous-system*	-
Enter the BGP IPv6 VRF configuration mode	**address-family ipv6 vrf** *vrf-name*	Mandatory By default, it is in the BGP IPv4 unicast configuration mode.
Configure BGP to re-distribute the static route	**redistribute static** [**route-map** *map-name* / **metric** *value*]	Optional By default, do not configure BGP to re-distribute the static route.

2. Configure PE-CE to use OSPFv3

Table 7-7 Configure PE-CE to use OSPFv3

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Create one OSPFv3 process and enter the OSPFv3 configuration mode	**ipv6 router ospf** *process-id* **vrf** *vrf-name*	Mandatory In VRF, enable the OSPF process. By default, the system does not enable the OSPF protocol. When enabling OSPF in the VRF, the OSPF process belonging to one VRF can only manage the interfaces belonging to the VRF.
Configure OSPFv3 router-id	**router-id** *router-id*	Mandatory By default, OSPFv3 does not configure router-id.
Return to the global configuration mode	**exit**	-
Enter the interface configuration mode	**interface** *interface-name*	-
Configure the interface to associate with VRF	**ip vrf forwarding** *vrf-name*	Mandatory By default, the interface is not associated with VRF.
Configure the interface IPv6 address	**ipv6 address** *ipv6-address/mask-len*	Mandatory By default, the interface is not configured with the IPv6 address.
Configure the connected interface of PE and CE to enable the OSPFv3 protocol	**ipv6 router ospf** *process-id* **area** *area-id* [**instance-id** *instance-id*]	Mandatory By default, the interface does not enable the OSPFv3 protocol.

Step	Command	Description
Return to the global configuration mode	**exit**	-
Enable the BGP protocol and enter the BGP configuration mode	**router bgp** *autonomous-system*	-
Enter the BGP IPv6 VRF configuration mode	**address-family ipv6 vrf** *vrf-name*	Mandatory By default, the system is in the BGP IPv4 unicast configuration mode.
Configure BGP to re-distribute OSPFv3	**redistribute ospf** *as-number* [**route-map** *map-name* / **metric** *value* / **match** *level*]	Optional By default, do not re-distribute the OSPF protocol route.

3. Configure PE-CE to use BGP4+

Table 7-8 Configure PE-CE to use BGP4+

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enable the BGP protocol and enter the BGP configuration mode	**router bgp** *autonomous-system*	-
Enter the BGP IPv6 VRF configuration mode	**address-family ipv6 vrf** *vrf-name*	Mandatory By default, the system is in the BGP IPv4 unicast configuration mode.
Configure CE as the EBGP neighbor	**neighbor** { *ipv6-address* | *peer-group-name* } **remote-as** *as-number*	Mandatory By default, do not configure any CE neighbor.

Configure BGP to Use RT for ORF Filter Function

This function only works in VPN-TARGET address family mode and is enabled by default. Do not support configuring the neighbor peer group. According to RFC 4684, it is not recommended to disable. After BGP learns RT NLRI, as long as the prefix information has the RT information, it can use the learned RT NLRI information to perform the corresponding policy control. It can also allow users not to give RT policy control. This command provides this option, command asynchronous processing.

Table 7-9 Configure BGP to use RT for the ORF filter function

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the BGP configuration mode	**router bgp** *autonomous-system*	-
Enter the VPN-TARGET address family configuration mode	**address-family ipv4 vpn-target**	Mandatory By default, BGP does not enter the VPN-TARGET address family mode.
Configure the neighbor to use RT for the ORF filter function	**neighbor** *neighbor-address* **constraint-rt-filter enable**	Optional By default, using RT for the ORF filter is enabled by default.
Configure the neighbor not to use RT for the ORF filter function	**neighbor** *neighbor-address* **constraint-rt-filter disable**	Mandatory By default, disable using RT for the ORF filter.

Note:

- Configure whether to permit the RT ORF function, only working in the filtering when advertising the VPN route. For example, when receiving the peer RT NLRI, no matter whether to enable the RT-Filter function, it needs to start the VPN route update releasing timer, and update the VPN route. You need to judge whether to enable RT-Filter only when performing the egress filter for VPN. In this way, for CISCO-like devices, there is no problem if not sending the Refresh packet after activating the VPN-Target address family.

Configure BGP to Set the RT Filter Table Installation Items of EBGP Neighbor

For the VPN-RT routes learned from the EBGP neighbor, besides the best route, permit the non-best route to install the RT filter table of the neighbor.

Table 7-10 Configure the BGP max, load balance items

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the BGP configuration mode	**router bgp** *autonomous-system*	-
Enter the VPN-TARGET address family configuration mode	**address-family ipv4 vpn-target**	Mandatory By default, BGP does not enter the VPN-TARGET address family mode.
Set the RT filter table installation items of the EBGP neighbor	**rt-filter external-path** *path-number*	Mandatory By default, only install one best route.

7.2.2. Configure M-VRF

Configuration Condition

Before configuring M-VRF, first complete the following task:

- Configure the link-layer protocol of the connecting interfaces of the M-VRF device with the PE and site and keep connected.

Configure M-VRF

M-VRF is one cheap method of expanding the VPN function to the CE. When the customer has multiple services, do not need to divide multiple services to one CE, but configure multiple VRFs on the M-VRF device, virtualizing multiple CEs and separating each service. The following describes one M-VRF example.

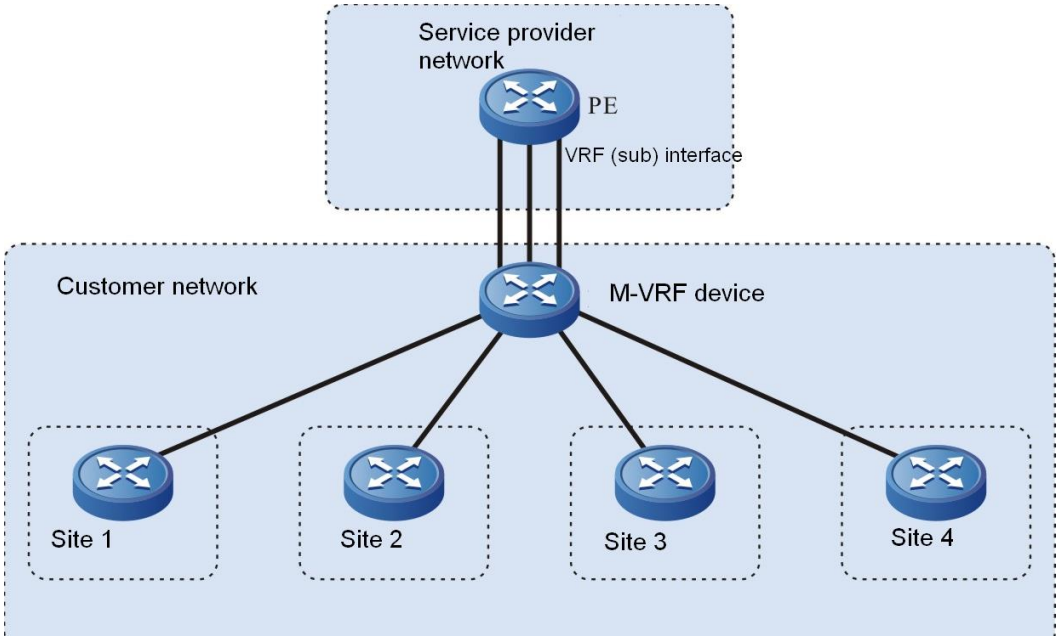

Figure 7-2 Networking of configuring M-VRF

On the M-VRF device, each VRF has one interface to connect the site and the other interface connects the PE. Usually, the M-VRF device is connected with the PE via the Ethernet link. Each VRF uses one interface (or sub interface).

1. Configure the route exchange between the M-VRF device and PE

The route exchange between the M-VRF device and the CE can use the IPv6 static route, OSPFv3 and BGP4+ route protocol. The following example uses the OSPFv3 to exchange the route.

Table 7-11 Configure the route exchange between the M-VRF device and PE

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Create one VRF and enter the VRF configuration mode	**ip vrf** *vrf-name*	Mandatory By default, do not configure any VRF.
Configure the VRF RD	**rd** *route-distinguisher*	Mandatory By default, do not configure the VRF RD.
Exit the VRF configuration mode	**exit**	-

Step	Command	Description
Create an OSPFv3 process and enter he OSPFv3 configuration mode	**ipv6 router ospf** *process-id* **vrf** *vrf-name*	Mandatory In VRF, enable the OSPFv3 process. By default, the system does not enable the OSPFv3 protocol. When enabling OSPFv3 in the VRF, the OSPFv3 process belonging to one VRF can only manage the interfaces that belong to the VRF.
Configure OSPFv3 router-id	**router-id** *router-id*	Mandatory By default, OSPFv3 does not configure router-id.
Return to the global configuration mode	**exit**	-
Enter the interface configuration mode	**interface** *interface_name*	-
Configure the interface to associate with VRF	**ip vrf forwarding** *vrf-name*	Mandatory By default, the interface does not associate with any VRF.
Configure the IPv6 address of the interface	**ipv6 address** *ipv6-address/mask-len*	Mandatory By default, the interface is not configured with the IPv6 address.
Configure the interface to enable the OSPFv3 protocol	**ipv6 router ospf** *process-id* **area** *area-id* [**instance-id** *instance-id*]	Mandatory By default, the interface does not enable the OSPFv3 protocol.

Note:

- On the M-VRF device, each VRF should be configured according to the above steps.
- For the configuration of the PE, refer to the part of “Configure VPN basic functions”.

2. Configure the route exchange between the M-VRF device and site

The route exchange between the M-VRF device and the site, you can use the IPv6 static route, OSPFv3 and BGP4+ route protocol. The following example uses the IPv6 static route.

Table 7-12 Configure the route exchange between the M-VRF and site

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Create one VRF and enter the VRF configuration mode	**ip vrf** *vrf-name*	Mandatory By default, do not configure any VRF.
Configure the VRF RD	**rd** *route-distinguisher*	Mandatory By default, do not configure the VRF RD.
Exit the VPN instance configuration mode	**exit**	-
Enter the interface configuration mode	**interface** *interface_name*	-
Configure the interface to associate with the VRF	**ip vrf forwarding** *vrf-name*	Mandatory By default, the interface does not associate with any VRF.
Configure the interface IPv6 address	**ipv6 address** *ipv6-address/mask-len*	Mandatory By default, the interface is not configured with the IPv6 address.
Exit the interface configuration mode	**exit**	-
Configure the IPv6 static route to the site	**ipv6 route vrf** *vrf-name1 ipv6-prefix/mask-length* { *interface-name* | [*nexthop-ipv6-address* [**vrf** *vrf-name2*]]} [**name** *nexthop-name*] [**tag** *tag-value*] [**track** *track-id*] [*administrative-distance*]	Mandatory By default, do not configure the IPv6 static route to the site.

Note:

- On the M-VRF device, each VRF should be configured according to the above steps.
- The configuration mode on the site is the same as the common IPv6 static route configuration.

7.2.3. Configure VPN Route Label Distributing

Configuration Condition

Before configuring the VPN route label distributing mode, first complete the following task:

- Configure VPN basic functions

Configure VPN Route Label Distributing

BGP has two modes of distributing the label for the VPN route: per-route label distributing mode and per-VRF label distributing mode. When adopting the per-route mode, BGP distributes different labels for each VPN route. When adopting per-VRF mode, BGP distributes the same label for the VPN routes in one VRF, but distributes different labels for the routes in different VRFs.

By default, BGP adopts the per-VRF label distributing mode. The mode can save the label resources. When there are lots of local released VPN routes, the per-VRF label distributing mode can reduce the generating of the ILM entries and improve the performance.

Table 7-13 Configure the VPN route label distributing

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enable the BGP protocol and enter the BGP configuration mode	**router bgp** *autonomous-system*	-
Configure the per-route label distributing mode	**no unque-label-per-vrf**	Optional By default, enable the per-VRF label distributing mode.

7.2.4. Configure VPN Cross-Domain

Configuration Condition

Before configuring the VPN cross-domain, first complete the following tasks:

- Configure the VPN basic functions
- Configure the ASBR direct-connected IP address, making the IP between ASBRs reachable

Configure Option-A Cross-Domain

Option-A cross-domain is also called VRF-to-VRF and it is the simplest mode of realizing the VPN access between AS. VRF-to-VRF takes another ASBR as the CE device to process the VPNv6 connectivity between AS. The following describes one VRF-to-VRF.

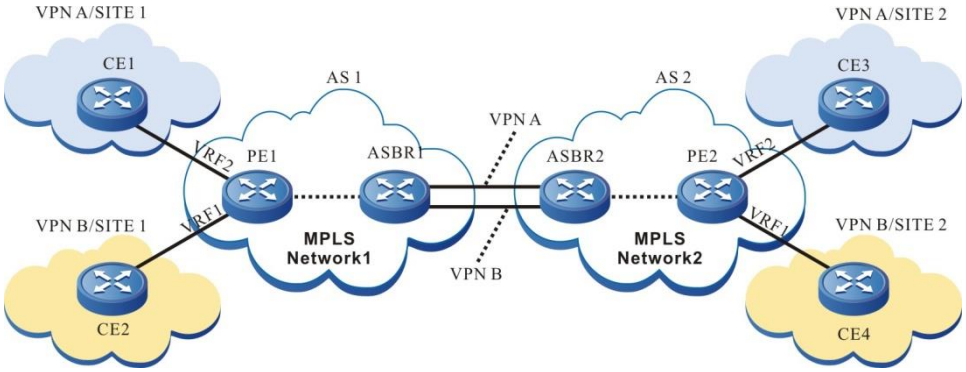

Figure 7-3 Configure Option-A cross-domain (VRF-to-VRF)

In the above figure, VPN site 1 and site 2 are connected to two different service providers respectively: AS1 and AS2. The service providers are connected via ASBR. Two AS areas configure the IPv6 MPLS L3VPN network. The VPN crossing the AS needs the local ASBR to serve as the PE device of the VPN and the peer ASBR to serve as the CE device of the VPN. Meanwhile, on two ASBR devices, configure the VRF of the VPN. In this way, the VPN route transmits the VPNv6 route via MP-IBGP in the AS. ASBR transmits the unicast route in the VRF of the VPN, so as to realize the inter-connection of site 1 and site 2.

The advantage of the VRF-to-VRF mode is that it is necessary to run MPLS between ASBR. The disadvantage is that ASBR needs to maintain all VPN routes and distribute the interface and link for each cross-domain VPN. Therefore, the expansibility is poor.

For the configuration of the VRF-to-VRF cross-domain mode, refer to the part of “Configure VPN Basic Functions”.

Configure Option-B Cross-Domain

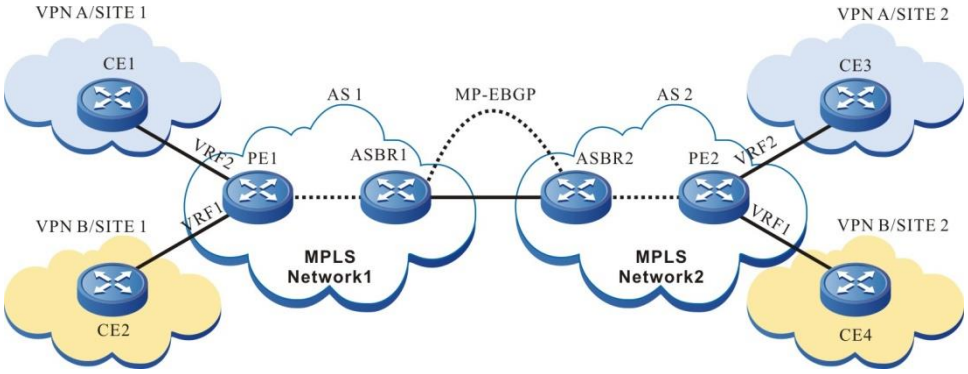

Figure 7-4 Configure Option-B cross-domain (MP-EBGP carries the VPNv6 route)

Option-B cross-domain needs to run MP-EBGP between ASBR. After ASBR learns all VPN routes of the local AS PE, distribute the new label for the VPN route, and then advertise the route information and new label to the peer ASBR. ASBR needs to maintain all VPN routes received from the local PE and the peer ASBR.

Option-B cross-domain does not need ASBR to configure the VRF for each VPN, does not need to import the VPNv6 route, and does not need to distribute the interface for each VPN, but ASBR still needs to maintain all VPNv6 routes, and distribute the new label for each label. Install the

ILM entry of the old and new label translation at the local. Therefore, ASBR has the good load capability.

Table 7-14 Configure Option-B cross-domain

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enable the MPLS forwarding globally	**mpls ip**	Mandatory By default, do not enable the MPLS forwarding.
Enter the interface configuration mode	**interface** *interface_name*	-
Enable the MPLS forwarding on the interface	**mpls ip**	Mandatory Configure on the interconnection interfaces of the two ASBR. By default, do not enable the MPLS forwarding on the interface.
Return to the global configuration mode	**exit**	-
Enable the BGP protocol and enter the BGP configuration mode	**router bgp** *autonomous-system*	-
Configure the peer ASBR as the EBGP neighbor	**neighbor** { *ipv4-address* | *peer-group-name* } **remote-as** *as-number*	Mandatory By default, do not configure any EBGP neighbor.
Enter the BGP VPNv6 configuration mode	**address-family vpnv6** [**unicast**]	Mandatory By default, the system is in the BGP IPv4 unicast configuration mode.

Step	Command	Description
Activate the MP-EBGP neighbor to advertise the VPN route	**neighbor** { *ipv4-address* | *peer-group-name* } **activate**	Mandatory By default, BGP only advertises the IPv4 unicast route.
Configure changing the next hop when advertising the route to the PE	**neighbor** { *ipv4-address* | *peer-group-name* } **next-hop-self**	Mandatory By default, do not configure changing the next hop when advertising the route to the PE.

Note:

- The above just lists the basic configuration of the Option-B cross-domain on ASBR. For the configuration of the ASBR and the PE, P devices in the AS, refer to the part of “Configure VPN Basic Functions”.

7.2.5. Configure VPN User to Access Internet

Configuration Condition

Before configuring the VPN user to access Internet, first complete the following task:

- Configure VPN basic functions

Configure CE to Access Internet

In the actual application environment, the customer does not hope the VPN user to access Internet directly, but requires controlling the connection of the VPN user with Internet via the security devices, such as firewall. Each VPN site sends the Internet data flow to the central site. The VPN member forwards the data flow of the accessed Internet to the central site by importing one default route of accessing Internet (the next hop is the central site CE). The central site forwards the data flow of the accessed Internet to the enterprise firewall. Perform the necessary access control and NAT processing in the firewall according to the made security policy. At last, the firewall forwards the data flow to Internet. The following figure describes one instance of using CE to access Internet.

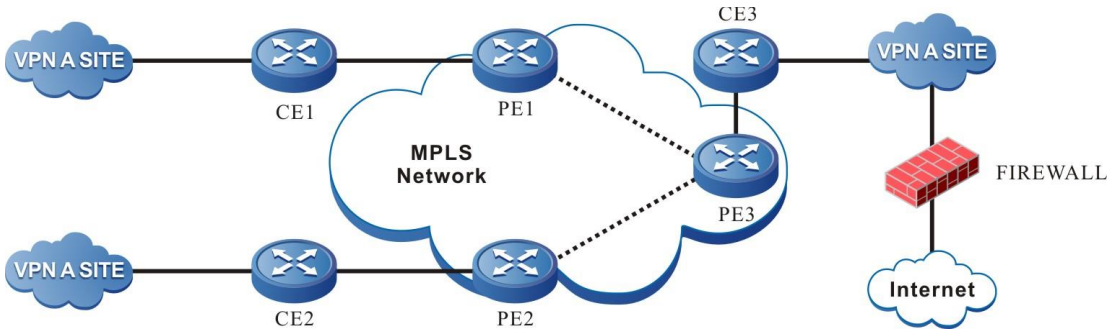

Figure 7-5 Configure CE to access Internet

In the above figure, CE3 serves as the central site of the customer controlling Internet access. You just need to configure the next hop as the default route of Internet gateway on CE3. The route is transmitted to the PE device via the route exchange of PE-CE, and then transmitted to

the VPN site via MP-IBGP. In this way, each VPN site can access Internet via the default route (the next hop is PE3). The data of the accessed Internet first reaches CE3 via MPLS, and then reaches Internet via the configured default route on CE3.

The CE access mode just needs to be configured and deployed in the VPN, but does not need the carrier to take part in. The user can freely control the security policy of the internal user accessing Internet. However, the mode requires the user to have strong security management capability, and the carrier cannot manage the user accessing Internet in a unified manner.

Table 7-15 Configure CE to access Internet

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
On the central site CE, configure the default route and the next hop is Internet gateway	**ipv6 route** [**vrf** *vrf-name1*] *ipv6-prefix/mask-length* { *interface-name* | [*nexthop-ipv6-address* [**vrf** *vrf-name2*]]} [**name** *nexthop-name*] [**tag** *tag-value*] [**track** *track-id*] [*administrative-distance*]	Mandatory By default, CE does not configure the default route of access Internet.

Note:

- For the configuration of the other devices, refer to the part of “Configure VPN Basic Functions”.
- If the PE and CE use the BGP4+ protocol, it is necessary to configure **default-information originate** in the BGP IPv6 unicast configuration mode of the CE3 device to import the default route to the BGP protocol.
- If the PE and CE use the IGP protocol, it is necessary to configure **default-information originate** in the BGP IPv6 VRF configuration mode of the PE3 device to import the default route to the BGP protocol.

7.2.6. Configure AS Coverage

Configuration Condition

Before configuring the AS coverage, first complete the following task:

- Configure the VPN basic functions
- Configure the PE-CE route exchange to use EBGP

Configure AS Coverage

When the PE and CE routers run BGP, the customer VPN may hope to re-use the AS number in different sites. As a result, when CP receives the PE route, the route AS-PATH attribute will contain the AS number of the CE device and the CE will drops the route from the PE. To solve the problem, PE needs to enable the BGP AS cover function. After the PE device enables the AS cover function and advertises the route to the CE neighbor, and if there is the same AS number as CE in the route AS-PATH, PE uses its own AS number to replace the AS number of the CE neighbor contained in the route AS-PATH, and then advertises to the CE neighbor.

Table 7-16 Configure the AS coverage

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enable the BGP protocol and enter the BGP configuration mode	**router bgp** *autonomous-system*	-
Enter the BGP IPv6 VRF configuration mode	**address-family ipv6 vrf** *vrf-name*	Mandatory By default, the system is in the BGP IPv4 unicast configuration mode.
Configure the AS cover function	**neighbor** { *ipv6-address* | *peer-group-name* } **as-override**	By default, do not enable the AS cover function.

7.2.7. Configure OSPFv3 False Link

Configuration Condition

Before configuring the OSPFv3 sham link, first complete the following task:

- Configure the VPN basic functions, configure the route exchange between PE and CE to use OSPFv3

Configure OSPFv3 False Link

In the IPv6 MPLS L3VPN environment, when there is the direct-associated backup link (called backdoor link) between two CE of different sites, the route in the OSPFv3 domain is prior to the external route re-distributed by BGP, and as a result, the traffic between CEs does not pass VPN, but first passes the backdoor link. To make the traffic between two CEs first pass VPN, it is necessary to set up one OSPFv3 sham link between two PEs.

The source address and destination address of the sham link are reachable in the BGP domain, and cannot be covered and re-distributed by OSPFv3. The route to the destination address of the sham link can only be learned by the BGP.

The configuration steps of the OSPFv3 sham link on the PE are as follows:

1. **Configure the VRF loopback interface**

Table 7-17 Configure the VRF loopback interface

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Create one loopback interface and enter the interface configuration mode	**interface loopback** *interface-number*	Mandatory By default, do not create a loopback interface.
Configure the loopback interface to associate VRF	**ip vrf forwarding** *vrf-name*	Mandatory By default, the interface does not associate with any VRF.
Configure the IP address of the loopback interface	**ipv6 address** *ipv6-address/mask-length*	Mandatory By default, do not configure the interface IPv6 address.

2. **Configure BGP to re-distribute OSPFv3 and direct-connected route of the loopback interface**

Table 7-18 Configure BGP to re-distribute OSPFv3 and the direct-connected route of the loopback interface

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enable the BGP protocol and enter the BGP configuration mode	**router bgp** *autonomous-system*	-
Enter the BGP IPv6 VRF configuration mode	**address-family ipv6 vrf** *vrf-name*	Mandatory By default, the system is in the BGP IPv4 unicast configuration mode.

Step	Command	Description
Configure BGP to re-distribute the direct-connected route of the loopback interface	**redistribute connected** [**route-map** *map-name* / **metric** *value*]	Mandatory By default, BGP does not re-distribute the direct-connected route.
Configure BGP to re-distribute OSPFv3	**redistribute ospf** *as-number* [**match** *route-sub-type* / **route-map** *map-name* / **metric** *value*]	Mandatory By default, BGP does not re-distribute the OSPFv3 route.

3. Configure the OSPFv3 sham link

Table 7-19 Configure the OSPFv3 sham link

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Create one OSPFv3 process and enter the OSPFv3 configuration mode	**ipv6 router ospf** *process-id* [**vrf** *vrf-name*]	Mandatory Enable or enable the OSPFv3 process in the VRF. By default, the system does not enable the OSPFv3 protocol. When enabling OSPFv3 in the VRF, the OSPFv3 process belonging to one VRF can only manage the interfaces belonging to the VRF.
Configure OSPFv3 router-id	**router-id** *router-id*	Mandatory By default, OSPFv3 is not configured with router-id.
Configure the OSPFv3 sham link	**area** *area-id* **sham-link** *source-ipv6-address desinationt-ipv6-address* [**cost** *cost*] [**ttl-security hops** *hops*]	Mandatory *source-ipv6-address* is the address of the local loopback interface. *desinationt-ipv6-address* is the peer loopback port address. By default, do not configure the OSPFv3 sham link.

7.2.8. Configure VPN ORF

Configuration Condition

Before configuring the VPN ORF function, first complete the following tasks:

- Enable the BGP protocol
- Configure the neighbor of the BGP VPN address family and set up the session successfully

Configure VPN ORF

In the VPN environment of BGP, the route transmitter RR will send all VPN routes to the peer PE or the peer RR. After receiving VPN routes, the peer PE or RR will filter out the unnecessary VPN routes according to the local configured IMPORT RT. In the larger VPN network, a large number of unnecessary VPN route information will be advertised and filtered in the network, causing a great waste of resources. Especially, the performance of some edge PE devices is low. When receiving a large number of VPN routes, the performance cannot be satisfied, which affects the normal VPN services.

The VPN ORF function is to solve the problem. The basic principle of VPN ORF is that the BGP router participating in VPN route distribution advertises its IMPORT RT using MP-BGP, uses the best route selection algorithm of standard BGP-4 to get the route distribution map of IMPORT, and takes the IMPORT information as ORF to perform the egress filtering for the VPN route. In this way, for the unnecessary VPN route, perform the restriction advertising at the VPN route source. In the practical network planning, RR usually plays the role, and the RR router generally has high performance.

Table 7-20 Configure the VPN ORF function

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the BGP configuration mode	**router bgp** *autonomous-system*	-
Enter the VPN-Target address family	**address-family ipv4 vpn-target**	-
Activate the neighbor in the VPN-Target address family; as for the IPv4 peer, activate the VPN-Target address family of the peer, and exchange the VPN RT information	**neighbor {** *neighbor-address* **|** *peer-group-name***} active**	-
In the VPN-Target address family, add one neighbor to the peer group	**neighbor** { *neighbor-address* } **peer-group** { *group-name* }	Optional

Step	Command	Description
In the PN-Target address family mode, enable the route reflection function	**neighbor {** *neighbor-address* **|** *peer-group-name* **} route-reflector-client**	Optional
In the VPN-Target address family mode, enable advertising the default route of RT NLRI	**neighbor** { *neighbor-address* **|** *peer-group-name* } **default-originate**	Optional

Caution:

- Activating the neighbor in the VPN-Target address family only supports the IPv4 neighbor, but you can perform the egress filtering for the VPNv4 or VPNv6 route at the same time.
- Activate the neighbor in the VPN-Target address family, and usually, the neighbor is also activated in the VPNv4 address family or VPNv6 address family.

7.2.9. IPv6 MPLS L3VPN Monitoring and Maintaining

Table 7-21 IPv6 MPLS L3VPN monitoring and maintaining

Command	Description
clear bgp { *****	*neighbor-address*	*as-number*	**peer-group** *peer-group-name*	**external** } **vpnv6 unicast**	Reset the VPNv6 neighbor
clear bgp { *****	*neighbor-address*	*as-number*	**peer-group** *peer-group-name*	**external** } **vpnv6 unicast** [**soft** [**in**	**out**]	**in prefix-filter**]	Soft-reset the BGP VPNv6 neighbor
show bgp ipv6 vrf *vrf-name* [	{ **begin** *line-string*	**exclude** *line-string*	**include** *line-string*	**redirect** { **file** *file-name*	**ftp** [**vrf** *vrf-name*] *server-ip user-name user-password file-name*	**ftps {[vrf** *vrf-name* **]** *host-name user-name user-password file-name* **VerifyType** [**none**	**peer**]}} }]	Display the BGP IPv6 VRF information
show bgp vpnv6 unicast { **all**	**vrf** *vrf-name*	**rd** *route-distinguisher* } [*ipv6-address*	*ipv6-address/mask-length*] [	{ **begin** *line-string*	**exclude** *line-string*	**include** *line-string*	**redirect** {**file** *file-name*	**ftp** [**vrf** *vrf-name*] *server-ip user-name user-password file-name*	**ftps {[vrf** *vrf-name* **]** *host-name user-name user-password file-name* **VerifyType** [**none**	**peer**]}} }]	Display the route database information in the BGP VPNv6 address family

Command	Description
show bgp vpnv6 unicast { **all** | **vrf** *vrf-name* } **dampening** { **dampened-paths** | **flap-statistics** | **parameters** } [| { **begin** *line-string* | **exclude** *line-string* | **include** *line-string* | **redirect** { **file** *file-name* | **ftp** [**vrf** *vrf-name*] *server-ip user-name user-password file-name* | **ftps {[vrf** *vrf-name* **]** *host-name user-name user-password file-name* **VerifyType** [**none** | **peer**]}} }]	Display the details of the BGP VPNv6 route dampening
show bgp vpnv6 unicast { **all** | **vrf** *vrf-name* | **rd** *route-distinguisher* } **labels**	Display the route label information in the BGP VPNv6 address family
show bgp vpnv6 unicast {**all | vrf** *vrf-name* | **rd** *route-distinguisher* } **neighbors** [*neighbor-address*] [| { **begin** *line-string* | **exclude** *line-string* | **include** *line-string* | **redirect** { **file** *file-name* | **ftp** [**vrf** *vrf-name*] *server-ip user-name user-password file-name* | **ftps {[vrf** *vrf-name* **]** *host-name user-name user-password file-name* **VerifyType** [**none** | **peer**]}} }]	Display the neighbor details in the BGP VPNv6 address family
show bgp vpnv6 unicast { **all** | **vrf** *vrf-name* | **rd** *route-distinguisher* } **summary**	Display all neighbor information in the BGP VPNv6 address family
show ipv6 route vrf *vrf-name* [*ipv6-address* | *ipv6-prefix* | **bgp** | **brief** | **connected** | **isis** | **linklocal** | **local** | **ospf** | **rip** | **static | statistic**] [| { **begin** *line-string* | **exclude** *line-string* | **include** *line-string* | **redirect** { **file** *file-name* | **ftp** [**vrf** *vrf-name*] *server-ip user-name user-password file-name* | **ftps {[vrf** *vrf-name* **]** *host-name user-name user-password file-name* **VerifyType** [**none** | **peer**]}} }]	Display the VRF information
show mpls forwarding-table [**detail**]	Display the MPLS forwarding information
show mpls forwarding-table ilm [**detail**]	Display the MPLS ILM forwarding information
show vrf [**brief** | **ipv6** | **vrf-name** *vrf-name* [**brief** | **ipv6**]]	Display the VRF information

7.3. IPv6 MPLS L3VPN Typical Configuration Example

7.3.1. Configure IPv6 MPLS L3VPN Basic Functions (Over IPv4 LSP)

Network Requirements

- Deploy IPv4 LDP in the backbone network.
- The whole MPLS network includes two VPNs, VPN1 and VPN2. The two VPNs uses different Route-Target, so as to ensure that two VPNs cannot communicate with each other.
- CE1 and CE3 belong to VPN1; CE2 and CE4 belong to VPN2.
- CE and PE adopt IPv6 BGP to exchange the route information.
- PEs adopt OSPF as IGP, IPv4 MPLS LDP assigns the label to make PEs communicate with each other. Configure MP-IBGP to exchange the VPNv6 route information.

Network Topology

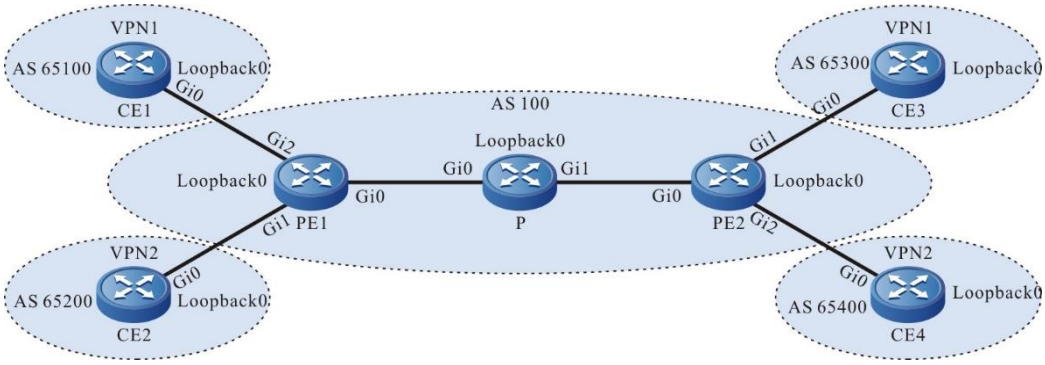

Figure 7-6Networking of configuring IPv6 MPLS L3VPN basic functions

Device	Interface	IP Address	Device	Interface	IP Address
CE1	Gi0	2001:1::2/64	P	Loopback0	3.3.3.3/32
	Loopback0	1::1/128	CE3	Gi0	2001:3::2/64
PE1	Gi0	10.0.0.1/24		Loopback0	3::3/128
	Gi1	2001:2::1/64	PE2	Gi0	20.0.0.1/24
	Gi2	2001:1::1/64		Gi1	2001:3::1/64
	Loopback0	1.1.1.1/32		Gi2	2001:4::1/64
CE2	Gi0	2001:2::2/64		Loopback0	2.2.2.2/32
	Loopback0	2::2/128	CE4	Gi0	2001:4::2/64

Device	Interface	IP Address	Device	Interface	IP Address
P	Gi0	10.0.0.2/24	CE4	Loopback0	4::4/128
	Gi1	20.0.0.2/24			

Configuration Steps

Step 1: Configure the IP address of the interface (omitted).

Step 2: Configure the global OSPF and advertise the global route.

#Configure the global OSPF on PE1.

```
PE1#configure terminal
PE1(config)#router ospf 100
PE1(config-ospf)#network 1.1.1.1 0.0.0.0 area 0
PE1(config-ospf)#network 10.0.0.0 0.0.0.255 area 0
PE1(config-ospf)#exit
```

#Configure the global OSPF on P.

```
P#configure terminal
P(config)#router ospf 100
P(config-ospf)#network 3.3.3.3 0.0.0.0 area 0
P(config-ospf)#network 10.0.0.0 0.0.0.255 area 0
P(config-ospf)#network 20.0.0.0 0.0.0.255 area 0
P(config-ospf)#exit
```

#Configure the global OSPF on PE2.

```
PE2#configure terminal
PE2(config)#router ospf 100
PE2(config-ospf)#network 2.2.2.2 0.0.0.0 area 0
PE2(config-ospf)#network 20.0.0.0 0.0.0.255 area 0
PE2(config-ospf)#exit
```

#After the configuration is complete, view the global route table on the device.

Take PE1 as an example:

```
PE1#show ip route
Codes: C - Connected, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external
```

```
C   10.0.0.0/24 is directly connected, 00:39:30, gigabitethernet0
O   20.0.0.0/24 [110/2] via 10.0.0.2, 00:11:15, gigabitethernet0
C   127.0.0.0/8 is directly connected, 1w2d:07:04:57, lo0
C   1.1.1.1/32 is directly connected, 00:39:09, loopback0
O   2.2.2.2/32 [110/3] via 10.0.0.2, 00:00:03, gigabitethernet0
O   3.3.3.3/32 [110/2] via 10.0.0.2, 00:00:44, gigabitethernet0
```

You can see that there is the route information of P and PE2 loopback ports in the global route table of PE1.

Note:

- For the checking method of P and PE2, refer to PE1.

Step 3: Enable MPLS IP and MPLS LDP.

#On PE1, enable the global MPLS IP and MPLS LDP. Meanwhile, enable MPLS IP and MPLS LDP on the interface.

```
PE1(config)#mpls ip
PE1(config)#mpls ldp
PE1(config-ldp)#router-id 1.1.1.1
PE1(config-ldp)#address-family ipv4
PE1(config-ldp-af4)#transport-address 1.1.1.1
PE1(config-ldp-af4)#exit
PE1(config-ldp)#exit
PE1(config)#interface gigabitethernet0
PE1(config-if-gigabitethernet0)#mpls ip
PE1(config-if-gigabitethernet0)#mpls ldp
PE1(config-if-gigabitethernet0)#exit
```

#On P, enable the global MPLS IP and MPLS LDP. Meanwhile, enable MPLS IP and MPLS LDP on the interface.

```
P(config)#mpls ip
P(config)#mpls ldp
P(config-ldp)#router-id 3.3.3.3
P(config-ldp)#address-family ipv4
P(config-ldp-af4)#transport-address 3.3.3.3
P(config-ldp-af4)#exit
P(config-ldp)#exit
P(config)#interface gigabitethernet0
P(config-if-gigabitethernet0)#mpls ip
P(config-if-gigabitethernet0)#mpls ldp
```

```
P(config-if-gigabitethernet0)#exit
P(config)#interface gigabitethernet1
P(config-if-gigabitethernet1)#mpls ip
P(config-if-gigabitethernet1)#mpls ldp
P(config-if-gigabitethernet1)#exit
```

#On PE2, enable the global MPLS IP and MPLS LDP. Meanwhile, enable MPLS IP and MPLS LDP on the interface.

```
PE2(config)#mpls ip
PE2(config)#mpls ldp
PE2(config-ldp)#router-id 2.2.2.2
PE2(config-ldp)#address-family ipv4
PE2(config-ldp-af4)#transport-address 2.2.2.2
PE2(config-ldp-af4)#exit
PE2(config-ldp)#exit
PE2(config)#interface gigabitethernet0
PE2(config-if-gigabitethernet0)#mpls ip
PE2(config-if-gigabitethernet0)#mpls ldp
PE2(config-if-gigabitethernet0)#exit
```

Note:

- router-id and transport-address can be configured manually and also can be generated automatically. Usually, they are configured the same. If not configuring router-id and transport-address manually, the device will select automatically. From the up interfaces, first select the Loopback interface with the maximum IP address. If the device does not configure the Loopback interface address, select the common interface with the maximum IP address.

#After the configuration is complete, view the LDP session information on the device.

Take the PE1 as an example:

```
PE1#show mpls ldp session
Peer IP Address   Peer Type    My Role   State        DS Cap   DeadTime
3.3.3.3           Multicast    Passive   OPERATIONAL  Disabled 00:02:20
Statistics for ldp sessions:
    Multicast sessions: 1
    Targeted sessions: 0
```

You can see that PE1 and P set up the LDP session successfully.

#View the route label information on the device.

Take the PE1 as an example:

```
PE1#show ip route 2.2.2.2 detail
Codes: C - Connected, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
    U - Per-user Static route
```

```
        O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external

O   2.2.2.2/32 [110/2] via 10.0.0.2, label 24016, 00:45:23, gigabitethernet0
                       10.0.0.2 [0], gigabitethernet0

PE1#show ip route 3.3.3.3 detail
Codes: C - Connected, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
    U - Per-user Static route
    O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external

O   3.3.3.3/32 [110/2] via 10.0.0.2, label 3, 00:45:23, gigabitethernet0
                       10.0.0.2 [0], gigabitethernet0
```

You can see that there is the route label information of P and PE2 loopback ports on PE1.

Note:

- For the checking method of P and PE2, refer to PE1.

Step 4: Configure the VPN instance and advertise the CE route to PE via IPv6 BGP.

#On PE1, configure the VPN instance and the IPv6 BGP in VPN1 and VPN2.

```
PE1(config)#ip vrf 1
PE1(config-vrf)#rd 100:1
PE1(config-vrf)#route-target 100:1
PE1(config-vrf)#exit
PE1(config)#ip vrf 2
PE1(config-vrf)#rd 200:1
PE1(config-vrf)#route-target 200:1
PE1(config-vrf)#exit
PE1(config)#interface gigabitethernet2
PE1(config-if-gigabitethernet2)#ip vrf forwarding 1
PE1(config-if-gigabitethernet2)#ipv6 address 2001:1::1/64
PE1(config-if-gigabitethernet2)#exit
PE1(config)#interface gigabitethernet1
PE1(config-if-gigabitethernet1)#ip vrf forwarding 2
```

```
PE1(config-if-gigabitethernet1)#ipv6 address 2001:2::1/64
PE1(config-if-gigabitethernet1)#exit
PE1(config)#router bgp 100
PE1(config-bgp)#address-family ipv6 vrf 1
PE1(config-bgp-af)#neighbor 2001:1::2 remote-as 65100
PE1(config-bgp-af)#exit-address-family
PE1(config-bgp)#address-family ipv6 vrf 2
PE1(config-bgp-af)#neighbor 2001:2::2 remote-as 65200
PE1(config-bgp-af)#exit-address-family
PE1(config-bgp)#exit
```

#Configure IPv6 BGP on CE1.

```
CE1#configure terminal
CE1(config)#router bgp 65100
CE1(config-bgp)#bgp router-id 11.11.11.11
CE1(config-bgp)#address-family ipv6
CE1(config-bgp-af)#neighbor 2001:1::1 remote-as 100
CE1(config-bgp-af)#network 1::1/128
CE1(config-bgp-af)#exit-address-family
CE1(config-bgp)#exit
```

#Configure IPv6 BGP on CE2.

```
CE2#configure terminal
CE2(config)#router bgp 65200
CE2(config-bgp)#bgp router-id 22.22.22.22
CE2(config-bgp)#address-family ipv6
CE2(config-bgp-af)#neighbor 2001:2::1 remote-as 100
CE2(config-bgp-af)#network 2::2/128
CE2(config-bgp-af)#exit-address-family
CE2(config-bgp)#exit
```

#Configure the VPN instance on PE2 and configure the IPv6 BGP in VPN1 and VPN2.

```
PE2(config)#ip vrf 1
PE2(config-vrf)#rd 100:1
PE2(config-vrf)#route-target 100:1
PE2(config-vrf)#exit
PE2(config)#ip vrf 2
PE2(config-vrf)#rd 200:1
PE2(config-vrf)#route-target 200:1
PE2(config-vrf)#exit
```

```
PE2(config)#interface gigabitethernet1
PE2(config-if-gigabitethernet1)#ip vrf forwarding 1
PE2(config-if-gigabitethernet1)#ipv6 address 2001:3::1/64
PE2(config-if-gigabitethernet1)#exit
PE2(config)#interface gigabitethernet2
PE2(config-if-gigabitethernet2)#ip vrf forwarding 2
PE2(config-if-gigabitethernet2)#ipv6 address 2001:4::1/64
PE2(config-if-gigabitethernet2)#exit
PE2(config)#router bgp 100
PE2(config-bgp)#address-family ipv6 vrf 1
PE2(config-bgp-af)#neighbor 2001:3::2 remote-as 65300
PE2(config-bgp-af)#exit-address-family
PE2(config-bgp)#address-family ipv6 vrf 2
PE2(config-bgp-af)#neighbor 2001:4::2 remote-as 65400
PE2(config-bgp-af)#exit-address-family
PE2(config-bgp)#exit
```

#Configure IPv6 BGP on CE3.

```
CE3#configure terminal
CE3(config)#router bgp 65300
CE3(config-bgp)#bgp router-id 33.33.33.33
CE3(config-bgp)#address-family ipv6
CE3(config-bgp-af)#neighbor 2001:3::1 remote-as 100
CE3(config-bgp-af)#network 3::3/128
CE3(config-bgp-af)#exit-address-family
CE3(config-bgp)#exit
```

#Configure IPv6 BGP on CE4.

```
CE4#configure terminal
CE4(config)#router bgp 65400
CE4(config-bgp)#bgp router-id 44.44.44.44
CE4(config-bgp)#address-family ipv6
CE4(config-bgp-af)#neighbor 2001:4::1 remote-as 100
CE4(config-bgp-af)#network 4::4/128
CE4(config-bgp-af)#exit-address-family
CE4(config-bgp)#exit
```

#After the configuration is complete, view the IPv6 BGP neighbor information on the PE.

Take PE1 as an example:

```
PE1#show bgp vpnv6 unicast all summary
```

```
BGP router identifier 1.1.1.1, local AS number 100
BGP VRF 1 Route Distinguisher:
100:1
BGP table version is 1
5 BGP AS-PATH entries
0 BGP community entries

Neighbor        V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
2001:1::2       4 65100      27      27        1    0    0 00:21:15        1

Total number of neighbors 1
BGP VRF 2 Route Distinguisher:
200:1
BGP table version is 1
5 BGP AS-PATH entries
0 BGP community entries

Neighbor        V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
2001:2::2       4 65200      26      26        1    0    0 00:20:42        1

Total number of neighbors 1
```

The content of the State/PfxRcd list is displayed as number (the number of the route prefixes received from the neighbor), and you can see that PE1 and CE1, CE2 set up the IPv6 BGP neighbor successfully.

#View the BGP VPNv6 route table and VPN route table on the PE.

Take PE1 as an example:

```
PE1#show bgp vpnv6 unicast vrf 1
BGP table version is 2, local router ID is 1.1.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network          Next Hop            Metric     LocPrf Weight Path
Route Distinguisher: 100:1 (Default for VRF 1)
[B]*> 1::1/128          2001:1::2                0             0 65100 i

PE1#show bgp vpnv6 unicast vrf 2
BGP table version is 2, local router ID is 1.1.1.1
```

```
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network          Next Hop          Metric     LocPrf Weight Path
Route Distinguisher: 200:1 (Default for VRF 2)
[B]*> 2::2/128          2001:2::2              0              0 65200 i

PE1#show ipv6 route vrf 1
Codes: C - Connected, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management



B   1::1/128 [20/0]
    via 2001:1::2, 00:09:07, gigabitethernet2
C   2001:1::/64 [0/0]
    via ::, 00:16:43, gigabitethernet2
L   2001:1::1/128 [0/0]
    via ::, 00:16:43, gigabitethernet2

PE1#show ipv6 route vrf 2
Codes: C - Connected, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management



B   2::2/128 [20/0]
    via 2001:2::2, 00:04:24, gigabitethernet1
C   2001:2::/64 [0/0]
    via ::, 17:00:48, gigabitethernet1
L   2001:2::1/128 [0/0]
    via ::, 17:00:48, gigabitethernet1
```

You can see that there is the routes to CE1 and CE2 in the VPN1 and VPN2 route tables of PE1.

Note:

- For the checking method of PE2, refer to PE1.

Step 5: Configure MP-IBGP, and use the loopback interface as the peer address.

#On PE1, configure MP-IBGP, enable the VPNv6 address family.

```
PE1(config)#router bgp 100
PE1(config-bgp)#neighbor 2.2.2.2 remote-as 100
PE1(config-bgp)#neighbor 2.2.2.2 update-source loopback 0
PE1(config-bgp)#address-family vpnv6
PE1(config-bgp-af)#neighbor 2.2.2.2 activate
PE1(config-bgp-af)#exit-address-family
PE1(config-bgp)#exit
```

#On PE2, configure MP-IBGP, enable the VPNv6 address family.

```
PE2(config)#router bgp 100
PE2(config-bgp)#neighbor 1.1.1.1 remote-as 100
PE2(config-bgp)#neighbor 1.1.1.1 update-source loopback 0
PE2(config-bgp)#address-family vpnv6
PE2(config-bgp-af)#neighbor 1.1.1.1 activate
PE2(config-bgp-af)#exit-address-family
PE2(config-bgp)#exit
```

Step 6: Check the result.

#After the configuration is complete, view the BGP neighbor information on the PE.

Take PE1 as an example:

```
PE1#show bgp vpnv6 unicast all summary
BGP router identifier 1.1.1.1, local AS number 100
BGP table version is 2
5 BGP AS-PATH entries
0 BGP community entries

Neighbor        V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
2.2.2.2         4   100       6       5        2    0    0 00:02:23        2

Total number of neighbors 1
BGP VRF 1 Route Distinguisher:
100:1
BGP table version is 1
5 BGP AS-PATH entries
0 BGP community entries
```

```
Neighbor        V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
2001:1::2       4 65100      27      27        1    0    0 00:21:15        1

Total number of neighbors 1
BGP VRF 2 Route Distinguisher:
200:1
BGP table version is 1
5 BGP AS-PATH entries
0 BGP community entries

Neighbor        V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
2001:2::2       4 65200      26      26        1    0    0 00:20:42        1

Total number of neighbors 1
```

The content of the State/PfxRcd list is displayed as number (the number of the route prefixes received from the neighbor), and you can see that PE1 and PE2 set up the BGP neighbor successfully.

#View the BGP VPNv6 route table and VPN route table on the PE.

Take PE1 as an example:

```
PE1#show bgp vpnv6 unicast vrf 1
BGP table version is 2, local router ID is 1.1.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network          Next Hop            Metric     LocPrf Weight Path
Route Distinguisher: 100:1 (Default for VRF 1)
[B]*> 1::1/128           2001:1::2                0             0 65100 i
[B]*>i3::3/128           ::ffff:2.2.2.2           0       100   0 65300 i

PE1#show bgp vpnv6 unicast vrf 2
BGP table version is 2, local router ID is 1.1.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network          Next Hop            Metric     LocPrf Weight Path
Route Distinguisher: 200:1 (Default for VRF 2)
[B]*> 2::2/128           2001:2::2                0             0 65200 i
[B]*>i4::4/128           ::ffff:2.2.2.2           0       100   0 65400 i
```

You can see that there is the route information to the peer CE3 and CE4 in the BGP VPNv6 route table of PE1.

```
PE1#show ipv6 route vrf 1
Codes: C - Connected, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management



B   1::1/128 [20/0]
      via 2001:1::2, 00:24:14, gigabitethernet2
B   3::3/128 [200/0]
      via ::ffff:2.2.2.2, 00:05:02, gigabitethernet0
C   2001:1::/64 [0/0]
      via ::, 00:31:49, gigabitethernet2
L   2001:1::1/128 [0/0]
      via ::, 00:31:49, gigabitethernet2

PE1#show ipv6 route vrf 1 3::3/128
Codes: C - Connected, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management



B   3::3/128 [200/0]
      via ::ffff:2.2.2.2 [0], label 25120, 00:05:10, gigabitethernet0
          ::ffff:10.0.0.2 [3], label 24016, gigabitethernet0
```

You can see that there is the route information to the peer CE3 in the VPN1 route table of PE1, the VPN label of the route is 25120, and the global label is 24016.

```
PE1#show ipv6 route vrf 2
Codes: C - Connected, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management



B   2::2/128 [20/0]
```

```
    via 2001:2::2, 00:19:31, gigabitethernet1
B   4::4/128 [200/0]
    via ::ffff:2.2.2.2, 00:05:04, gigabitethernet0
C   2001:2::/64 [0/0]
    via ::, 17:15:55, gigabitethernet1
L   2001:2::1/128 [0/0]
    via ::, 17:15:55, gigabitethernet1
```

```
PE1#show ipv6 route vrf 2 4::4/128
Codes: C - Connected, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management
```

```
B   4::4/128 [200/0]
    via ::ffff:2.2.2.2 [0], label 25121, 00:05:20, gigabitethernet0
        ::ffff:10.0.0.2 [3], label 24016, gigabitethernet0
```

You can see that there is the route information to the peer CE4 in the VPN2 route table of PE1, the VPN label of the route is 25121, and the global label is 24016.

#View the MPLS forwarding table on the PE.

Take PE1 as an example:

PE1#show mpls forwarding-table

```
Pro: L - LDP, O - OSPF, B - MP-BGP, R - RSVP, M - Mapped-Route, S - Static
Label,ML - mLDP (ML FEC: Root address/OT/OV), RM - RSVP P2MP (RM FEC: P2MP
ID/TID)
```

Pro	Ident	FEC	Inlabel	Outlabel	Outgoing	Next hop
B	1	::/0	25120	/	/	::
B	2	::/0	25121	/	/	::

You can see that there is the route label information of VPN1 and VPN2 in the MPLS forwarding table of PE1.

Note:

- For the checking method of PE2, refer to PE1.

#Ping the loopback port of CE3 at CE1 and view whether the ping can be connected.

```
CE1#ping ipv6 3::3 -s 1::1

Press key (ctrl + shift + 6) interrupt it.
```

```
Reply from  3::3: bytes = 76  time < 16 ms
Reply from  3::3: bytes = 76  time < 16 ms
Reply from  3::3: bytes = 76  time < 16 ms
Reply from  3::3: bytes = 76  time < 16 ms
Reply from  3::3: bytes = 76  time < 16 ms
Success rate is 100% (5/5). Round-trip min/avg/max = 0/0/0 ms.
```

#Ping the loopback port of CE4 at CE1 and view whether the ping can be connected.

```
CE1#ping ipv6 4::4 -s 1::1


Press key (ctrl + shift + 6) interrupt it.
Send a packet to 4::4, request timed out.
Send a packet to 4::4, request timed out.
Send a packet to 4::4, request timed out.
Send a packet to 4::4, request timed out.
Send a packet to 4::4, request timed out.
Success rate is 0% (0/5).
```

You can see that the devices in one VPN can communicate normally, the devices of different VPNs cannot communicate, and the routes are separated.

7.3.2. Configure IPv6 MPLS L3VPN Basic Functions (Over IPv6 LSP)

Network Requirements

- Deploy IPv6 LDP in the backbone network.
- The whole MPLS network includes two VPNs, VPN1 and VPN2. The two VPNs uses different Route-Target, so as to ensure that two VPNs cannot communicate with each other.
- CE1 and CE3 belong to VPN1; CE2 and CE4 belong to VPN2.
- CE and PE adopt IPv6 BGP to exchange the route information.
- PEs adopt OSPFv3 as IGP, IPv6 MPLS LDP assigns the label to make PEs communicate with each other. Configure MP-IBGP to exchange the VPNv6 route information.

Network Topology

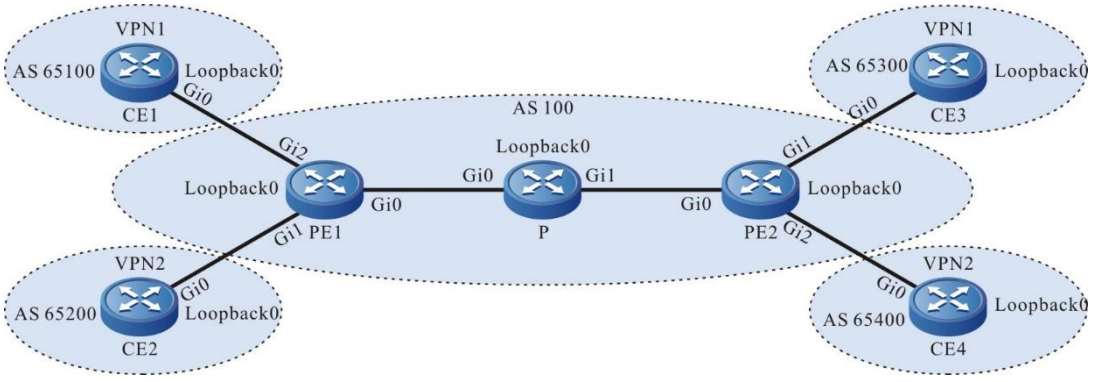

Figure 7-7 Networking of configuring IPv6 MPLS L3VPN basic functions

Device	Interface	IP Address	Device	Interface	IP Address
CE1	Gi0	2001:1::2/64	P	Loopback0	22::1/128
	Loopback0	1::1/128	CE3	Gi0	2001:5::2/64
PE1	Gi0	2001:3::1/64		Loopback0	3::3/128
	Gi1	2001:2::1/64	PE2	Gi0	2001:4::2/64
	Gi2	2001:1::1/64		Gi1	2001:5::1/64
	Loopback0	11::1/128		Gi2	2001:6::1/64
CE2	Gi0	2001:2::2/64		Loopback0	33::1/128
	Loopback0	2::2/128	CE4	Gi0	2001:6::2/64
P	Gi0	2001:3::2/64	CE4	Loopback0	4::4/128
	Gi1	2001:4::1/64			

Configuration Steps

Step 1: Configure the IP address of the interface (omitted).

Step 2: Configure the global OSPFv3 and advertise the global route.

#Configure the global OSPFv3 on PE1.

```
PE1#configure terminal
PE1(config)#ipv6 router ospf 100
PE1(config-ospf6)#router-id 1.1.1.1
PE1(config-ospf6)#exit
PE1(config)#interface loopback 0
PE1(config-if-loopback0)#ipv6 router ospf 100 area 0
PE1(config-if-loopback0)#exit
PE1(config)#interface gigabitethernet 0
PE1(config-if-gigabitethernet0)#ipv6 router ospf 100 area 0
PE1(config-if-gigabitethernet0)#exit
```

#Configure the global OSPFv3 on P.

```
P#configure terminal
P(config)#ipv6 router ospf 100
P(config-ospf6)#router-id 2.2.2.2
P(config-ospf6)#exit
P(config)#interface loopback 0
P(config-if-loopback0)#ipv6 router ospf 100 area 0
P(config-if-loopback0)#exit
P(config)#interface gigabitethernet 0
P(config-if-gigabitethernet0)#ipv6 router ospf 100 area 0
P(config-if-gigabitethernet0)#exit
P(config)#interface gigabitethernet 1
P(config-if-gigabitethernet1)#ipv6 router ospf 100 area 0
P(config-if-gigabitethernet1)#exit
```

#Configure the global OSPFv3 on PE2.

```
PE2#configure terminal
PE2(config)#ipv6 router ospf 100
PE2(config-ospf6)#router-id 3.3.3.3
PE2(config-ospf6)#exit
PE2(config)#interface loopback 0
PE2(config-if-loopback0)#ipv6 router ospf 100 area 0
PE2(config-if-loopback0)#exit
PE2(config)#interface gigabitethernet 0
PE2(config-if-gigabitethernet0)#ipv6 router ospf 100 area 0
PE2(config-if-gigabitethernet0)#exit
```

#After the configuration is complete, view the global route table on the device.

Take PE1 as an example:

```
PE1#show ipv6 route
Codes: C - Connected, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management



L   ::1/128 [0/0]
     via ::, 3d:00:05:42, lo0
LC  11::1/128 [0/0]
```

```
       via ::, 3d:00:04:55, loopback0
O   22::1/128 [110/1]
       via fe80::201:7aff:fe94:9a32, 3d:00:00:56, gigabitethernet0
O   33::1/128 [110/2]
       via fe80::201:7aff:fe94:9a32, 3d:00:01:56, gigabitethernet0
C   2001:3::/64 [0/0]
       via ::, 3d:00:01:51, gigabitethernet0
L   2001:3::1/128 [0/0]
       via ::, 3d:00:01:51, gigabitethernet0
O   2001:4::/64 [110/1]
       via fe80::201:7aff:fe94:9a32, 3d:00:02:00, gigabitethernet0
```

You can see that there is the route information of P and PE2 loopback ports in the global route table of PE1.

Note:

- For the checking method of P and PE2, refer to PE1..

Step 3: Enable MPLS IP and IPv6 MPLS LDP.

#On PE1, enable the global MPLS IP and IPv6 MPLS LDP. Meanwhile, enable MPLS IP and IPv6 MPLS LDP on the interface.

```
PE1(config)#mpls ip
PE1(config)#mpls ldp
PE1(config-ldp)#router-id 1.1.1.1
PE1(config-ldp)#address-family ipv6
PE1(config-ldp-af6)#transport-address 11::1
PE1(config-ldp-af6)#exit
PE1(config-ldp)#exit
PE1(config)#interface gigabitethernet0
PE1(config-if-gigabitethernet0)#mpls ip
PE1(config-if-gigabitethernet0)#mpls ldp ipv6
PE1(config-if-gigabitethernet0)#exit
```

#On P, enable the global MPLS IP and IPv6 MPLS LDP. Meanwhile, enable MPLS IP and IPv6 MPLS LDP on the interface.

```
P(config)#mpls ip
P(config)#mpls ldp
P(config-ldp)#router-id 2.2.2.2
P(config-ldp)#address-family ipv6
P(config-ldp-af6)#transport-address 22::1
P(config-ldp-af6)#exit
```

```
P(config-ldp)#exit
P(config)#interface gigabitethernet0
P(config-if-gigabitethernet0)#mpls ip
P(config-if-gigabitethernet0)#mpls ldp ipv6
P(config-if-gigabitethernet0)#exit
P(config)#interface gigabitethernet1
P(config-if-gigabitethernet1)#mpls ip
P(config-if-gigabitethernet1)#mpls ldp ipv6
P(config-if-gigabitethernet1)#exit
```

#On PE2, enable the global MPLS IP and IPv6 MPLS LDP. Meanwhile, enable MPLS IP and IPv6 MPLS LDP on the interface.

```
PE2(config)#mpls ip
PE2(config)#mpls ldp
PE2(config-ldp)#router-id 3.3.3.3
PE2(config-ldp)#address-family ipv6
PE2(config-ldp-af6)#transport-address 33::1
PE2(config-ldp-af6)#exit
PE2(config-ldp)#exit
PE2(config)#interface gigabitethernet0
PE2(config-if-gigabitethernet0)#mpls ip
PE2(config-if-gigabitethernet0)#mpls ldp ipv6
PE2(config-if-gigabitethernet0)#exit
```

#After the configuration is complete, view the LDP session information on the device.

Take PE1 as an example:

```
PE1#show mpls ldp ipv6 session
Peer IPv6 Address                Peer Type     My Role   State        DS Cap
DeadTime
22::1                            Multicast     Passive   OPERATIONAL  Disabled
00:02:54
Statistics for ldp ipv6 sessions:
    Multicast sessions: 1
    Targeted sessions: 0
```

You can see that PE1 and P set up the LDP session successfully.

#View the route label information on the device.

Take PE1 as an example:

```
PE1#show ipv6 route 22::1
Codes: C - Connected, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
    U - Per-user Static route
```

```
        O - OSPF, OE-OSPF External, M - Management


    O   22::1/128 [110/1]
        via fe80::201:7aff:fe94:9a32 [1], label 3, 3d:00:02:50, gigabitethernet0
          fe80::201:7aff:fe94:9a32 [0], gigabitethernet0

    PE1#show ipv6 route 33::1
    Codes: C - Connected, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
        U - Per-user Static route
        O - OSPF, OE-OSPF External, M - Management


    O   33::1/128 [110/2]
        via fe80::201:7aff:fe94:9a32 [1], label 24016, 3d:00:03:50, gigabitethernet0
          fe80::201:7aff:fe94:9a32 [0], gigabitethernet0
```

You can see that the loopback port route from PE1 to P and PE2 has the label information.

Note:

- For the checking method of P and PE2, refer to PE1

Step 4: Configure the VPN instance and advertise the CE route to PE via IPv6 BGP.

#On PE1, configure the VPN instance and the IPv6 BGP in VPN1 and VPN2.

```
PE1(config)#ip vrf 1
PE1(config-vrf)#rd 100:1
PE1(config-vrf)#route-target 100:1
PE1(config-vrf)#exit
PE1(config)#ip vrf 2
PE1(config-vrf)#rd 200:1
PE1(config-vrf)#route-target 200:1
PE1(config-vrf)#exit
PE1(config)#interface gigabitethernet2
PE1(config-if-gigabitethernet2)#ip vrf forwarding 1
PE1(config-if-gigabitethernet2)#ipv6 address 2001:1::1/64
PE1(config-if-gigabitethernet2)#exit
PE1(config)#interface gigabitethernet1
```

```
PE1(config-if-gigabitethernet1)#ip vrf forwarding 2
PE1(config-if-gigabitethernet1)#ipv6 address 2001:2::1/64
PE1(config-if-gigabitethernet1)#exit
PE1(config)#router bgp 100
PE1(config-bgp)#bgp router-id 1.1.1.1
PE1(config-bgp)#address-family ipv6 vrf 1
PE1(config-bgp-af)#neighbor 2001:1::2 remote-as 65100
PE1(config-bgp-af)#exit-address-family
PE1(config-bgp)#address-family ipv6 vrf 2
PE1(config-bgp-af)#neighbor 2001:2::2 remote-as 65200
PE1(config-bgp-af)#exit-address-family
PE1(config-bgp)#exit
```

#On CE1, configure IPv6 BGP.

```
CE1#configure terminal
CE1(config)#router bgp 65100
CE1(config-bgp)#bgp router-id 11.11.11.11
CE1(config-bgp)#address-family ipv6
CE1(config-bgp-af)#neighbor 2001:1::1 remote-as 100
CE1(config-bgp-af)#network 1::1/128
CE1(config-bgp-af)#exit-address-family
CE1(config-bgp)#exit
```

#On CE2, configure IPv6 BGP.

```
CE2#configure terminal
CE2(config)#router bgp 65200
CE2(config-bgp)#bgp router-id 22.22.22.22
CE2(config-bgp)#address-family ipv6
CE2(config-bgp-af)#neighbor 2001:2::1 remote-as 100
CE2(config-bgp-af)#network 2::2/128
CE2(config-bgp-af)#exit-address-family
CE2(config-bgp)#exit
```

#On PE2, configure the VPN instance and the IPv6 BGP in VPN1 and VPN2.

```
PE2(config)#ip vrf 1
PE2(config-vrf)#rd 100:1
PE2(config-vrf)#route-target 100:1
PE2(config-vrf)#exit
PE2(config)#ip vrf 2
PE2(config-vrf)#rd 200:1
```

```
PE2(config-vrf)#route-target 200:1
PE2(config-vrf)#exit
PE2(config)#interface gigabitethernet1
PE2(config-if-gigabitethernet1)#ip vrf forwarding 1
PE2(config-if-gigabitethernet1)#ipv6 address 2001:5::1/64
PE2(config-if-gigabitethernet1)#exit
PE2(config)#interface gigabitethernet2
PE2(config-if-gigabitethernet2)#ip vrf forwarding 2
PE2(config-if-gigabitethernet2)#ipv6 address 2001:6::1/64
PE2(config-if-gigabitethernet2)#exit
PE2(config)#router bgp 100
PE2(config-bgp)#bgp router-id 3.3.3.3
PE2(config-bgp)#address-family ipv6 vrf 1
PE2(config-bgp-af)#neighbor 2001:5::2 remote-as 65300
PE2(config-bgp-af)#exit-address-family
PE2(config-bgp)#address-family ipv6 vrf 2
PE2(config-bgp-af)#neighbor 2001:6::2 remote-as 65400
PE2(config-bgp-af)#exit-address-family
PE2(config-bgp)#exit
```

#On CE3, configure IPv6 BGP.

```
CE3#configure terminal
CE3(config)#router bgp 65300
CE3(config-bgp)#bgp router-id 33.33.33.33
CE3(config-bgp)#address-family ipv6
CE3(config-bgp-af)#neighbor 2001:5::1 remote-as 100
CE3(config-bgp-af)#network 3::3/128
CE3(config-bgp-af)#exit-address-family
CE3(config-bgp)#exit
```

#On CE4, configure IPv6 BGP.

```
CE4#configure terminal
CE4(config)#router bgp 65400
CE4(config-bgp)#bgp router-id 44.44.44.44
CE4(config-bgp)#address-family ipv6
CE4(config-bgp-af)#neighbor 2001:6::1 remote-as 100
CE4(config-bgp-af)#network 4::4/128
CE4(config-bgp-af)#exit-address-family
CE4(config-bgp)#exit
```

#After configuration, view the IPv6 BGP neighbor information on the PE.

Take PE1 as an example:

```
PE1#show bgp vpnv6 unicast all summary
BGP router identifier 1.1.1.1, local AS number 100
BGP VRF 1 Route Distinguisher:
100:1
BGP table version is 1
5 BGP AS-PATH entries
0 BGP community entries

Neighbor        V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
2001:1::2       4 65100      27      27        1    0    0 00:21:15        1

Total number of neighbors 1
BGP VRF 2 Route Distinguisher:
200:1
BGP table version is 1
5 BGP AS-PATH entries
0 BGP community entries

Neighbor        V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
2001:2::2       4 65200      26      26        1    0    0 00:20:42        1

Total number of neighbors 1
```

The content of the State/PfxRcd list is displayed as number (the number of the route prefixes received from the neighbor), and you can see that PE1 and CE1, CE2 set up the IPv6 BGP neighbor successfully.

#On PE, view the BGP route table and VPN route table.

Take PE1 as an example:

```
PE1#show bgp vpnv6 unicast vrf 1
BGP table version is 2, local router ID is 1.1.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network          Next Hop            Metric     LocPrf Weight Path
Route Distinguisher: 100:1 (Default for VRF 1)
[B]*> 1::1/128          2001:1::2                0             0 65100 i
```

```
PE1#show bgp vpnv6 unicast vrf 2
BGP table version is 2, local router ID is 1.1.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network          Next Hop            Metric     LocPrf Weight Path
Route Distinguisher: 200:1 (Default for VRF 2)
[B]*> 2::2/128          2001:2::2                0             0 65200 i

PE1#show ipv6 route vrf 1
Codes: C - Connected, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management



B   1::1/128 [20/0]
    via 2001:1::2, 00:09:07, gigabitethernet2
C   2001:1::/64 [0/0]
    via ::, 00:16:43, gigabitethernet2
L   2001:1::1/128 [0/0]
    via ::, 00:16:43, gigabitethernet2

PE1#show ipv6 route vrf 2
Codes: C - Connected, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management



B   2::2/128 [20/0]
    via 2001:2::2, 00:04:24, gigabitethernet1
C   2001:2::/64 [0/0]
    via ::, 17:00:48, gigabitethernet1
L   2001:2::1/128 [0/0]
    via ::, 17:00:48, gigabitethernet1
```

You can see that there is the routes to CE1 and CE2 in the VPN1 and VPN2 route tables of PE1.

Note:

- For the checking method of PE2, refer to PE1.

Step 5: Configure MP-IBGP, and use the loopback interface as the peer address.

#On PE1, configure MP-IBGP, enable the VPNv6 address family.

```
PE1(config)#router bgp 100
PE1(config-bgp)#neighbor 33::1 remote-as 100
PE1(config-bgp)#neighbor 33::1 update-source loopback 0
PE1(config-bgp)#address-family vpnv6
PE1(config-bgp-af)#neighbor 33::1 activate
PE1(config-bgp-af)#exit-address-family
PE1(config-bgp)#exit
```

#On PE2, configure MP-IBGP, enable the VPNv6 address family.

```
PE2(config)#router bgp 100
PE2(config-bgp)#neighbor 11::1 remote-as 100
PE2(config-bgp)#neighbor 11::1 update-source loopback 0
PE2(config-bgp)#address-family vpnv6
PE2(config-bgp-af)#neighbor 11::1 activate
PE2(config-bgp-af)#exit-address-family
PE2(config-bgp)#exit
```

Step 6: Check the result.

#After configuration, view the BGP neighbor information on PPE..

Take PE1 as an example:

```
PE1#show bgp vpnv6 unicast all summary
BGP router identifier 1.1.1.1, local AS number 100
BGP table version is 2
5 BGP AS-PATH entries
0 BGP community entries

Neighbor        V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
33::1           4   100       6       5        2    0    0 00:02:23        2

Total number of neighbors 1
BGP VRF 1 Route Distinguisher:
100:1
BGP table version is 1
```

```
5 BGP AS-PATH entries
0 BGP community entries

Neighbor        V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
2001:1::2       4 65100      27      27        1    0    0 00:21:15        1

Total number of neighbors 1
BGP VRF 2 Route Distinguisher:
200:1
BGP table version is 1
5 BGP AS-PATH entries
0 BGP community entries

Neighbor        V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
2001:2::2       4 65200      26      26        1    0    0 00:20:42        1

Total number of neighbors 1
```

The content of the State/PfxRcd list is displayed as number (the number of the route prefixes received from the neighbor), and you can see that PE1 and PE2 set up the BGP neighbor successfully.

#On PE, view the BGP VPNv6 route table and VPN route table.

Take PE1 as an example:

```
PE1#show bgp vpnv6 unicast vrf 1
BGP table version is 2, local router ID is 1.1.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network          Next Hop            Metric     LocPrf Weight Path
Route Distinguisher: 100:1 (Default for VRF 1)
[B]*> 1::1/128          2001:1::2                0             0 65100 i
[B]*>i3::3/128          33:1                     0       100   0 65300 i

PE1#show bgp vpnv6 unicast vrf 2
BGP table version is 2, local router ID is 1.1.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network          Next Hop            Metric     LocPrf Weight Path
```

```
Route Distinguisher: 200:1 (Default for VRF 2)
[B]*> 2::2/128          2001:2::2              0             0 65200 i
[B]*>i4::4/128          33:1                   0       100   0 65400 i
```

You can see that there is the route information to the peer CE3 and CE4 in the BGP VPNv6 route table of PE1.

```
PE1#show ipv6 route vrf 1
Codes: C - Connected, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management



B   1::1/128 [20/0]
    via 2001:1::2, 00:24:14, gigabitethernet2
B   3::3/128 [200/0]
    via 33:1, 00:05:02, gigabitethernet0
C   2001:1::/64 [0/0]
    via ::, 00:31:49, gigabitethernet2
L   2001:1::1/128 [0/0]
    via ::, 00:31:49, gigabitethernet2

PE1#show ipv6 route vrf 1 3::3/128
Codes: C - Connected, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management



B   3::3/128 [200/0]
    via 33:1 [0], label 25120, 00:05:10, gigabitethernet0
      fe80::201:7aff:fe94:9a32 [1], label 24016, gigabitethernet0
```

You can see that there is the route information to the peer CE3 in the VPN1 route table of PE1, the VPN label of the route is 25120, and the global label is 24016.

```
PE1#show ipv6 route vrf 2
Codes: C - Connected, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management
```

```
B   2::2/128 [20/0]
    via 2001:2::2, 00:19:31, gigabitethernet1
B   4::4/128 [200/0]
    via 33:1, 00:05:04, gigabitethernet0
C   2001:2::/64 [0/0]
    via ::, 17:15:55, gigabitethernet1
L   2001:2::1/128 [0/0]
    via ::, 17:15:55, gigabitethernet1

PE1#show ipv6 route vrf 2 4::4/128
Codes: C - Connected, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management

B   4::4/128 [200/0]
    via 33:1 [0], label 25121, 00:05:20, gigabitethernet0
       fe80::201:7aff:fe94:9a32 [1], label 24016, gigabitethernet0
```

You can see that there is the route information to the peer CE4 in the VPN2 route table of PE1, the VPN label of the route is 25121, and the global label is 24016.

#View the MPLS forwarding table on the PE.

Take PE1 as an example:

PE1#show mpls forwarding-table

```
Pro: L - LDP, O - OSPF, B - MP-BGP, R - RSVP, M - Mapped-Route, S - Static
Label,ML - mLDP (ML FEC: Root address/OT/OV), RM - RSVP P2MP (RM FEC: P2MP
ID/TID)

Pro Ident       FEC          Inlabel Outlabel Outgoing          Next hop
B   1           ::/0         25121   /        /                 ::
B   2           ::/0         25120   /        /                 ::
```

You can see that there is the route label information of VPN1 and VPN2 in the MPLS forwarding table of PE1.

Note:

- For the checking method of PE2, refer to PE1.

#Ping the loopback port of CE3 at CE1 and view whether the ping can be connected.

```
CE1#ping ipv6 3::3 -s 1::1

Press key (ctrl + shift + 6) interrupt it.
Reply from  3::3: bytes = 76  time < 16 ms
Reply from  3::3: bytes = 76  time < 16 ms
Reply from  3::3: bytes = 76  time < 16 ms
Reply from  3::3: bytes = 76  time < 16 ms
Reply from  3::3: bytes = 76  time < 16 ms
Success rate is 100% (5/5). Round-trip min/avg/max = 0/0/0 ms.
```

#Ping the loopback port of CE4 at CE1 and view whether the ping can be connected.

```
CE1#ping ipv6 4::4 -s 1::1

Press key (ctrl + shift + 6) interrupt it.
Send a packet to 4::4, request timed out.
Send a packet to 4::4, request timed out.
Send a packet to 4::4, request timed out.
Send a packet to 4::4, request timed out.
Send a packet to 4::4, request timed out.
Success rate is 0% (0/5).
```

You can see that the devices in one VPN can communicate normally, the devices of different VPNs cannot communicate, and the routes are separated.

7.3.3. Configure Cross-Domain OptionA (Over IPv4 LSP)

Network Requirements

- Deploy IPv4 LDP in the backbone network.
- The whole MPLS network includes two AS domains. CE1 is connected via AS100 and CE2 is connected via AS200.
- CE1 and CE2 belong to VPN1 at the same time; use IPv6 BGP to exchange the route with PE.
- Use the VRF-to-VRF mode to exchange the route information between ASBR.
- Route-Targets of the VPN instances of different AS do not need to match.
- ASBR and PE use MP-IBGP to exchange the VPNv6 route information.

Network Topology

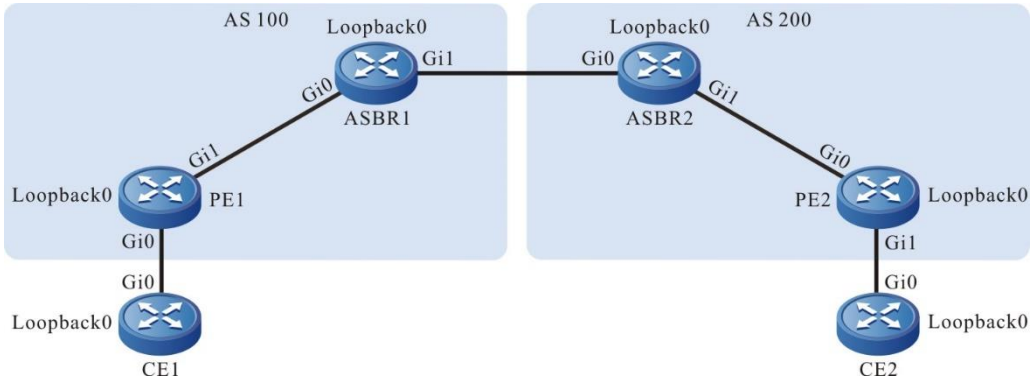

Figure 7-8 Networking of configuring the cross-domain OptionA

Device	Interface	IP Address	Device	Interface	IP Address
CE1	Gi0	2001:1::2/64	ASBR2	Gi0	2001:2::2/64
	Loopback0	1::1/128		Gi1	20.0.0.1/24
PE1	Gi0	2001:1::1/64		Loopback0	3.3.3.3/32
	Gi1	10.0.0.1/24	PE2	Gi0	20.0.0.2/24
	Loopback0	1.1.1.1/32		Gi1	2001:3::1/64
ASBR1	Gi0	2001:2::1/64		Loopback0	4.4.4.4/32
	Gi1	10.0.0.2/24	CE2	Gi0	2001:3::2/64
	Loopback0	2.2.2.2/32		Loopback0	2::2/128

Configuration Steps

Step 1: Configure the IP address of the interface (omitted).

Step 2: In one AS domain, configure the global OSPF to advertise the global route.

#Configure the global OSPF on PE1.

```
PE1#configure terminal
PE1(config)#router ospf 100
PE1(config-ospf)#network 10.0.0.0 0.0.0.255 area 0
PE1(config-ospf)#network 1.1.1.1 0.0.0.0 area 0
PE1(config-ospf)#exit
```

#Configure the global OSPF on ASBR1.

```
ASBR1#configure terminal
ASBR1(config)#router ospf 100
ASBR1(config-ospf)#network 10.0.0.0 0.0.0.255 area 0
ASBR1(config-ospf)#network 2.2.2.2 0.0.0.0 area 0
ASBR1(config-ospf)#exit
```

#Configure the global OSPF on ASBR2.

```
ASBR2#configure terminal
ASBR2(config)#router ospf 100
ASBR2(config-ospf)#network 20.0.0.0 0.0.0.255 area 0
ASBR2(config-ospf)#network 3.3.3.3 0.0.0.0 area 0
ASBR2(config-ospf)#exit
```

#Configure the global OSPF on PE2.

```
PE2#configure terminal
PE2(config)#router ospf 100
PE2(config-ospf)#network 20.0.0.0 0.0.0.255 area 0
PE2(config-ospf)#network 4.4.4.4 0.0.0.0 area 0
PE2(config-ospf)#exit
```

#After the configuration is complete, view the global route table on the device.

Take PE1 as an example:

```
PE1#show ip route
Codes: C - Connected, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
    U - Per-user Static route
    O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external



C   10.0.0.0/24 is directly connected, 00:08:24, gigabitethernet1
C   127.0.0.0/8 is directly connected, 1w3d:09:58:00, lo0
C   1.1.1.1/32 is directly connected, 03:36:57, loopback0
O   2.2.2.2/32 [110/2] via 10.0.0.2, 00:03:18, gigabitethernet1
```

You can see that there is the route information of ASBR1 loopback port in the global route table of PE1.

Note:

- For the checking method of PE2 and ASBR, refer to PE1.

Step 3: Enable MPLS IP and MPLS LDP.

#On PE1, enable the global MPLS IP and MPLS LDP. Meanwhile, enable MPLS IP and MPLS LDP on the interface.

```
PE1(config)#mpls ip
PE1(config)#mpls ldp
PE1(config-ldp)#router-id 1.1.1.1
PE1(config-ldp)#address-family ipv4
PE1(config-ldp-af4)#transport-address 1.1.1.1
PE1(config-ldp-af4)#exit
PE1(config-ldp)#exit
PE1(config)#interface gigabitethernet1
PE1(config-if-gigabitethernet1)#mpls ip
PE1(config-if-gigabitethernet1)#mpls ldp
PE1(config-if-gigabitethernet1)#exit
```

#On ASBR1, enable the global MPLS IP and MPLS LDP. Meanwhile, enable MPLS IP and MPLS LDP on the interface.

```
ASBR1(config)#mpls ip
ASBR1(config)#mpls ldp
ASBR1(config-ldp)#router-id 2.2.2.2
ASBR1(config-ldp)#address-family ipv4
ASBR1(config-ldp-af4)#transport-address 2.2.2.2
ASBR1(config-ldp-af4)#exit
ASBR1(config-ldp)#exit
ASBR1(config)#interface gigabitethernet0
ASBR1(config-if-gigabitethernet0)#mpls ip
ASBR1(config-if-gigabitethernet0)#mpls ldp
ASBR1(config-if-gigabitethernet0)#exit
```

#On ASBR2, enable the global MPLS IP and MPLS LDP. Meanwhile, enable MPLS IP and MPLS LDP on the interface.

```
ASBR2(config)#mpls ip
ASBR2(config)#mpls ldp
ASBR2(config-ldp)#router-id 3.3.3.3
ASBR2(config-ldp)#address-family ipv4
ASBR2(config-ldp-af4)#transport-address 3.3.3.3
ASBR2(config-ldp-af4)#exit
ASBR2(config-ldp)#exit
ASBR2(config)#interface gigabitethernet1
ASBR2(config-if-gigabitethernet1)#mpls ip
ASBR2(config-if-gigabitethernet1)#mpls ldp
```

```
ASBR2(config-if-gigabitethernet1)#exit
```

#On PE2, enable the global MPLS IP and MPLS LDP. Meanwhile, enable MPLS IP and MPLS LDP on the interface.

```
PE2(config)#mpls ip
PE2(config)#mpls ldp
PE2(config-ldp)#router-id 4.4.4.4
PE2(config-ldp)#address-family ipv4
PE2(config-ldp-af4)#transport-address 4.4.4.4
PE2(config-ldp-af4)#exit
PE2(config-ldp)#exit
PE2(config)#interface gigabitethernet0
PE2(config-if-gigabitethernet0)#mpls ip
PE2(config-if-gigabitethernet0)#mpls ldp
PE2(config-if-gigabitethernet0)#exit
```

#After the configuration is complete, view the LDP session information on the device.

Take PE1 as an example:

```
PE1#show mpls ldp session
Peer IP Address    Peer Type    My Role   State        DS Cap    DeadTime
2.2.2.2            Multicast    Passive   OPERATIONAL  Disabled  00:02:20
Statistics for ldp sessions:
    Multicast sessions: 1
    Targeted sessions: 0
```

You can see that PE1 and ASBR1 set up the LDP session successfully.

#View the route label information on the device.

Take PE1 as an example:

```
PE1#show ip route 2.2.2.2 detail
Codes: C - Connected, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
    U - Per-user Static route
    O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external




O   2.2.2.2/32 [110/2] via 10.0.0.2, label 3, 00:5:23, gigabitethernet1
                       10.0.0.2 [0], gigabitethernet1
```

You can see that the loopback port route from PE1 to ASBR1 has the label information.

Note:

- For the checking method of PE2 and ASBR, refer to PE1.

Step 4: Configure the VPN instance and advertise the CE route to PE via IPv6 BGP.

#Configure IPv6 BGP on CE1.

```
CE1#configure terminal
CE1(config)#router bgp 65100
CE1(config-bgp)#bgp router-id 11.11.11.11
CE1(config-bgp)#address-family ipv6
CE1(config-bgp-af)#neighbor 2001:1::1 remote-as 100
CE1(config-bgp-af)#network 1::1/128
CE1(config-bgp-af)#exit-address-family
CE1(config-bgp)#exit
```

#On PE1, configure the VPN instance and IPv6 BGP in VPN.

```
PE1(config)#ip vrf 1
PE1(config-vrf)#rd 100:1
PE1(config-vrf)#route-target 100:1
PE1(config-vrf)#exit
PE1(config)#interface gigabitethernet0
PE1(config-if-gigabitethernet0)#ip vrf forwarding 1
PE1(config-if-gigabitethernet0)#ipv6 address 2001:1::1/64
PE1(config-if-gigabitethernet0)#exit
PE1(config)#router bgp 100
PE1(config-bgp)#address-family ipv6 vrf 1
PE1(config-bgp-af)#neighbor 2001:1::2 remote-as 65100
PE1(config-bgp-af)#exit-address-family
PE1(config-bgp)#exit
```

#On ASBR1, configure the VPN instance.

```
ASBR1(config)#ip vrf 1
ASBR1(config-vrf)#rd 100:1
ASBR1(config-vrf)#route-target 100:1
ASBR1(config-vrf)#exit
ASBR1(config)#interface gigabitethernet1
ASBR1(config-if-gigabitethernet1)#ip vrf forwarding 1
ASBR1(config-if-gigabitethernet1)#ipv6 address 2001:2::1/64
ASBR1(config-if-gigabitethernet1)#exit
```

#On ASBR2, configure the VPN instance.

```
ASBR2(config)#ip vrf 1
ASBR2(config-vrf)#rd 200:1
ASBR2(config-vrf)#route-target 200:1
ASBR2(config-vrf)#exit
ASBR2(config)#interface gigabitethernet0
ASBR2(config-if-gigabitethernet0)#ip vrf forwarding 1
ASBR2(config-if-gigabitethernet0)#ipv6 address 2001:2::2/64
ASBR2(config-if-gigabitethernet0)#exit
```

#On PE2, configure the VPN instance and IPv6 BGP in VPN.

```
PE2(config)#ip vrf 1
PE2(config-vrf)#rd 200:1
PE2(config-vrf)#route-target 200:1
PE2(config-vrf)#exit
PE2(config)#interface gigabitethernet1
PE2(config-if-gigabitethernet1)#ip vrf forwarding 1
PE2(config-if-gigabitethernet1)#ipv6 address 2001:3::1/64
PE2(config-if-gigabitethernet1)#exit
PE2(config)#router bgp 200
PE2(config-bgp)#address-family ipv6 vrf 1
PE2(config-bgp-af)#neighbor 2001:3::2 remote-as 65200
PE2(config-bgp-af)#exit-address-family
PE2(config-bgp)#exit
```

#Configure IPv6 BGP on CE2.

```
CE2#configure terminal
CE2(config)#router bgp 65200
CE2(config-bgp)#bgp router-id 22.22.22.22
CE2(config-bgp)#address-family ipv6
CE2(config-bgp-af)#neighbor 2001:3::1 remote-as 200
CE2(config-bgp-af)#network 2::2/128
CE2(config-bgp-af)#exit-address-family
CE2(config-bgp)#exit
```

#After the configuration is complete, view the VPN route table on the PE.

Take PE1 as an example:

```
PE1#show ipv6 route vrf 1
Codes: C - Connected, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management
```

```
B   1::1/128 [20/0]
    via 2001:1::2, 02:42:12, gigabitethernet0
C   2001:1::/64 [0/0]
    via ::, 03:28:51, gigabitethernet0
L   2001:1::1/128 [0/0]
    via ::, 03:28:51, gigabitethernet0
```

You can see that there is the route to CE1 in the VPN1 route table of PE1.

Note:

- For the checking method of PE2, refer to PE1..

Step 5: Configure MP-IBGP between PE and ASBR, and use the loopback interface as the peer address; configure IPv6 BGP to exchange the route information between ASBRs.

#On PE1, configure MP-IBGP, enable the VPNv6 address family.

```
PE1(config)#router bgp 100
PE1(config-bgp)#neighbor 2.2.2.2 remote-as 100
PE1(config-bgp)#neighbor 2.2.2.2 update-source loopback 0
PE1(config-bgp)#address-family vpnv6
PE1(config-bgp-af)#neighbor 2.2.2.2 activate
PE1(config-bgp-af)#exit-address-family
PE1(config-bgp)#exit
```

#On ASBR1, configure MP-IBGP with PE1, enable the VPNv6 address family, and configure EBGP with ASBR2 in the IPv6 VRF address family.

```
ASBR1(config)#router bgp 100
ASBR1(config-bgp)#neighbor 1.1.1.1 remote-as 100
ASBR1(config-bgp)#neighbor 1.1.1.1 update-source loopback 0
ASBR1(config-bgp)#address-family vpnv6
ASBR1(config-bgp-af)#neighbor 1.1.1.1 activate
ASBR1(config-bgp-af)#exit-address-family
ASBR1(config-bgp)#address-family ipv6 vrf 1
ASBR1(config-bgp-af)#neighbor 2001:2::2 remote-as 200
ASBR1(config-bgp-af)#exit-address-family
ASBR1(config-bgp)#exit
```

#On ASBR2, configure MP-IBGP with PE2, enable the VPNv6 address family, and configure EBGP with ASBR1 in the IPv6 VRF address family.

```
ASBR2(config)#router bgp 200
ASBR2(config-bgp)#neighbor 4.4.4.4 remote-as 200
ASBR2(config-bgp)#neighbor 4.4.4.4 update-source loopback 0
ASBR2(config-bgp)#address-family vpnv6
ASBR2(config-bgp-af)#neighbor 4.4.4.4 activate
ASBR2(config-bgp-af)#exit-address-family
ASBR2(config-bgp)#address-family ipv6 vrf 1
ASBR2(config-bgp-af)#neighbor 2001:2::1 remote-as 100
ASBR2(config-bgp-af)#exit-address-family
ASBR2(config-bgp)#exit
```

#On PE2, configure MP-IBGP, and enable the VPNv6 address family.

```
PE2(config)#router bgp 200
PE2(config-bgp)#neighbor 3.3.3.3 remote-as 200
PE2(config-bgp)#neighbor 3.3.3.3 update-source loopback 0
PE2(config-bgp)#address-family vpnv6
PE2(config-bgp-af)#neighbor 3.3.3.3 activate
PE2(config-bgp-af)#exit-address-family
PE2(config-bgp)#exit
```

Step 6: Check the result.

#After the configuration is complete, view the BGP neighbor information on the PE and ASBR. Take PE1, ASBR1 as an example:

```
PE1#show bgp vpnv6 unicast all summary
BGP router identifier 1.1.1.1, local AS number 100
BGP table version is 8
3 BGP AS-PATH entries
0 BGP community entries

Neighbor        V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
2.2.2.2         4   100      18      17        8    0    0 00:13:09        1

Total number of neighbors 1
BGP VRF 1 Route Distinguisher:
100:1
BGP table version is 1
3 BGP AS-PATH entries
0 BGP community entries
```

```
Neighbor        V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
2001:1::2       4 65100     210     213        1    0    0 03:00:14        1

Total number of neighbors 1
```

The content of the State/PfxRcd list is displayed as number (the number of the route prefixes received from the neighbor), and you can see that PE1 and ASBR1, CE1 set up the BGP neighbor successfully.

```
ASBR1#show bgp vpnv6 unicast all summary
BGP router identifier 2.2.2.2, local AS number 100
BGP table version is 4
3 BGP AS-PATH entries
0 BGP community entries

Neighbor        V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
1.1.1.1         4   100      18      18        4    0    0 00:13:39        1

Total number of neighbors 1
BGP VRF 1 Route Distinguisher:
100:1
BGP table version is 1
3 BGP AS-PATH entries
0 BGP community entries

Neighbor        V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
2001:2::2       4   200      14      15        1    0    0 00:11:09        1

Total number of neighbors 1
```

The content of the State/PfxRcd list is displayed as number (the number of the route prefixes received from the neighbor), and you can see that ASBR1 and PE1, ASBR2 set up the BGP neighbor successfully.

#View the BGP VPNv6 route table on the PE and ASBR.

Take PE1, ASBR1 as an example:

```
PE1#show bgp vpnv6 unicast vrf 1
BGP table version is 8, local router ID is 1.1.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
```

```
    Network          Next Hop          Metric     LocPrf Weight Path
Route Distinguisher: 100:1 (Default for VRF 1)
[B]*> 1::1/128          2001:1::2              0              0 65100 i
[B]*>i2::2/128          ::ffff:2.2.2.2         0      100     0 200 65200 i

ASBR1#show bgp vpnv6 unicast vrf 1
BGP table version is 4, local router ID is 2.2.2.2
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
    Network          Next Hop          Metric     LocPrf Weight Path
Route Distinguisher: 100:1 (Default for VRF 1)
[B]*>i1::1/128          ::ffff:1.1.1.1         0      100     0 65100 i
[B]*> 2::2/128          2001:2::2              0              0 200 65200 i
```

You can see that there is the BGP route information to the peer CE2 in the BGP VPNv6 route table of PE1 and ASBR1.

#View the MPLS forwarding table on the PE and ASBR.

Take PE1, ASBR1 as an example:

PE1#show mpls forwarding-table

```
Pro: L - LDP, O - OSPF, B - MP-BGP, R - RSVP, M - Mapped-Route, S - Static
Label,ML - mLDP (ML FEC: Root address/OT/OV), RM - RSVP P2MP (RM FEC: P2MP
ID/TID)

Pro Ident       FEC             Inlabel Outlabel Outgoing          Next hop
B   1           ::/0            24000   /        /                 ::

ASBR1#show mpls forwarding-table
Pro: L - LDP, O - OSPF, B - MP-BGP, R - RSVP, M - Mapped-Route, S - Static
Label,ML - mLDP (ML FEC: Root address/OT/OV), RM - RSVP P2MP (RM FEC: P2MP
ID/TID)

Pro Ident       FEC             Inlabel Outlabel Outgoing          Next hop
B   1           ::/0            24000   /        /                 ::
```

You can see that there is the route label information of VPN1 in the MPLS forwarding table of PE1 and ASBR1.

Note:

- For the checking method of PE2, ASBR2 , refer to PE1, ASBR1.

#View the route table on the PE and CE.

Take PE1, CE1 as an example:

```
PE1#show ipv6 route vrf 1
Codes: C - Connected, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management



B   1::1/128 [20/0]
    via 2001:1::2, 15:07:48, gigabitethernet0
B   2::2/128 [200/0]
    via ::ffff:2.2.2.2, 12:07:59, gigabitethernet1
C   2001:1::/64 [0/0]
    via ::, 15:54:27, gigabitethernet0
L   2001:1::1/128 [0/0]
    via ::, 15:54:27, gigabitethernet0

PE1#show ipv6 route vrf 1 2::2/128
Codes: C - Connected, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management



B   2::2/128 [200/0]
    via ::ffff:2.2.2.2 [0], label 16, 12:08:30, gigabitethernet1
        ::ffff:10.0.0.2 [2], label 3, gigabitethernet1
```

You can see that there is the route information to the peer CE2 in the VPN1 route table of PE1, the VPN label of the route is 24000, and the global label is 3.

```
CE1#show ipv6 route
Codes: C - Connected, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management
```

```
L   ::1/128 [0/0]
    via ::, 1d:22:44:29, lo0
LC  1::1/128 [0/0]
    via ::, 16:04:31, loopback0
B   2::2/128 [20/0]
    via 2001:1::1, 12:08:25, gigabitethernet0
C   2001:1::/64 [0/0]
    via ::, 15:55:13, gigabitethernet0
L   2001:1::2/128 [0/0]
    via ::, 15:55:13, gigabitethernet0
```

You can see that there is the route information to the peer CE2 in the route table of PE1 and CE1.

#On CE1, ping the loopback port of CE2 and view whether the ping can be connected.

```
CE1#ping ipv6 2::2 -s 1::1

Press key (ctrl + shift + 6) interrupt it.
Reply from  2::2: bytes = 76  time < 16 ms
Reply from  2::2: bytes = 76  time < 16 ms
Reply from  2::2: bytes = 76  time < 16 ms
Reply from  2::2: bytes = 76  time < 16 ms
Reply from  2::2: bytes = 76  time < 16 ms
Success rate is 100% (5/5). Round-trip min/avg/max = 0/0/0 ms.
```

You can see that CE1 can ping CE2.

7.3.4. Configure Cross-Domain OptionA (Over IPv6 LSP)

Network Requirements

- Deploy IPv6 LDP in the backbone network.
- The whole MPLS network includes two AS domains. CE1 is connected via AS100 and CE2 is connected via AS200.
- CE1 and CE2 belong to VPN1 at the same time; use IPv6 BGP to exchange the route with PE.
- Use the VRF-to-VRF mode to exchange the route information between ASBR.
- Route-Targets of the VPN instances of different AS do not need to match.
- ASBR and PE use MP-IBGP to exchange the VPNv6 route information.

Network Topology

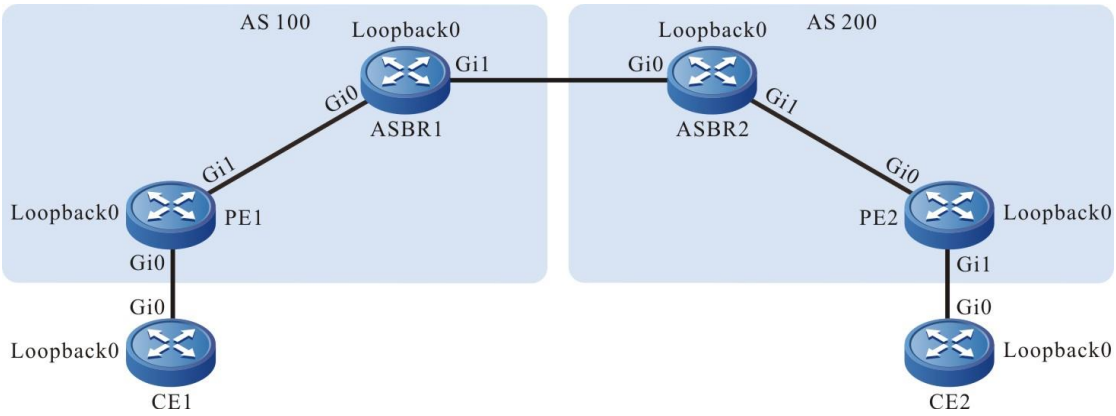

Figure 7-9 Networking of configuring the cross-domain OptionA

Device	Interface	IP Address	Device	Interface	IP Address
CE1	Gi0	2001:1::2/64	ASBR2	Gi0	2001:2::2/64
	Loopback0	1::1/128		Gi1	20::1/64
PE1	Gi0	2001:1::1/64		Loopback0	3:3:3::3/128
	Gi1	10::1/64	PE2	Gi0	20::2/64
	Loopback0	1:1:1::1/128		Gi1	2001:3::1/64
ASBR1	Gi0	10::2/64		Loopback0	4:4:4::4/32
	Gi1	2001:2::1/64	CE2	Gi0	2001:3::2/64
	Loopback0	2:2:2::2/128		Loopback0	2::2/128

Configuration Steps

Step 1: Configure the IP address of the interface (omitted).

Step 2: In one AS domain, configure the global OSPF to advertise the global route.

#Configure the global OSPFv3 on PE1.

```
PE1#configure terminal
PE1(config)#router ospf 100
PE1(config-ospf)#router-id 1.1.1.1
PE1(config-ospf)#exit
PE1(config)#interface loopback 0
```

```
PE1(config-if-loopback0)#ipv6 router ospf 100 area 0
PE1(config-if-loopback0)#exit
PE1(config)#interface gigabitethernet 1
PE1(config-if-gigabitethernet1)#ipv6 router ospf 100 area 0
PE1(config-if-gigabitethernet1)#exit
```

#Configure the global OSPFv3 on ASBR1.

```
ASBR1#configure terminal
ASBR1(config)#router ospf 100
ASBR1(config-ospf)#router-id 2.2.2.2
ASBR1(config-ospf)#exit
ASBR1(config)#interface loopback 0
ASBR1(config-if-loopback0)#ipv6 router ospf 100 area 0
ASBR1(config-if-loopback0)#exit
ASBR1(config)#interface gigabitethernet 0
ASBR1(config-if-gigabitethernet0)#ipv6 router ospf 100 area 0
ASBR1(config-if-gigabitethernet0)#exit
```

#Configure the global OSPFv3 on ASBR2.

```
ASBR2#configure terminal
ASBR2(config)#router ospf 100
ASBR2(config-ospf)#router-id 3.3.3.3
ASBR2(config-ospf)#exit
ASBR2(config)#interface loopback 0
ASBR2(config-if-loopback0)#ipv6 router ospf 100 area 0
ASBR2(config-if-loopback0)#exit
ASBR2(config)#interface gigabitethernet 1
ASBR2(config-if-gigabitethernet1)#ipv6 router ospf 100 area 0
ASBR2(config-if-gigabitethernet1)#exit
```

#Configure the global OSPFv3 on PE2.

```
PE2#configure terminal
PE2(config)#router ospf 100
PE2(config-ospf)#router-id 4.4.4.4
PE2(config-ospf)#exit
PE2(config)#interface loopback 0
PE2(config-if-loopback0)#ipv6 router ospf 100 area 0
PE2(config-if-loopback0)#exit
PE2(config)#interface gigabitethernet 0
PE2(config-if-gigabitethernet0)#ipv6 router ospf 100 area 0
```

```
PE2(config-if-gigabitethernet0)#exit
```

#After the configuration is complete, view the global route table on the device.

Take PE1 as an example:

```
PE1#show ipv6 route
Codes: C - Connected, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management
```

```
L   ::1/128 [0/0]
      via ::, 3d:00:05:42, lo0
LC  1:1:1::1/128 [0/0]
      via ::, 3d:00:04:55, loopback0
O   2:2:2::2/128 [110/1]
      via fe80::201:7aff:fe94:9a32, 3d:00:00:56, gigabitethernet1
C   10::/64 [0/0]
      via ::, 3d:00:01:51, gigabitethernet1
L   10::1/128 [0/0]
      via ::, 3d:00:01:51, gigabitethernet1
```

You can see that the loopback port route from PE1 to ASBR1 has the label information.

Note:

- For the checking method of PE2 and ASBR, refer to PE1.

Step 3: Enable MPLS IP and IPv6 MPLS LDP.

#On PE1, enable the global MPLS IP and IPv6 MPLS LDP. Meanwhile, enable MPLS IP and IPv6 MPLS LDP on the interface.

```
PE1(config)#mpls ip
PE1(config)#mpls ldp
PE1(config-ldp)#router-id 1.1.1.1
PE1(config-ldp)#address-family ipv6
PE1(config-ldp-af6)#transport-address 1:1:1::1
PE1(config-ldp-af6)#exit
PE1(config-ldp)#exit
PE1(config)#interface gigabitethernet1
PE1(config-if-gigabitethernet1)#mpls ip
PE1(config-if-gigabitethernet1)#mpls ldp ipv6
PE1(config-if-gigabitethernet1)#exit
```

#On ASBR1, enable the global MPLS IP and IPv6 MPLS LDP. Meanwhile, enable MPLS IP and IPv6 MPLS LDP on the interface.

```
ASBR1(config)#mpls ip
ASBR1(config)#mpls ldp
ASBR1(config-ldp)#router-id 2.2.2.2
ASBR1(config-ldp)#address-family ipv6
ASBR1(config-ldp-af6)#transport-address 2:2:2::2
ASBR1(config-ldp-af6)#exit
ASBR1(config-ldp)#exit
ASBR1(config)#interface gigabitethernet0
ASBR1(config-if-gigabitethernet0)#mpls ip
ASBR1(config-if-gigabitethernet0)#mpls ldp ipv6
ASBR1(config-if-gigabitethernet0)#exit
```

#On ASBR2, enable the global MPLS IP and IPv6 MPLS LDP. Meanwhile, enable MPLS IP and IPv6 MPLS LDP on the interface.

```
ASBR2(config)#mpls ip
ASBR2(config)#mpls ldp
ASBR2(config-ldp)#router-id 3.3.3.3
ASBR2(config-ldp)#address-family ipv6
ASBR2(config-ldp-af6)#transport-address 3:3:3::3
ASBR2(config-ldp-af6)#exit
ASBR2(config-ldp)#exit
ASBR2(config)#interface gigabitethernet1
ASBR2(config-if-gigabitethernet1)#mpls ip
ASBR2(config-if-gigabitethernet1)#mpls ldp ipv6
ASBR2(config-if-gigabitethernet1)#exit
```

#On PE2, enable the global MPLS IP and IPv6 MPLS LDP. Meanwhile, enable MPLS IP and IPv6 MPLS LDP on the interface.

```
PE2(config)#mpls ip
PE2(config)#mpls ldp
PE2(config-ldp)#router-id 4.4.4.4
PE2(config-ldp)#address-family ipv6
PE2(config-ldp-af6)#transport-address 4:4:4::4
PE2(config-ldp-af6)#exit
PE2(config-ldp)#exit
PE2(config)#interface gigabitethernet0
PE2(config-if-gigabitethernet0)#mpls ip
PE2(config-if-gigabitethernet0)#mpls ldp ipv6
```

```
PE2(config-if-gigabitethernet0)#exit
```

#After the configuration is complete, view the LDP session information on the device.

Take PE1 as an example:

```
PE1#show mpls ldp ipv6 session
Peer IPv6 Address                Peer Type     My Role   State         DS Cap
DeadTime
2:2:2::2                         Multicast     Passive   OPERATIONAL   Disabled
00:02:06
Statistics for ldp ipv6 sessions:
    Multicast sessions: 1
    Targeted sessions: 0
```

You can see that PE1 sets up the LDP session with ASBR1 successfully.

#View the route label information on the device.

Take PE1 as an example:

```
PE1#show ipv6 route 2:2:2::2
Codes: C - Connected, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
    U - Per-user Static route
    O - OSPF, OE-OSPF External, M - Management
```

```
O   2:2:2::2/128 [110/1]
   via fe80::201:7aff:fe94:9a32 [1], label 3, 3d:00:02:50, gigabitethernet1
      fe80::201:7aff:fe94:9a32 [0], gigabitethernet1
```

You can see that the loopback port route from PE1 to ASBR1 has the label information.

Note:

- For the checking methods of PE2 and ASBR, refer to PE1.

Step 4: Configure the VPN instance and advertise the CE route to PE via IPv6 BGP.

#On CE1, configure IPv6 BGP.

```
CE1#configure terminal
CE1(config)#router bgp 65100
CE1(config-bgp)#bgp router-id 11.11.11.11
CE1(config-bgp)#address-family ipv6
CE1(config-bgp-af)#neighbor 2001:1::1 remote-as 100
CE1(config-bgp-af)#network 1::1/128
CE1(config-bgp-af)#exit-address-family
CE1(config-bgp)#exit
```

#On PE1, configure the VPN instance and IPv6 BGP in VPN.

```
PE1(config)#ip vrf 1
PE1(config-vrf)#rd 100:1
PE1(config-vrf)#route-target 100:1
PE1(config-vrf)#exit
PE1(config)#interface gigabitethernet0
PE1(config-if-gigabitethernet0)#ip vrf forwarding 1
PE1(config-if-gigabitethernet0)#ipv6 address 2001:1::1/64
PE1(config-if-gigabitethernet0)#exit
PE1(config)#router bgp 100
PE1(config-bgp)#address-family ipv6 vrf 1
PE1(config-bgp-af)#neighbor 2001:1::2 remote-as 65100
PE1(config-bgp-af)#exit-address-family
PE1(config-bgp)#exit
```

#On ASBR1, configure the VPN instance.

```
ASBR1(config)#ip vrf 1
ASBR1(config-vrf)#rd 100:1
ASBR1(config-vrf)#route-target 100:1
ASBR1(config-vrf)#exit
ASBR1(config)#interface gigabitethernet1
ASBR1(config-if-gigabitethernet1)#ip vrf forwarding 1
ASBR1(config-if-gigabitethernet1)#ipv6 address 2001:2::1/64
ASBR1(config-if-gigabitethernet1)#exit
```

#On ASBR2, configure the VPN instance.

```
ASBR2(config)#ip vrf 1
ASBR2(config-vrf)#rd 100:1
ASBR2(config-vrf)#route-target 100:1
ASBR2(config-vrf)#exit
ASBR2(config)#interface gigabitethernet0
ASBR2(config-if-gigabitethernet0)#ip vrf forwarding 1
ASBR2(config-if-gigabitethernet0)#ipv6 address 2001:2::2/64
ASBR2(config-if-gigabitethernet0)#exit
```

#On PE2, configure the VPN instance and IPv6 BGP in VPN.

```
PE2(config)#ip vrf 1
PE2(config-vrf)#rd 100:1
PE2(config-vrf)#route-target 100:1
PE2(config-vrf)#exit
```

```
PE2(config)#interface gigabitethernet1
PE2(config-if-gigabitethernet1)#ip vrf forwarding 1
PE2(config-if-gigabitethernet1)#ipv6 address 2001:3::1/64
PE2(config-if-gigabitethernet1)#exit
PE2(config)#router bgp 200
PE2(config-bgp)#address-family ipv6 vrf 1
PE2(config-bgp-af)#neighbor 2001:3::2 remote-as 65200
PE2(config-bgp-af)#exit-address-family
PE2(config-bgp)#exit
```

#On CE2, configure IPv6 BGP.

```
CE2#configure terminal
CE2(config)#router bgp 65200
CE2(config-bgp)#bgp router-id 22.22.22.22
CE2(config-bgp)#address-family ipv6
CE2(config-bgp-af)#neighbor 2001:3::1 remote-as 200
CE2(config-bgp-af)#network 2::2/128
CE2(config-bgp-af)#exit-address-family
CE2(config-bgp)#exit
```

#After configuration, view the VPN route table on the PE.

Take PE1 as an example:

```
PE1#show ipv6 route vrf 1
Codes: C - Connected, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management




B   1::1/128 [20/0]
    via 2001:1::2, 02:42:12, gigabitethernet0
C   2001:1::/64 [0/0]
    via ::, 03:28:51, gigabitethernet0
L   2001:1::1/128 [0/0]
    via ::, 03:28:51, gigabitethernet0
```

You can see that there is the route to CE1 in the VPN1 route table of PE1.

Note:

- For the checking method of PE2, refer to PE1.

Step 5: Configure MP-IBGP between PE and ASBR, and use the loopback interface as the peer address; configure IPv6 BGP to exchange the route information between ASBRs.

#On PE1, configure MP-IBGP, enable the VPNv6 address family.

```
PE1(config)#router bgp 100
PE1(config-bgp)#neighbor 2:2:2::2 remote-as 100
PE1(config-bgp)#neighbor 2:2:2::2 update-source loopback 0
PE1(config-bgp)#address-family vpnv6
PE1(config-bgp-af)#neighbor 2:2:2::2 activate
PE1(config-bgp-af)#exit-address-family
PE1(config-bgp)#exit
```

#On ASBR1, configure MP-IBGP with PE1, enable the VPNv6 address family, and configure EBGP with ASBR2 in the IPv6 VRF address family.

```
ASBR1(config)#router bgp 100
ASBR1(config-bgp)#neighbor 1:1:1::1 remote-as 100
ASBR1(config-bgp)#neighbor 1:1:1::1 update-source loopback 0
ASBR1(config-bgp)#address-family vpnv6
ASBR1(config-bgp-af)#neighbor 1:1:1::1 activate
ASBR1(config-bgp-af)#exit-address-family
ASBR1(config-bgp)#address-family ipv6 vrf 1
ASBR1(config-bgp-af)#neighbor 2001:2::2 remote-as 200
ASBR1(config-bgp-af)#exit-address-family
ASBR1(config-bgp)#exit
```

#On ASBR2, configure MP-IBGP with PE1, enable the VPNv6 address family, and configure EBGP with ASBR2 in the IPv6 VRF address family.

```
ASBR2(config)#router bgp 200
ASBR2(config-bgp)#neighbor 4:4:4::4 remote-as 200
ASBR2(config-bgp)#neighbor 4:4:4::4 update-source loopback 0
ASBR2(config-bgp)#address-family vpnv6
ASBR2(config-bgp-af)#neighbor 4:4:4::4 activate
ASBR2(config-bgp-af)#exit-address-family
ASBR2(config-bgp)#address-family ipv6 vrf 1
ASBR2(config-bgp-af)#neighbor 2001:2::1 remote-as 100
ASBR2(config-bgp-af)#exit-address-family
ASBR2(config-bgp)#exit
```

#On PE2, configure MP-IBGP, enable the VPNv6 address family.

```
PE2(config)#router bgp 200
```

```
PE2(config-bgp)#neighbor 3:3:3::3 remote-as 200
PE2(config-bgp)#neighbor 3:3:3::3 update-source loopback 0
PE2(config-bgp)#address-family vpnv6
PE2(config-bgp-af)#neighbor 3:3:3::3 activate
PE2(config-bgp-af)#exit-address-family
PE2(config-bgp)#exit
```

Step 6: Check the result.

#After configuration, view the BGP neighbor information on PE and ASBR.

Take PE1 and ASBR1 as an example:

```
PE1#show bgp vpnv6 unicast all summary
BGP router identifier 1.1.1.1, local AS number 100
BGP table version is 3
2 BGP AS-PATH entries
0 BGP community entries

Neighbor      V      AS MsgRcvd MsgSent  TblVer  InQ OutQ Up/Down  State/PfxRcd
2:2:2::2      4      100      3      3       2    0    0 00:01:09        1

Total number of neighbors 1
BGP VRF 1 Route Distinguisher:
100:1
BGP table version is 1
3 BGP AS-PATH entries
0 BGP community entries

Neighbor      V    AS MsgRcvd MsgSent  TblVer  InQ OutQ Up/Down  State/PfxRcd
2001:1::2     4 65100     210     213       1    0    0 03:00:14        1

Total number of neighbors 1
```

The content of the State/PfxRcd list is displayed as number (the number of the route prefixes received from the neighbor), and you can see that PE1 and ASBR1, CE1 set up the BGP neighbor successfully.

```
PE1#show bgp vpnv6 unicast all summary
BGP router identifier 2.2.2.2, local AS number 100
BGP table version is 3
2 BGP AS-PATH entries
0 BGP community entries
```

```
Neighbor        V         AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
1:1:1::1        4        100       3       3        2    0    0 00:02:09        1

Total number of neighbors 1
BGP VRF 1 Route Distinguisher:
10:1
BGP table version is 1
2 BGP AS-PATH entries
0 BGP community entries

Neighbor        V         AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
2001:2::2       4        200       3       4        1    0    0 00:00:18        1

Total number of neighbors 1
```

The content of the State/PfxRcd list is displayed as number (the number of the route prefixes received from the neighbor), and you can see that ASBR1 and PE1, ASBR2 set up the BGP neighbor successfully.

#View the BGP VPNv6 route table on the PE and ASBR.

Take PE1, ASBR1 as an example:

```
PE1#show bgp vpnv6 unicast vrf 1
BGP table version is 8, local router ID is 1.1.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network          Next Hop            Metric     LocPrf Weight Path
Route Distinguisher: 100:1 (Default for VRF 1)
[B]*> 1::1/128          2001:1::2                0              0 65100 i
[B]*>i2::2/128          2:2:2::2                 0       100    0 200 65200 i

ASBR1#show bgp vpnv6 unicast vrf 1
BGP table version is 4, local router ID is 2.2.2.2
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network          Next Hop            Metric     LocPrf Weight Path
Route Distinguisher: 100:1 (Default for VRF 1)
[B]*>i1::1/128          1:1:1::1                 0       100    0 65100 i
```

[B]*> 2::2/128 2001:2::2 0 0 200 65200 i

You can see that there is the BGP route information to the peer CE2 in the BGP VPNv6 route table of PE1 and ASBR1.

#View the MPLS forwarding table on the PE and ASBR.

Take PE1, ASBR1 as an example:

PE1#show mpls forwarding-table

Pro: L - LDP, O - OSPF, B - MP-BGP, R - RSVP, M - Mapped-Route, S - Static Label,ML - mLDP (ML FEC: Root address/OT/OV), RM - RSVP P2MP (RM FEC: P2MP ID/TID)

Pro	Ident	FEC	Inlabel	Outlabel	Outgoing	Next hop
B	1	::/0	24000	/	/	::

ASBR1#show mpls forwarding-table

Pro: L - LDP, O - OSPF, B - MP-BGP, R - RSVP, M - Mapped-Route, S - Static Label,ML - mLDP (ML FEC: Root address/OT/OV), RM - RSVP P2MP (RM FEC: P2MP ID/TID)

Pro	Ident	FEC	Inlabel	Outlabel	Outgoing	Next hop
B	1	::/0	24000	/	/	::

You can see that there is the route label information of VPN1 in the MPLS forwarding table of PE1 and ASBR1.

Note:

- For the checking methods of PE2 and ASBR2, refer to PE1, ASBR1.

#View the route table on PE and CE.

Take PE1 and CE1 as an example:

PE1#show ipv6 route vrf 1

Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS

U - Per-user Static route

O - OSPF, OE-OSPF External, M - Management

B 1::1/128 [20/0]

via 2001:1::2, 15:07:48, gigabitethernet0

B 2::2/128 [200/0]

via 2:2:2::2, 12:07:59, gigabitethernet1

```
C   2001:1::/64 [0/0]
    via ::, 15:54:27, gigabitethernet0
L   2001:1::1/128 [0/0]
    via ::, 15:54:27, gigabitethernet0

PE1#show ipv6 route vrf 1 2::2/128
Codes: C - Connected, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management

B   2::2/128 [200/0]
    via 2:2:2::2 [0], label 24000, 12:08:30, gigabitethernet1
       fe80::201:7aff:fe94:9a32 [2], label 3, gigabitethernet1
```

You can see that there is the route information to the peer CE2 in the VPN1 route table of PE1, the VPN label of the route is 24000, and the global label is 3.

```
CE1#show ipv6 route
Codes: C - Connected, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management

L   ::1/128 [0/0]
    via ::, 1d:22:44:29, lo0
LC  1::1/128 [0/0]
    via ::, 16:04:31, loopback0
B   2::2/128 [20/0]
    via 2001:1::1, 12:08:25, gigabitethernet0
C   2001:1::/64 [0/0]
    via ::, 15:55:13, gigabitethernet0
L   2001:1::2/128 [0/0]
    via ::, 15:55:13, gigabitethernet0
```

You can see that there is the route information to the peer CE2 in the route table of PE1 and CE1.

#On CE1, ping the loopback port of CE2 and view whether the ping can be connected.

```
CE1#ping ipv6 2::2 -s 1::1

Press key (ctrl + shift + 6) interrupt it.
Reply from  2::2: bytes = 76  time < 16 ms
Reply from  2::2: bytes = 76  time < 16 ms
Reply from  2::2: bytes = 76  time < 16 ms
Reply from  2::2: bytes = 76  time < 16 ms
Reply from  2::2: bytes = 76  time < 16 ms
Success rate is 100% (5/5). Round-trip min/avg/max = 0/0/0 ms.
```

You can see that CE1 can ping CE2.

7.3.5. Configure Cross-Domain OptionB (Over IPv4 LSP)

Network Requirements

- Deploy IPv4 LDP in the backbone network.
- The whole MPLS network includes two AS domains. CE1 is connected via AS100 and CE2 is connected via AS200.
- CE1 and CE2 belong to VPN1 at the same time; use IPv6 BGP to exchange the route with PE.
- Use the MP-EBGP to exchange the VPNv6 route information between ASBR.
- ASBR and PE use MP-IBGP to exchange the VPNv6 route information.

Network Topology

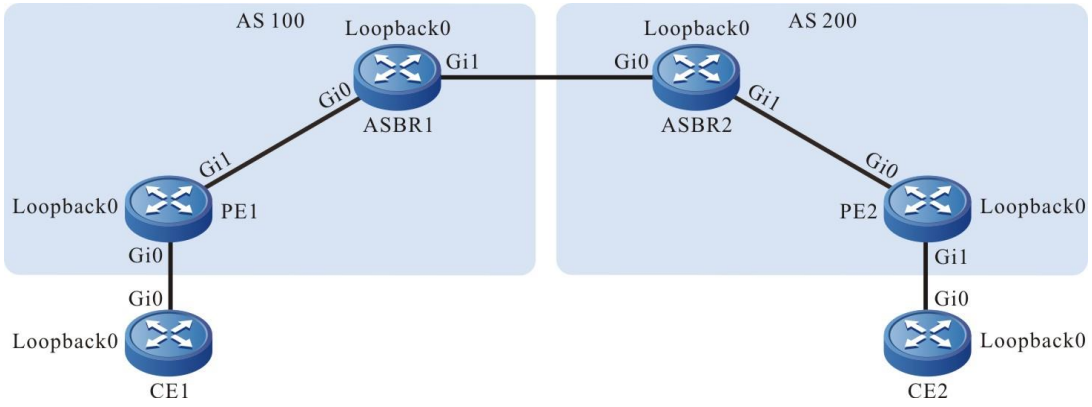

Figure 7-10 Networking of configuring cross-domain OptionB

Device	Interface	IP Address	Device	Interface	IP Address
CE1	Gi0	2001:1::2/64	ASBR2	Gi0	30.0.0.2/24
	Loopback0	1::1/128		Gi1	20.0.0.1/24
PE1	Gi0	2001:1::1/64		Loopback0	3.3.3.3/32
	Gi1	10.0.0.1/24	PE2	Gi0	20.0.0.2/24
	Loopback0	1.1.1.1/32		Gi1	2001:2::1/64
ASBR1	Gi0	30.0.0.1/24		Loopback0	4.4.4.4/32
	Gi1	10.0.0.2/24	CE2	Gi0	2001:2::2/64
	Loopback0	2.2.2.2/32		Loopback0	2::2/128

Configuration Steps

Step 1: Configure the IP address of the interface (omitted).

Step 2: In one AS domain, configure the global OSPF to advertise the global route.

#Configure the global OSPF on PE1.

```
PE1#configure terminal
PE1(config)#router ospf 100
PE1(config-ospf)#network 10.0.0.0 0.0.0.255 area 0
PE1(config-ospf)#network 1.1.1.1 0.0.0.0 area 0
PE1(config-ospf)#exit
```

#Configure the global OSPF on ASBR1.

```
ASBR1#configure terminal
ASBR1(config)#router ospf 100
ASBR1(config-ospf)#network 10.0.0.0 0.0.0.255 area 0
ASBR1(config-ospf)#network 2.2.2.2 0.0.0.0 area 0
ASBR1(config-ospf)#exit
```

#Configure the global OSPF on ASBR2.

```
ASBR2#configure terminal
ASBR2(config)#router ospf 100
ASBR2(config-ospf)#network 20.0.0.0 0.0.0.255 area 0
```

```
ASBR2(config-ospf)#network 3.3.3.3 0.0.0.0 area 0
ASBR2(config-ospf)#exit
```

#Configure the global OSPF on PE2.

```
PE2(config)#router ospf 100
PE2(config-ospf)#network 20.0.0.0 0.0.0.255 area 0
PE2(config-ospf)#network 4.4.4.4 0.0.0.0 area 0
PE2(config-ospf)#exit
```

#After the configuration is complete, view the global route table on the device.

Take PE1 as an example:

```
PE1#show ip route
Codes: C - Connected, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external



C   10.0.0.0/24 is directly connected, 00:08:24, gigabitethernet1
C   127.0.0.0/8 is directly connected, 1w3d:09:58:00, lo0
C   1.1.1.1/32 is directly connected, 03:36:57, loopback0
O   2.2.2.2/32 [110/2] via 10.0.0.2, 00:03:18, gigabitethernet1
```

You can see that there is the route information of ASBR1 loopback port in the global route table of PE1.

Note:

- For the checking method of PE2 and ASBR, refer to PE1.

Step 3: Enable MPLS IP and MPLS LDP.

#On PE1, enable the global MPLS IP and MPLS LDP. Meanwhile, enable MPLS IP and MPLS LDP on the interface.

```
PE1(config)#mpls ip
PE1(config)#mpls ldp
PE1(config-ldp)#router-id 1.1.1.1
PE1(config-ldp)#address-family ipv4
PE1(config-ldp-af4)#transport-address 1.1.1.1
PE1(config-ldp-af4)#exit
PE1(config-ldp)#exit
PE1(config)#interface gigabitethernet1
PE1(config-if-gigabitethernet1)#mpls ip
PE1(config-if-gigabitethernet1)#mpls ldp
```

```
PE1(config-if-gigabitethernet1)#exit
```

#On ASBR1, enable the global MPLS IP and MPLS LDP; meanwhile, enable MPLS IP and MPLS LDP on the interface with PE1. The interfaces between ASBRs only need to enable MPLS IP, but do not need to configure MPLS LDP.

```
ASBR1(config)#mpls ip
ASBR1(config)#mpls ldp
ASBR1(config-ldp)#router-id 2.2.2.2
ASBR1(config-ldp)#address-family ipv4
ASBR1(config-ldp-af4)#transport-address 2.2.2.2
ASBR1(config-ldp-af4)#exit
ASBR1(config-ldp)#exit
ASBR1(config)#interface gigabitethernet0
ASBR1(config-if-gigabitethernet0)#mpls ip
ASBR1(config-if-gigabitethernet0)#mpls ldp
ASBR1(config-if-gigabitethernet0)#exit
ASBR1(config)#interface gigabitethernet1
ASBR1(config-if-gigabitethernet1)#mpls ip
ASBR1(config-if-gigabitethernet1)#exit
```

#On ASBR2, enable the global MPLS IP and MPLS LDP; meanwhile, enable MPLS IP and MPLS LDP on the interface with PE2. The interfaces between ASBRs only need to enable MPLS IP, but do not need to configure MPLS LDP.

```
ASBR2(config)#mpls ip
ASBR2(config)#mpls ldp
ASBR2(config-ldp)#router-id 3.3.3.3
ASBR2(config-ldp)#address-family ipv4
ASBR2(config-ldp-af4)#transport-address 3.3.3.3
ASBR2(config-ldp-af4)#exit
ASBR2(config-ldp)#exit
ASBR2(config)#interface gigabitethernet0
ASBR2(config-if-gigabitethernet0)#mpls ip
ASBR2(config-if-gigabitethernet0)#exit
ASBR2(config)#interface gigabitethernet1
ASBR2(config-if-gigabitethernet1)#mpls ip
ASBR2(config-if-gigabitethernet1)#mpls ldp
ASBR2(config-if-gigabitethernet1)#exit
```

#On PE2, enable the global MPLS IP and MPLS LDP. Meanwhile, enable MPLS IP and MPLS LDP on the interface.

```
PE2(config)#mpls ip
```

```
PE2(config)#mpls ldp
PE2(config-ldp)#router-id 4.4.4.4
PE2(config-ldp)#address-family ipv4
PE2(config-ldp-af4)#transport-address 4.4.4.4
PE2(config-ldp-af4)#exit
PE2(config-ldp)#exit
PE2(config)#interface gigabitethernet0
PE2(config-if-gigabitethernet0)#mpls ip
PE2(config-if-gigabitethernet0)#mpls ldp
PE2(config-if-gigabitethernet0)#exit
```

#After the configuration is complete, view the LDP session information on the device.

Take PE1 as an example:

```
PE1#show mpls ldp session
Peer IP Address    Peer Type    My Role   State        DS Cap    DeadTime
2.2.2.2            Multicast    Passive   OPERATIONAL  Disabled  00:02:20
Statistics for ldp sessions:
    Multicast sessions: 1
    Targeted sessions: 0
```

You can see that PE1 and ASBR1 set up the LDP session successfully.

#View the route label information on the device.

Take PE1 as an example:

```
PE1#show ip route 2.2.2.2 detail
Codes: C - Connected, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
    U - Per-user Static route
    O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external




O   2.2.2.2/32 [110/2] via 10.0.0.2, label 3, 00:5:23, gigabitethernet1
                       10.0.0.2 [0], gigabitethernet1
```

You can see that the loopback port rouet from PE1 to ASBR1 has the label information.

Note:

- For the checking method of PE2 and ASBR, refer to PE1.

Step 4: Configure the VPN instance and advertise the CE route to the PE via IPv6 BGP.

#On CE1, configure IPv6 BGP.

```
CE1#configure terminal
CE1(config)#router bgp 65100
CE1(config-bgp)#bgp router-id 11.11.11.11
CE1(config-bgp)#address-family ipv6
CE1(config-bgp-af)#neighbor 2001:1::1 remote-as 100
CE1(config-bgp-af)#network 1::1/128
CE1(config-bgp-af)#exit-address-family
CE1(config-bgp)#exit
```

#On PE1, configure the VPN instance and IPv6 BGP in the VPN instance.

```
PE1(config)#ip vrf 1
PE1(config-vrf)#rd 100:1
PE1(config-vrf)#route-target 100:1
PE1(config-vrf)#exit
PE1(config)#interface gigabitethernet0
PE1(config-if-gigabitethernet0)#ip vrf forwarding 1
PE1(config-if-gigabitethernet0)#ipv6 address 2001:1::1/64
PE1(config-if-gigabitethernet0)#exit
PE1(config)#router bgp 100
PE1(config-bgp)#address-family ipv6 vrf 1
PE1(config-bgp-af)#neighbor 2001:1::2 remote-as 65100
PE1(config-bgp-af)#exit-address-family
PE1(config-bgp)#exit
```

#On PE2, configure the VPN instance and IPv6 BGP in the VPN instance.

```
PE2(config)#ip vrf 1
PE2(config-vrf)#rd 100:1
PE2(config-vrf)#route-target 100:1
PE2(config-vrf)#exit
PE2(config)#interface gigabitethernet1
PE2(config-if-gigabitethernet1)#ip vrf forwarding 1
PE2(config-if-gigabitethernet1)#ipv6 address 2001:2::1/64
PE2(config-if-gigabitethernet1)#exit
PE2(config)#router bgp 200
PE2(config-bgp)#address-family ipv6 vrf 1
PE2(config-bgp-af)#neighbor 2001:2::2 remote-as 65200
PE2(config-bgp-af)#exit-address-family
PE2(config-bgp)#exit
```

#On CE2, configure IPv6 BGP.

```
CE2#configure terminal
CE2(config)#router bgp 65200
CE2(config-bgp)#bgp router-id 22.22.22.22
CE2(config-bgp)#address-family ipv6
CE2(config-bgp-af)#neighbor 2001:2::1 remote-as 200
CE2(config-bgp-af)#network 2::2/128
CE2(config-bgp-af)#exit-address-family
CE2(config-bgp)#exit
```

#After the configuration is complete, view the VPN route table on the PE.

Take PE1 as an example:

```
PE1#show ipv6 route vrf 1
Codes: C - Connected, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management
```

```
B   1::1/128 [20/0]
    via 2001:1::2, 02:42:12, gigabitethernet0
C   2001:1::/64 [0/0]
    via ::, 03:28:51, gigabitethernet0
L   2001:1::1/128 [0/0]
    via ::, 03:28:51, gigabitethernet0
```

You can see that there is the route to the CE1 in the VPN1 route table of PE1.

Note:

- For the checking method of PE2, refer to PE1..

Step 5: Configure MP-IBGP between PE and ASBR, and use the loopback interface as the peer address; configure MP-EBGP between ASBRs.

#On PE1, configure MP-IBGP, enable the VPNv6 address family.

```
PE1(config)#router bgp 100
PE1(config-bgp)#neighbor 2.2.2.2 remote-as 100
PE1(config-bgp)#neighbor 2.2.2.2 update-source loopback0
PE1(config-bgp)#address-family vpnv6
PE1(config-bgp-af)#neighbor 2.2.2.2 activate
PE1(config-bgp-af)#exit-address-family
PE1(config-bgp-af)#exit
```

#On ASBR1, configure MP-IBGP with PE1, configure MP-EBGP between ASBR1 and ASBR2, and enable the VPNv6 address family.

```
ASBR1(config)#router bgp 100
ASBR1(config-bgp)#neighbor 30.0.0.2 remote-as 200
ASBR1(config-bgp)#neighbor 1.1.1.1 remote-as 100
ASBR1(config-bgp)#neighbor 1.1.1.1 update-source loopback0
ASBR1(config-bgp)#address-family vpnv6
ASBR1(config-bgp-af)#neighbor 30.0.0.2 activate
ASBR1(config-bgp-af)#neighbor 1.1.1.1 activate
ASBR1(config-bgp-af)#neighbor 1.1.1.1 next-hop-self
ASBR1(config-bgp-af)#exit-address-family
ASBR1(config-bgp)#exit
```

#On ASBR2, configure MP-IBGP with PE2, configure MP-EBGP between ASBR1 and ASBR2, and enable the VPNv6 address family.

```
ASBR2(config)#router bgp 200
ASBR2(config-bgp)#neighbor 30.0.0.1 remote-as 100
ASBR2(config-bgp)#neighbor 4.4.4.4 remote-as 200
ASBR2(config-bgp)#neighbor 4.4.4.4 update-source loopback0
ASBR2(config-bgp)#address-family vpnv6
ASBR2(config-bgp-af)#neighbor 30.0.0.1 activate
ASBR2(config-bgp-af)#neighbor 4.4.4.4 activate
ASBR2(config-bgp-af)#neighbor 4.4.4.4 next-hop-self
ASBR2(config-bgp-af)#exit-address-family
ASBR2(config-bgp)#exit
```

#On PE2, configure MP-IBGP, and enable the VPNv6 address family

```
PE2(config)#router bgp 200
PE2(config-bgp)#neighbor 3.3.3.3 remote-as 200
PE2(config-bgp)#neighbor 3.3.3.3 update-source loopback0
PE2(config-bgp)#address-family vpnv6
PE2(config-bgp-af)#neighbor 3.3.3.3 activate
PE2(config-bgp-af)#exit-address-family
PE2(config-bgp)#exit
```

Step 6: Check the result.

#After the configuration is complete, view the BGP neighbor information on the PE and ASBR.

Take PE1, ASBR1 as an example:

```
PE1#show bgp vpnv6 unicast all summary
BGP router identifier 1.1.1.1, local AS number 100
```

```
BGP table version is 10
3 BGP AS-PATH entries
0 BGP community entries

Neighbor        V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
2.2.2.2         4   100     933     925       10    0    0 13:19:00        1

Total number of neighbors 1
BGP VRF 1 Route Distinguisher:
100:1
BGP table version is 1
3 BGP AS-PATH entries
0 BGP community entries

Neighbor        V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
2001:1::2       4 65100    1117    1124        1    0    0 16:06:05        1

Total number of neighbors 1
```

The content of the State/PfxRcd list is displayed as number (the number of the route prefixes received from the neighbor), and you can see that PE1 and ASBR1 set up the BGP neighbor successfully.

```
ASBR1#show bgp vpnv6 unicast all summary
BGP router identifier 2.2.2.2, local AS number 100
BGP table version is 9
3 BGP AS-PATH entries
0 BGP community entries

Neighbor        V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
1.1.1.1         4   100     926     934        9    0    0 13:20:03        1
30.0.0.2        4   200      14      13        9    0    0 00:09:47        1

Total number of neighbors 2
```

The content of the State/PfxRcd list is displayed as number (the number of the route prefixes received from the neighbor), and you can see that ASBR1 and PE1, ASBR2 set up the BGP neighbor successfully.

#View the BGP VPNv6 route table on the PE and ASBR.

Take PE1, ASBR1 as an example:

```
PE1#show bgp vpnv6 unicast vrf 1
```

```
BGP table version is 10, local router ID is 1.1.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network          Next Hop            Metric     LocPrf Weight Path
Route Distinguisher: 100:1 (Default for VRF 1)
[B]*> 1::1/128           2001:1::2                0              0 65100 i
[B]*>i2::2/128           ::ffff:2.2.2.2           0       100    0 200 65200 i

ASBR1#show bgp vpnv6 unicast all
BGP table version is 9, local router ID is 2.2.2.2
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network          Next Hop            Metric     LocPrf Weight Path
Route Distinguisher: 100:1
[B]*>i1::1/128           ::ffff:1.1.1.1           0       100    0 65100 i
[B]*> 2::2/128           ::ffff:30.0.0.2          0              0 200 65200 i
```

You can see that there is the BGP route information to the peer CE2 in the BGP VPNv6 route table of PE1 and ASBR1.

#View the MPLS forwarding table on the PE and ASBR.

Take PE1, ASBR1 as an example:

```
PE1#show mpls forwarding-table
Pro: L - LDP, O - OSPF, B - MP-BGP, R - RSVP, M - Mapped-Route, S - Static
Label,ML - mLDP (ML FEC: Root address/OT/OV), RM - RSVP P2MP (RM FEC: P2MP
ID/TID)

Pro Ident        FEC             Inlabel Outlabel Outgoing            Next hop
B   1            ::/0            24000   /        /                   ::

ASBR1#show mpls forwarding-table
Pro: L - LDP, O - OSPF, B - MP-BGP, R - RSVP, M - Mapped-Route, S - Static
Label,ML - mLDP (ML FEC: Root address/OT/OV), RM - RSVP P2MP (RM FEC: P2MP
ID/TID)

Pro Ident        FEC             Inlabel Outlabel Outgoing          Next hop
```

```
B   global      1::1/128          24000   24000   gigabitethernet0    1.1.1.1
B   global      2::2/128          24001   24000   gigabitethernet1    30.0.0.2
```

You can see that there is the route label information of VPN1 in the MPLS forwarding table of PE1 and ASBR1.

Note:

- For the checking method of PE2, ASBR2 , refer to PE1, ASBR1.

#View the route table on the device.

Take PE1, CE1 as an example:

```
PE1#show ipv6 route vrf 1
Codes: C - Connected, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management

B   1::1/128 [20/0]
    via 2001:1::2, 16:21:29, gigabitethernet0
B   2::2/128 [200/0]
    via ::ffff:2.2.2.2, 00:15:51, gigabitethernet1
C   2001:1::/64 [0/0]
    via ::, 17:08:07, gigabitethernet0
L   2001:1::1/128 [0/0]
    via ::, 17:08:07, gigabitethernet0

PE1#show ipv6 route vrf 1 2::2/128
Codes: C - Connected, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management

B   2::2/128 [200/0]
    via ::ffff:2.2.2.2 [0], label 16, 12:08:30, gigabitethernet1
        ::ffff:10.0.0.2 [2], label 3, gigabitethernet1
```

You can see that there is the route information to the peer CE2 in the VPN1 route table of PE1, the VPN label of the route is 16, and the global label is 3.

```
CE1#show ipv6 route
Codes: C - Connected, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management



L   ::1/128 [0/0]
      via ::, 1d:23:59:08, lo0
LC  1::1/128 [0/0]
      via ::, 17:19:10, loopback0
B   2::2/128 [20/0]
      via 2001:1::1, 00:17:03, gigabitethernet0
C   2001:1::/64 [0/0]
      via ::, 17:09:51, gigabitethernet0
L   2001:1::2/128 [0/0]
      via ::, 17:09:51, gigabitethernet0
```

You can see that there is the route information to the peer CE2 in the route table of PE1 and CE1.

#On CE1, ping the loopback port of CE2 and view whether the ping can be connected.

```
CE1#ping ipv6 2::2 -s 1::1


Press key (ctrl + shift + 6) interrupt it.
Reply from  2::2: bytes = 76  time < 16 ms
Reply from  2::2: bytes = 76  time < 16 ms
Reply from  2::2: bytes = 76  time < 16 ms
Reply from  2::2: bytes = 76  time < 16 ms
Reply from  2::2: bytes = 76  time < 16 ms
Success rate is 100% (5/5). Round-trip min/avg/max = 0/0/0 ms.
```

You can see that CE1 can ping CE2.

7.3.6. Configure Cross-Domain OptionB (Over IPv6 LSP)

Network Requirements

- Deploy IPv6 LDP in the backbone network.
- The whole MPLS network includes two AS domains. CE1 is connected via AS100 and CE2 is connected via AS200.
- CE1 and CE2 belong to VPN1 at the same time; use IPv6 BGP to exchange the route with PE.
- Use the MP-EBGP to exchange the VPNv6 route information between ASBR and PE.

- Use MP-EBGP to exchange the VPNv6 route information between ASBRs.

Network Topology

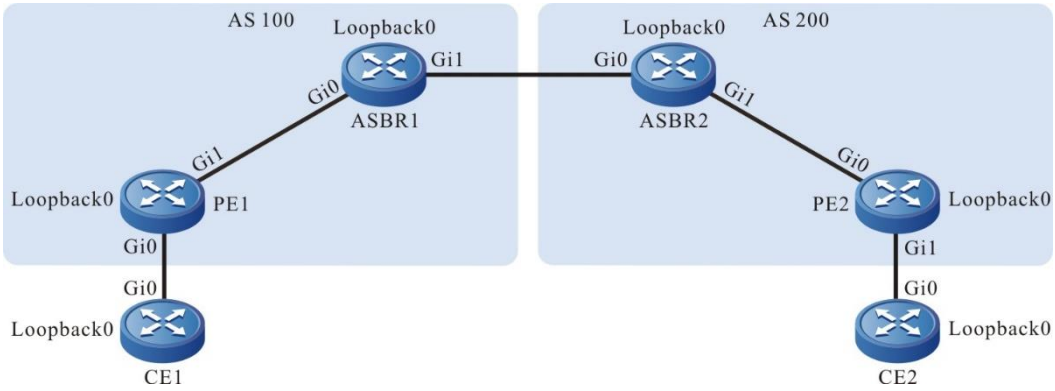

Figure 7-11 Networking of configuring cross-domain OptionB

Device	Interface	IP Address	Device	Interface	IP Address
CE1	Gi0	2001:1::2/64	ASBR2	Gi0	30::2/64
	Loopback0	1::1/128		Gi1	20::1/64
PE1	Gi0	2001:1::1/64		Loopback0	3:3:3::3/32
	Gi1	10::1/64	PE2	Gi0	20::2/64
	Loopback0	1:1:1::1/128		Gi1	2001:2::1/64
ASBR1	Gi0	10::2/64		Loopback0	4:4:4::4/128
	Gi1	30::1/64	CE2	Gi0	2001:2::2/64
	Loopback0	2:2:2::2/128		Loopback0	2::2/128

Configuration Steps

Step 1: Configure the IP address of the interface (omitted).

Step 2: In one AS domain, configure the global OSPF and advertise the global route.

#Configure the global OSPFv3 on PE1.

```
PE1#configure terminal
PE1(config)#ipv6 router ospf 100
```

```
PE1(config-ospf6)#router-id 1.1.1.1
PE1(config-ospf6)#exit
PE1(config)#interface loopback 0
PE1(config-if-loopback0)#ipv6 router ospf 100 area 0
PE1(config-if-loopback0)#exit
PE1(config)#interface gigabitethernet 1
PE1(config-if-gigabitethernet1)#ipv6 router ospf 100 area 0
PE1(config-if-gigabitethernet1)#exit
```

#Configure the global OSPFv3 on ASBR1.

```
ASBR1#configure terminal
ASBR1(config)#ipv6 router ospf 100
ASBR1(config-ospf6)#router-id 2.2.2.2
ASBR1(config-ospf6)#exit
ASBR1(config)#interface loopback 0
ASBR1(config-if-loopback0)#ipv6 router ospf 100 area 0
ASBR1(config-if-loopback0)#exit
ASBR1(config)#interface gigabitethernet 0
ASBR1(config-if-gigabitethernet0)#ipv6 router ospf 100 area 0
ASBR1(config-if-gigabitethernet0)#exit
```

#Configure the global OSPFv3 on ASBR2.

```
ASBR2#configure terminal
ASBR2(config)#ipv6 router ospf 100
ASBR2(config-ospf6)#router-id 3.3.3.3
ASBR2(config-ospf6)#exit
ASBR2(config)#interface loopback 0
ASBR2(config-if-loopback0)#ipv6 router ospf 100 area 0
ASBR2(config-if-loopback0)#exit
ASBR2(config)#interface gigabitethernet 1
ASBR2(config-if-gigabitethernet1)#ipv6 router ospf 100 area 0
ASBR2(config-if-gigabitethernet1)#exit
```

#Configure the global OSPFv3 on PE2.

```
PE2#configure terminal
PE2(config)#ipv6 router ospf 100
PE2(config-ospf6)#router-id 4.4.4.4
PE2(config-ospf6)#exit
PE2(config)#interface loopback 0
PE2(config-if-loopback0)#ipv6 router ospf 100 area 0
```

```
PE2(config-if-loopback0)#exit
PE2(config)#interface gigabitethernet 0
PE2(config-if-gigabitethernet0)#ipv6 router ospf 100 area 0
PE2(config-if-gigabitethernet0)#exit
```

#After the configuration is complete, view the global route table on the device.

Take PE1 as an example:

```
PE1#show ipv6 route
Codes: C - Connected, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management
```

```
L   ::1/128 [0/0]
      via ::, 3d:00:05:42, lo0
LC  1:1:1::1/128 [0/0]
      via ::, 3d:00:04:55, loopback0
O   2:2:2::2/128 [110/1]
      via fe80::201:7aff:fe94:9a32, 3d:00:00:56, gigabitethernet1
C   10::/64 [0/0]
      via ::, 3d:00:01:51, gigabitethernet1
L   10::1/128 [0/0]
      via ::, 3d:00:01:51, gigabitethernet1
```

You can see that there is the route information of the ASBR1 loopback port in the global route table of PE1.

Note:

- For the checking method of PE2, ASBR2 , refer to PE1.

Step 3: Enable MPLS IP and IPv6 MPLS LDP.

#On PE1, enable the global MPLS IP and IPv6 MPLS LDP. Meanwhile, enable MPLS IP and IPv6 MPLS LDP on the interface.

```
PE1(config)#mpls ip
PE1(config)#mpls ldp
PE1(config-ldp)#router-id 1.1.1.1
PE1(config-ldp)#address-family ipv6
PE1(config-ldp-af6)#transport-address 1:1:1::1
PE1(config-ldp-af6)#exit
PE1(config-ldp)#exit
```

```
PE1(config)#interface gigabitethernet1
PE1(config-if-gigabitethernet1)#mpls ip
PE1(config-if-gigabitethernet1)#mpls ldp ipv6
PE1(config-if-gigabitethernet1)#exit
```

#On ASBR1, enable the global MPLS IP and IPv6 MPLS LDP. Meanwhile, enable MPLS IP and IPv6 MPLS LDP on the interface.

```
ASBR1(config)#mpls ip
ASBR1(config)#mpls ldp
ASBR1(config-ldp)#router-id 2.2.2.2
ASBR1(config-ldp)#address-family ipv6
ASBR1(config-ldp-af6)#transport-address 2:2:2::2
ASBR1(config-ldp-af6)#exit
ASBR1(config-ldp)#exit
ASBR1(config)#interface gigabitethernet0
ASBR1(config-if-gigabitethernet0)#mpls ip
ASBR1(config-if-gigabitethernet0)#mpls ldp ipv6
ASBR1(config-if-gigabitethernet0)#exit
```

#On ASBR2, enable the global MPLS IP and IPv6 MPLS LDP. Meanwhile, enable MPLS IP and IPv6 MPLS LDP on the interface.

```
ASBR2(config)#mpls ip
ASBR2(config)#mpls ldp
ASBR2(config-ldp)#router-id 3.3.3.3
ASBR2(config-ldp)#address-family ipv6
ASBR2(config-ldp-af6)#transport-address 3:3:3::3
ASBR2(config-ldp-af6)#exit
ASBR2(config-ldp)#exit
ASBR2(config)#interface gigabitethernet1
ASBR2(config-if-gigabitethernet1)#mpls ip
ASBR2(config-if-gigabitethernet1)#mpls ldp ipv6
ASBR2(config-if-gigabitethernet1)#exit
```

#On PE2, enable the global MPLS IP and IPv6 MPLS LDP. Meanwhile, enable MPLS IP and IPv6 MPLS LDP on the interface.

```
PE2(config)#mpls ip
PE2(config)#mpls ldp
PE2(config-ldp)#router-id 4.4.4.4
PE2(config-ldp)#address-family ipv6
PE2(config-ldp-af6)#transport-address 4:4:4::4
PE2(config-ldp-af6)#exit
```

```
PE2(config-ldp)#exit
PE2(config)#interface gigabitethernet0
PE2(config-if-gigabitethernet0)#mpls ip
PE2(config-if-gigabitethernet0)#mpls ldp ipv6
PE2(config-if-gigabitethernet0)#exit
```

#After the configuration is complete, view the LDP session information on the device.

Take PE1 as an example:

```
PE1#show mpls ldp ipv6 session
Peer IPv6 Address                Peer Type     My Role   State         DS Cap
DeadTime
2:2:2::2                         Multicast     Passive   OPERATIONAL   Disabled
00:02:06
Statistics for ldp ipv6 sessions:
    Multicast sessions: 1
    Targeted sessions: 0
```

You can see that PE1 sets up the LDP session with ASBR1 successfully.

#View the route label information on the device.

Take PE1 as an example:

```
PE1#show ipv6 route 2:2:2::2
Codes: C - Connected, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
    U - Per-user Static route
    O - OSPF, OE-OSPF External, M - Management

O   2:2:2::2/128 [110/1]
   via fe80::201:7aff:fe94:9a32 [1], label 3, 3d:00:02:50, gigabitethernet1
      fe80::201:7aff:fe94:9a32 [0], gigabitethernet1
```

You can see that the loopback port route from PE1 to ASBR1 has the label information.

Note:

- For the checking method of PE2, ASBR , refer to PE1.

Step 4: Configure the VPN instance and advertise the CE route to PE via IPv6 BGP.

#On CE1, configure IPv6 BGP.

```
CE1#configure terminal
CE1(config)#router bgp 65100
CE1(config-bgp)#bgp router-id 11.11.11.11
```

```
CE1(config-bgp)#address-family ipv6
CE1(config-bgp-af)#neighbor 2001:1::1 remote-as 100
CE1(config-bgp-af)#network 1::1/128
CE1(config-bgp-af)#exit-address-family
CE1(config-bgp)#exit
```

#On PE1, configure the VPN instance and IPv6 BGP in VPN.

```
PE1(config)#ip vrf 1
PE1(config-vrf)#rd 100:1
PE1(config-vrf)#route-target 100:1
PE1(config-vrf)#exit
PE1(config)#interface gigabitethernet0
PE1(config-if-gigabitethernet0)#ip vrf forwarding 1
PE1(config-if-gigabitethernet0)#ipv6 address 2001:1::1/64
PE1(config-if-gigabitethernet0)#exit
PE1(config)#router bgp 100
PE1(config-bgp)#address-family ipv6 vrf 1
PE1(config-bgp-af)#neighbor 2001:1::2 remote-as 65100
PE1(config-bgp-af)#exit-address-family
PE1(config-bgp)#exit
```

#On PE2, configure the VPN instance and IPv6 BGP in VPN.

```
PE2(config)#ip vrf 1
PE2(config-vrf)#rd 100:1
PE2(config-vrf)#route-target 100:1
PE2(config-vrf)#exit
PE2(config)#interface gigabitethernet1
PE2(config-if-gigabitethernet1)#ip vrf forwarding 1
PE2(config-if-gigabitethernet1)#ipv6 address 2001:2::1/64
PE2(config-if-gigabitethernet1)#exit
PE2(config)#router bgp 200
PE2(config-bgp)#address-family ipv6 vrf 1
PE2(config-bgp-af)#neighbor 2001:2::2 remote-as 65200
PE2(config-bgp-af)#exit-address-family
PE2(config-bgp)#exit
```

#On CE2, configure IPv6 BGP.

```
CE2#configure terminal
CE2(config)#router bgp 65200
CE2(config-bgp)#bgp router-id 22.22.22.22
```

```
CE2(config-bgp)#address-family ipv6
CE2(config-bgp-af)#neighbor 2001:2::1 remote-as 200
CE2(config-bgp-af)#network 2::2/128
CE2(config-bgp-af)#exit-address-family
CE2(config-bgp)#exit
```

#After configuration, view the VPN route table.

Take PE1 as an example:

```
PE1#show ipv6 route vrf 1
Codes: C - Connected, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
    U - Per-user Static route
    O - OSPF, OE-OSPF External, M - Management
```

```
B   1::1/128 [20/0]
    via 2001:1::2, 02:42:12, gigabitethernet0
C   2001:1::/64 [0/0]
    via ::, 03:28:51, gigabitethernet0
L   2001:1::1/128 [0/0]
    via ::, 03:28:51, gigabitethernet0
```

You can see that the VPN1 route table of PE1 has the route to CE1.

Note:

- For the checking method of PE2, refer to PE1.

Step 5: Configure MP-IBGP between PE and ASBR, and use the loopback interface as the peer address; Configure MP-EBGP between ASBRs.

#On PE1, configure MP-IBGP, enable the VPNv6 address family.

```
PE1(config)#router bgp 100
PE1(config-bgp)#neighbor 2:2:2::2 remote-as 100
PE1(config-bgp)#neighbor 2:2:2::2 update-source loopback0
PE1(config-bgp)#address-family vpnv6
PE1(config-bgp-af)#neighbor 2:2:2::2 activate
PE1(config-bgp-af)#exit-address-family
PE1(config-bgp-af)#exit
```

#On ASBR1, configure MP-IBGP with PE1, configure MP-EBGP between ASBR1 and ASBR2, and enable VPNv6 address family.

```
ASBR1(config)#router bgp 100
ASBR1(config-bgp)#neighbor 30::2 remote-as 200
```

```
ASBR1(config-bgp)#neighbor 1:1:1::1 remote-as 100
ASBR1(config-bgp)#neighbor 1:1:1::1 update-source loopback0
ASBR1(config-bgp)#address-family vpnv6
ASBR1(config-bgp-af)#neighbor 30::2 activate
ASBR1(config-bgp-af)#neighbor 1:1:1::1 activate
ASBR1(config-bgp-af)#neighbor 1:1:1::1 next-hop-self
ASBR1(config-bgp-af)#exit-address-family
ASBR1(config-bgp)#exit
```

#On ASBR2, configure MP-IBGP with PE2, configure MP-EBGP between ASBR1 and ASBR2, and enable VPNv6 address family.

```
ASBR2(config)#router bgp 200
ASBR2(config-bgp)#neighbor 30::1 remote-as 100
ASBR2(config-bgp)#neighbor 4:4:4::4 remote-as 200
ASBR2(config-bgp)#neighbor 4:4:4::4 update-source loopback0
ASBR2(config-bgp)#address-family vpnv6
ASBR2(config-bgp-af)#neighbor 30::1 activate
ASBR2(config-bgp-af)#neighbor 4:4:4::4 activate
ASBR2(config-bgp-af)#neighbor 4:4:4::4 next-hop-self
ASBR2(config-bgp-af)#exit-address-family
ASBR2(config-bgp)#exit
```

#On PE2, configure MP-IBGP, enable the VPNv6 address family.

```
PE2(config)#router bgp 200
PE2(config-bgp)#neighbor 3:3:3::3 remote-as 200
PE2(config-bgp)#neighbor 3:3:3::3 update-source loopback0
PE2(config-bgp)#address-family vpnv6
PE2(config-bgp-af)#neighbor 3:3:3::3 activate
PE2(config-bgp-af)#exit-address-family
PE2(config-bgp)#exit
```

Step 6: Check the result.

#After configuration, view the BGP neighbor information on the PE and ASBR.

Take PE1 and ASBR1 as an example:

```
PE1#show bgp vpnv6 unicast all summary
BGP router identifier 1.1.1.1, local AS number 100
BGP table version is 3
2 BGP AS-PATH entries
0 BGP community entries
```

```
Neighbor        V         AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
2:2:2::2        4        100       3       3        2    0    0 00:01:09        1

Total number of neighbors 1
BGP VRF 1 Route Distinguisher:
100:1
BGP table version is 1
3 BGP AS-PATH entries
0 BGP community entries

Neighbor        V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
2001:1::2       4 65100     210     213        1    0    0 03:00:14        1

Total number of neighbors 1
```

The content of the State/PfxRcd list is displayed as number (the number of the route prefixes received from the neighbor), and you can see that PE1 and ASBR1 set up the BGP neighbor successfully.

```
ASBR1#show bgp vpnv6 unicast all summary
BGP router identifier 2.2.2.2, local AS number 100
BGP table version is 9
3 BGP AS-PATH entries
0 BGP community entries

Neighbor        V         AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
1:1:1::1        4        100      58      57        4    0    0 00:08:39        1
30::2           4        200      34      47        4    0    0 00:05:32        1

Total number of neighbors 2
```

The content of the State/PfxRcd list is displayed as number (the number of the route prefixes received from the neighbor), and you can see that ASBR1 and PE1, ASBR2 set up the BGP neighbor successfully.

#View the BGP VPNv6 route table on the PE and ASBR.

Take PE1, ASBR1 as an example:

```
PE1#show bgp vpnv6 unicast vrf 1
BGP table version is 10, local router ID is 1.1.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
```

```
    Network          Next Hop          Metric     LocPrf Weight Path
Route Distinguisher: 100:1 (Default for VRF 1)
[B]*> 1::1/128          2001:1::2              0              0 65100 i
[B]*>i2::2/128          2:2:2::2               0      100     0 200 65200 i

ASBR1#show bgp vpnv6 unicast all
BGP table version is 9, local router ID is 2.2.2.2
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
    Network          Next Hop          Metric     LocPrf Weight Path
Route Distinguisher: 100:1
[B]*>i1::1/128          1:1:1::1         0       100      0 65100 i
[B]*> 2::2/128          30::2(fe80::201:7aff:fe99:c735)
                                         0              0 200 65200 i
```

You can see that there is the BGP route information to the peer CE2 in the BGP VPNv6 route table of PE1 and ASBR1.

#View the MPLS forwarding table on the PE and ASBR.

Take PE1, ASBR1 as an example:

```
PE1#show mpls forwarding-table
Pro: L - LDP, O - OSPF, B - MP-BGP, R - RSVP, M - Mapped-Route, S - Static
Label,ML - mLDP (ML FEC: Root address/OT/OV), RM - RSVP P2MP (RM FEC: P2MP
ID/TID)

Pro Ident        FEC             Inlabel Outlabel Outgoing            Next hop
B   1            ::/0            24000   /        /                   ::

ASBR1#show mpls forwarding-table
Pro: L - LDP, O - OSPF, B - MP-BGP, R - RSVP, M - Mapped-Route, S - Static
Label,ML - mLDP (ML FEC: Root address/OT/OV), RM - RSVP P2MP (RM FEC: P2MP
ID/TID)

Pro Ident        FEC             Inlabel Outlabel Outgoing            Next hop
B   global       1::1/128        24000   24000    gigabitethernet0    1:1:1::1
B   global       2::2/128        24001   24000    gigabitethernet1    30::2
```

You can see that there is the route label information of VPN1 in the MPLS forwarding table of PE1 and ASBR1.

Note:

- For the checking method of PE2, ASBR2 , refer to PE1, ASBR1.

#View the route table on the device.

Take PE1, CE1 as an example:

```
PE1#show ipv6 route vrf 1
Codes: C - Connected, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
     U - Per-user Static route
     O - OSPF, OE-OSPF External, M - Management



B   1::1/128 [20/0]
    via 2001:1::2, 16:21:29, gigabitethernet0
B   2::2/128 [200/0]
    via 2:2:2::2, 00:15:51, gigabitethernet1
C   2001:1::/64 [0/0]
    via ::, 17:08:07, gigabitethernet0
L   2001:1::1/128 [0/0]
    via ::, 17:08:07, gigabitethernet0

PE1#show ipv6 route vrf 1 2::2/128
Codes: C - Connected, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
     U - Per-user Static route
     O - OSPF, OE-OSPF External, M - Management



B   2::2/128 [200/0]
    via 2:2:2::2 [0], label 24000, 12:08:30, gigabitethernet1
       fe80::201:7aff:fe94:9a32 [2], label 3, gigabitethernet1
```

You can see that there is the route information to the peer CE2 in the VPN1 route table of PE1, the VPN label of the route is 24000, and the global label is 3.

```
CE1#show ipv6 route
Codes: C - Connected, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
     U - Per-user Static route
     O - OSPF, OE-OSPF External, M - Management
```

```
L   ::1/128 [0/0]
    via ::, 1d:23:59:08, lo0
LC  1::1/128 [0/0]
    via ::, 17:19:10, loopback0
B   2::2/128 [20/0]
    via 2001:1::1, 00:17:03, gigabitethernet0
C   2001:1::/64 [0/0]
    via ::, 17:09:51, gigabitethernet0
L   2001:1::2/128 [0/0]
    via ::, 17:09:51, gigabitethernet0
```

You can see that there is the route information to the peer CE2 in the route table of CE1.

#On CE1, ping the loopback port of CE2 and view whether the ping can be connected.

```
CE1#ping ipv6 2::2 -s 1::1

Press key (ctrl + shift + 6) interrupt it.
Reply from  2::2: bytes = 76  time < 16 ms
Reply from  2::2: bytes = 76  time < 16 ms
Reply from  2::2: bytes = 76  time < 16 ms
Reply from  2::2: bytes = 76  time < 16 ms
Reply from  2::2: bytes = 76  time < 16 ms
Success rate is 100% (5/5). Round-trip min/avg/max = 0/0/0 ms.
```

You can see that CE1 can ping CE2.

7.3.7. Configure VPNv6 Route Reflector (Over IPv4 LSP)

Network Requirements

- Deploy IPv4 LDP in the backbone network.
- CE1 and CE2 belong to VPN1 at the same time and use IPv6 BGP to exchange the route information with the PE.
- PE1 and PE2 exchange the VPNv6 route information with RR via MP-IBGP.
- On the RR, configure PE1 and PE2 as the reflector client.

Network Topology

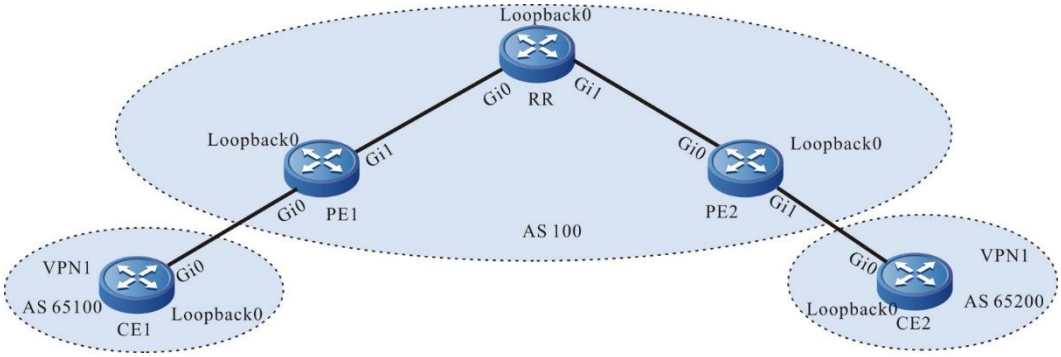

Figure 7-12 Configure VPNv6 route recflector

Device	Interface	IP Address	Device	Interface	IP Address
CE1	Gi0	2001:1::2/64	RR	Loopback0	2.2.2.2/32
	Loopback0	1::1/128	PE2	Gi0	20.0.0.2/24
PE1	Gi0	2001:1::1/64		Gi1	2001:2::1/64
	Gi1	10.0.0.1/24		Loopback0	3.3.3.3/32
	Loopback0	1.1.1.1/32	CE2	Gi0	2001:2::2/64
RR	Gi0	10.0.0.2/24		Loopback0	2::2/128
	Gi1	20.0.0.1/24			

Configuration Steps

Step 1: Configure the IP address of the interface (omitted).

Step 2: Configure the global OSPF and advertise the global route.

#Configure the global OSPF on PE1.

```
PE1#configure terminal
PE1(config)#router ospf 100
PE1(config-ospf)#network 1.1.1.1 0.0.0.0 area 0
PE1(config-ospf)#network 10.0.0.0 0.0.0.255 area 0
PE1(config-ospf)#exit
```

#Configure the global OSPF on RR.

```
RR#configure terminal
RR(config)#router ospf 100
```

```
RR(config-ospf)#network 10.0.0.0 0.0.0.255 area 0
RR(config-ospf)#network 20.0.0.0 0.0.0.255 area 0
RR(config-ospf)#network 2.2.2.2 0.0.0.0 area 0
RR(config-ospf)#exit
```

#Configure the global OSPF on PE2.

```
PE2#configure terminal
PE2(config)#router ospf 100
PE2(config-ospf)#network 2.2.2.2 0.0.0.0 area 0
PE2(config-ospf)#network 20.0.0.0 0.0.0.255 area 0
PE2(config-ospf)#exit
```

#After the configuration is complete, view the global route table on the device.

Take PE1 as an example:

```
PE1#show ip route
Codes: C - Connected, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
    U - Per-user Static route
    O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external



C   10.0.0.0/24 is directly connected, 00:39:30, gigabitethernet0
O   20.0.0.0/24 [110/2] via 10.0.0.2, 00:11:15, gigabitethernet0
C   127.0.0.0/8 is directly connected, 1w2d:07:04:57, lo0
C   1.1.1.1/32 is directly connected, 00:39:09, loopback0
O   2.2.2.2/32 [110/3] via 10.0.0.2, 00:00:03, gigabitethernet0
O   3.3.3.3/32 [110/2] via 10.0.0.2, 00:00:44, gigabitethernet0
```

You can see that there is the route information of the RR and PE2 loopback ports in the global route table of PE1.

Note:

- For the checking method of RR, PE2, refer to PE1..

Step 3: Enable MPLS IP and MPLS LDP.

#On PE1, enable the global MPLS IP and MPLS LDP. Meanwhile, enable MPLS IP and MPLS LDP on the interface.

```
PE1(config)#mpls ip
PE1(config)#mpls ldp
PE1(config-ldp)#router-id 1.1.1.1
PE1(config-ldp)#address-family ipv4
PE1(config-ldp-af4)#transport-address 1.1.1.1.
```

```
PE1(config-ldp-af4)#exit
PE1(config-ldp)#exit
PE1(config)#interface gigabitethernet1
PE1(config-if-gigabitethernet1)#mpls ip
PE1(config-if-gigabitethernet1)#mpls ldp
PE1(config-if-gigabitethernet1)#exit
```

#On RR, enable the global MPLS IP and MPLS LDP. Meanwhile, enable MPLS IP and MPLS LDP on the interface.

```
RR(config)#mpls ip
RR(config)#mpls ldp
RR(config-ldp)#router-id 2.2.2.2
RR(config-ldp)#address-family ipv4
RR(config-ldp-af4)#transport-address 2.2.2.2
RR(config-ldp-af4)#exit
RR(config-ldp)#exit
RR(config)#interface gigabitethernet0
RR(config-if-gigabitethernet0)#mpls ip
RR(config-if-gigabitethernet0)#mpls ldp
RR(config-if-gigabitethernet0)#exit
RR(config)#interface gigabitethernet1
RR(config-if-gigabitethernet1)#mpls ip
RR(config-if-gigabitethernet1)#mpls ldp
RR(config-if-gigabitethernet1)#exit
```

#On PE2, enable the global MPLS IP and MPLS LDP. Meanwhile, enable MPLS IP and MPLS LDP on the interface.

```
PE2(config)#mpls ip
PE2(config)#mpls ldp
PE2(config-ldp)#router-id 3.3.3.3
PE2(config-ldp)#address-family ipv4
PE2(config-ldp-af4)#transport-address 3.3.3.3
PE2(config-ldp-af4)#exit
PE2(config-ldp)#exit
PE2(config)#interface gigabitethernet0
PE2(config-if-gigabitethernet0)#mpls ip
PE2(config-if-gigabitethernet0)#mpls ldp
PE2(config-if-gigabitethernet0)#exit
```

Note:

- router-id and transport-address can be configured manually and also can be generated automatically. Usually, they are configured the same. If not configuring router-id and transport-address manually, the device will select automatically. From the up interfaces, first select the Loopback interface with the maximum IP address. If the device does not configure the Loopback interface address, select the common interface with the maximum IP address.

#After the configuration is complete, view the LDP session information on the device.

Take PE1 as an example:

```
PE1#show mpls ldp session
Peer IP Address    Peer Type    My Role   State        DS Cap    DeadTime
2.2.2.2            Multicast    Passive   OPERATIONAL  Disabled  00:02:20
Statistics for ldp sessions:
    Multicast sessions: 1
    Targeted sessions: 0
```

You can see that PE1 and RR set up the LDP session successfully.

#View the route label information on the device.

Take PE1 as an example:

```
PE1#show ip route 2.2.2.2 detail
Codes: C - Connected, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
    U - Per-user Static route
    O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external



O   2.2.2.2/32 [110/2] via 10.0.0.2, label 3, 00:5:23, gigabitethernet1
                       10.0.0.2 [0], gigabitethernet1

PE1#show ip route 3.3.3.3 detail
Codes: C - Connected, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
    U - Per-user Static route
    O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external



O   3.3.3.3/32 [110/2] via 10.0.0.2, label 24001, 00:5:23, gigabitethernet1
                       10.0.0.2 [0], gigabitethernet1
```

You can see that the loopback port route from PE1 to RR, PE2 has the label information.

Note:

- For the checking method of RR and PE2, refer to PE1.

Step 4: Configure the VPN instance and advertise the CE route to the PE via IPv6 BGP.

#On PE1, configure the VPN instance and IPv6 BGP in VPN1.

```
PE1(config)#ip vrf 1
PE1(config-vrf)#rd 100:1
PE1(config-vrf)#route-target 100:1
PE1(config-vrf)#exit
PE1(config)#interface gigabitethernet0
PE1(config-if-gigabitethernet0)#ip vrf forwarding 1
PE1(config-if-gigabitethernet0)#ipv6 address 2001:1::1/64
PE1(config-if-gigabitethernet0)#exit
PE1(config-bgp)#address-family ipv6 vrf 1
PE1(config-bgp-af)#neighbor 2001:1::2 remote-as 65100
PE1(config-bgp-af)#exit-address-family
PE1(config-bgp)#exit
```

#On CE1, configure IPv6 BGP.

```
CE1#configure terminal
CE1(config)#router bgp 65100
CE1(config-bgp)#bgp router-id 11.11.11.11
CE1(config-bgp)#address-family ipv6
CE1(config-bgp-af)#neighbor 2001:1::1 remote-as 100
CE1(config-bgp-af)#network 1::1/128
CE1(config-bgp-af)#exit-address-family
CE1(config-bgp)#exit
```

#On PE2, configure the VPN instance and configure IPv6 BGP in VPN1.

```
PE2(config)#ip vrf 1
PE2(config-vrf)#rd 100:1
PE2(config-vrf)#route-target 100:1
PE2(config-vrf)#exit
PE2(config)#interface gigabitethernet1
PE2(config-if-gigabitethernet1)#ip vrf forwarding 1
PE2(config-if-gigabitethernet1)#ipv6 address 2001:2::1/64
PE2(config-if-gigabitethernet1)#exit
PE2(config-bgp)#address-family ipv6 vrf 1
```

```
PE2(config-bgp-af)#neighbor 2001:2::2 remote-as 65200
PE2(config-bgp-af)#exit-address-family
PE2(config-bgp)#exit
```

#On CE2, configure IPv6 BGP.

```
CE2#configure terminal
CE2(config)#router bgp 65200
CE2(config-bgp)#bgp router-id 33.33.33.33
CE2(config-bgp)#address-family ipv6
CE2(config-bgp-af)#neighbor 2001:2::1 remote-as 100
CE2(config-bgp-af)#network 2::2/128
CE2(config-bgp-af)#exit-address-family
CE2(config-bgp)#exit
```

#After the configuration is complete, view the IPv6 BGP neighbor information on the PE.

Take PE1 as an example:

```
PE1#show bgp vpnv6 unicast all summary
BGP router identifier 1.1.1.1, local AS number 100
BGP VRF 1 Route Distinguisher:
100:1
BGP table version is 1
2 BGP AS-PATH entries
0 BGP community entries

Neighbor        V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
2001:1::2       4 65100      27      27        1    0    0 00:21:15        1

Total number of neighbors 1
```

The content of the State/PfxRcd list is displayed as number (the number of the route prefixes received from the neighbor), and you can see that PE1 and CE1 set up the IPv6 BGP neighbor successfully.

#View the BGP VPNv6 route table and VPN route table on the PE.

Take PE1 as an example:

```
PE1#show bgp vpnv6 unicast vrf 1
BGP table version is 12, local router ID is 1.1.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network          Next Hop            Metric     LocPrf Weight Path
```

```
Route Distinguisher: 100:1 (Default for VRF 1)
[B]*> 1::1/128          2001:1::2              0             0 65100 i

PE1#show ipv6 route vrf 1
Codes: C - Connected, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management



B   1::1/128 [20/0]
    via 2001:1::2, 17:37:49, gigabitethernet0
C   2001:1::/64 [0/0]
    via ::, 18:24:27, gigabitethernet0
L   2001:1::1/128 [0/0]
    via ::, 18:24:27, gigabitethernet0
```

You can see that there is the route to CE1 in the VPN1 route table of PE1.

Note:

- For the checking method of PE2, refer to PE1.

Step 5: Configure MP-IBGP, and use the loopback interface as the peer address.

#On PE1, configure MP-IBGP ane enable the VPNv6 address family.

```
PE1(config)#router bgp 100
PE1(config-bgp)#neighbor 2.2.2.2 remote-as 100
PE1(config-bgp)#neighbor 2.2.2.2 update-source loopback 0
PE1(config-bgp)#address-family vpnv6
PE1(config-bgp-af)#neighbor 2.2.2.2 activate
PE1(config-bgp-af)#exit-address-family
PE1(config-bgp)#exit
```

#On RR, configure MP-IBGP ane enable the VPNv6 address family.

```
RR(config)#router bgp 100
RR(config-bgp)#neighbor 1.1.1.1 remote-as 100
RR(config-bgp)#neighbor 1.1.1.1 update-source loopback 0
RR(config-bgp)#neighbor 3.3.3.3 remote-as 100
RR(config-bgp)#neighbor 3.3.3.3 update-source loopback 0
RR(config-bgp)#address-family vpnv6
RR(config-bgp-af)#neighbor 1.1.1.1 activate
```

```
RR(config-bgp-af)#neighbor 3.3.3.3 activate
RR(config-bgp-af)#exit-address-family
RR(config-bgp)#exit
```

#On PE2, configure MP-IBGP ane enable the VPNv6 address family.

```
PE2(config)#router bgp 100
PE2(config-bgp)#neighbor 2.2.2.2 remote-as 100
PE2(config-bgp)#neighbor 2.2.2.2 update-source loopback 0
PE2(config-bgp)#address-family vpnv6
PE2(config-bgp-af)#neighbor 2.2.2.2 activate
PE2(config-bgp-af)#exit-address-family
PE2(config-bgp)#exit
```

#After the configuration is complete, view the BGP neighbor information on the PE and RR.

Take PE1 as an example:

```
PE1#show bgp vpnv6 unicast all summary
BGP router identifier 1.1.1.1, local AS number 100
BGP table version is 12
2 BGP AS-PATH entries
0 BGP community entries

Neighbor        V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
2.2.2.2         4   100       3       4       12    0    0 00:01:44        0

Total number of neighbors 1
BGP VRF 1 Route Distinguisher:
100:1
BGP table version is 1
2 BGP AS-PATH entries
0 BGP community entries

Neighbor        V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
2001:1::2       4 65100    1230    1235        1    0    0 17:43:38        1

Total number of neighbors 1
```

The content of the Up/Down list is displayed as specific time (the time of the neighbor UP), and you can see that PE1 and RR set up the BGP neighbor successfully.

Note:

- For the checking method of RR and PE2, refer to PE1.

Step 6: On the RR, configure PE1 and PE2 as the reflector client.

#On the RR, configure PE1 and PE2 as the reflector client.

```
RR(config)#router bgp 100
RR(config-bgp)#address-family vpnv6
RR(config-bgp-af)#neighbor 1.1.1.1 route-reflector-client
RR(config-bgp-af)#neighbor 3.3.3.3 route-reflector-client
RR(config-bgp-af)#exit-address-family
RR(config-bgp)#exit
```

Step 7: Check the result.

#On the PE, view the BGP VPNv6 route table and the VPN route table.

Take PE1 as an example:

```
PE1#show bgp vpnv6 unicast vrf 1
BGP table version is 13, local router ID is 1.1.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network          Next Hop            Metric     LocPrf Weight Path
Route Distinguisher: 100:1 (Default for VRF 1)
[B]*> 1::1/128          2001:1::2               0              0 65100 i
[B]*>i2::2/128          ::ffff:3.3.3.3          0       100    0 65200 i

PE1#show ipv6 route vrf 1
Codes: C - Connected, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management



B   1::1/128 [20/0]
    via 2001:1::2, 17:54:59, gigabitethernet0
B   2::2/128 [200/0]
    via ::ffff:3.3.3.3, 00:04:36, gigabitethernet1
C   2001:1::/64 [0/0]
    via ::, 18:41:37, gigabitethernet0
L   2001:1::1/128 [0/0]
    via ::, 18:41:37, gigabitethernet0
```

```
PE1#show ipv6 route vrf 1 2::2/128
Codes: C - Connected, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management



B   2::2/128 [200/0]
    via ::ffff:3.3.3.3 [0], label 5120, 00:05:10, gigabitethernet1
        ::ffff:10.0.0.2 [3], label 17, gigabitethernet1
```

You can see that there is the route information to the peer CE3 in the VPN1 route table of PE1, the VPN label of the route is 5120, and the global label is 24001.

You can see that there is the route information to the peer CE2 in the BGP VPNv6 route table of PE1 and VPN1 route table.

#On PE and RR, view the MPLS forwarding table.

Take PE1 as an example:

```
PE1#show mpls forwarding-table PE1#show mpls forwarding-table
Pro: L - LDP, O - OSPF, B - MP-BGP, R - RSVP, M - Mapped-Route, S - Static
Label,ML - mLDP (ML FEC: Root address/OT/OV), RM - RSVP P2MP (RM FEC: P2MP
ID/TID)



Pro Ident       FEC             Inlabel Outlabel Outgoing       Next hop
B   1           ::/0            25120   /       /               ::
```

You can see that there is the route label information of VPN1 in the MPLS forwarding table of PE1.

Note:

- For the checking method of RR and PE2, refer to PE1..

#On CE1, ping the loopback port of CE3 and view whether the ping can be connected.

```
CE1#ping ipv6 2::2 -s 1::1


Press key (ctrl + shift + 6) interrupt it.
Reply from  2::2: bytes = 76  time < 16 ms
Reply from  2::2: bytes = 76  time < 16 ms
Reply from  2::2: bytes = 76  time < 16 ms
Reply from  2::2: bytes = 76  time < 16 ms
Reply from  2::2: bytes = 76  time < 16 ms
```

```
Success rate is 100% (5/5). Round-trip min/avg/max = 0/0/0 ms.
```

You can see that CE1 can ping CE2.

7.3.8. Configure VPNv6 Route Reflector (Over IPv6 LSP)

Network Requirements

- Deploy IPv6 LDP in the backbone network.
- CE1 and CE2 belong to VPN1 at the same time and use IPv6 BGP to exchange the route information with the PE.
- PE1 and PE2 exchange the VPNv6 route information with RR via MP-IBGP.
- On the RR, configure PE1 and PE2 as the reflector client.

Network Topology

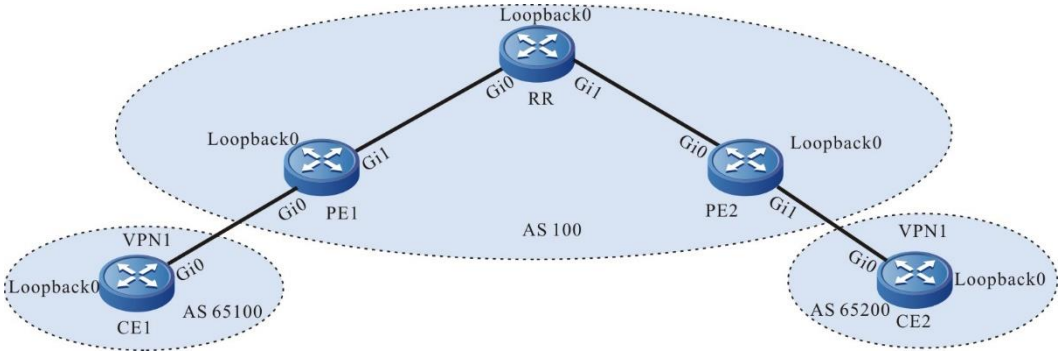

Figure 7-13 Configure VPNv6 route recflector

Device	Interface	IP Address	Device	Interface	IP Address
CE1	Gi0	2001:1::2/64	RR	Loopback0	2:2:2::2/128
	Loopback0	1::1/128	PE2	Gi0	20::2/24
PE1	Gi0	2001:1::1/64		Gi1	2001:2::1/64
	Gi1	10::1/64		Loopback0	3:3:3::3/32
	Loopback0	1:1:1::1/128	CE2	Gi0	2001:2::2/64
RR	Gi0	10::2/64		Loopback0	2::2/128
	Gi1	20::1/64			

Configuration Steps

Step 1: Configure the IP address of the interface (omitted).

Step 2: Configure the global OSPF and advertise the global route.

#Configure the global OSPF on PE1.

```
PE1#configure terminal
PE1(config)#ipv6 router ospf 100
PE1(config-ospf6)#router-id 1.1.1.1
PE1(config-ospf6)#exit
PE1(config)#interface loopback 0
PE1(config-if-loopback0)#ipv6 router ospf 100 area 0
PE1(config-if-loopback0)#exit
PE1(config)#interface gigabitethernet 0
PE1(config-if-gigabitethernet0)#ipv6 router ospf 100 area 0
PE1(config-if-gigabitethernet0)#exit
PE1(config)#interface gigabitethernet 1
PE1(config-if-gigabitethernet1)#ipv6 router ospf 100 area 0
PE1(config-if-gigabitethernet1)#exit
```

#Configure the global OSPF on RR.

```
RR#configure terminal
RR(config)#ipv6 router ospf 100
RR(config-ospf6)#router-id 2.2.2.2
RR(config-ospf6)#exit
RR(config)#interface loopback 0
RR(config-if-loopback0)#ipv6 router ospf 100 area 0
RR(config-if-loopback0)#exit
RR(config)#interface gigabitethernet 0
RR(config-if-gigabitethernet0)#ipv6 router ospf 100 area 0
RR(config-if-gigabitethernet0)#exit
RR(config)#interface gigabitethernet 1
RR(config-if-gigabitethernet1)#ipv6 router ospf 100 area 0
RR(config-if-gigabitethernet1)#exit
```

#Configure the global OSPF on PE2.

```
PE2#configure terminal
PE2(config)#ipv6 router ospf 100
PE2(config-ospf6)#router-id 3.3.3.3
PE2(config-ospf6)#exit
PE2(config)#interface gigabitethernet 0
PE2(config-if-gigabitethernet0)#ipv6 router ospf 100 area 0
```

```
PE2(config-if-gigabitethernet0)#exit
```

#After the configuration is complete, view the global route table on the device.

Take PE1 as an example:

```
PE1#show ipv6 route
Codes: C - Connected, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management




L   ::1/128 [0/0]
       via ::, 3d:00:05:42, lo0
LC  1:1:1::1/128 [0/0]
       via ::, 3d:00:04:55, loopback0
O   2:2:2::2/128 [110/1]
       via fe80::201:7aff:fe94:9a32, 3d:00:00:56, gigabitethernet1
O   3:3:3::3/128 [110/2]
       via fe80::201:7aff:fe94:9a32, 3d:00:00:56, gigabitethernet1
C   10::/64 [0/0]
       via ::, 3d:00:01:51, gigabitethernet1
L   10::1/128 [0/0]
       via ::, 3d:00:01:51, gigabitethernet1
```

You can see that there is the route information of RR and PE2 loopback port in the global route table of PE1.

Note:

- For the checking method of RR, PE2, refer to PE1.

Step 3: Enable MPLS IP and IPv6 MPLS LDP.

#On PE1, enable the global MPLS IP and IPv6 MPLS LDP. Meanwhile, enable MPLS IP and IPv6 MPLS LDP on the interface.

```
PE1(config)#mpls ip
PE1(config)#mpls ldp
PE1(config-ldp)#router-id 1.1.1.1
PE1(config-ldp)#address-family ipv6
PE1(config-ldp-af6)#transport-address 1:1:1::1
PE1(config-ldp-af6)#exit
PE1(config-ldp)#exit
PE1(config)#interface gigabitethernet1
```

```
PE1(config-if-gigabitethernet1)#mpls ip
PE1(config-if-gigabitethernet1)#mpls ldp ipv6
PE1(config-if-gigabitethernet1)#exit
```

#On RR, enable the global MPLS IP and MPLS LDP. Meanwhile, enable MPLS IP and MPLS LDP on the interface.

```
RR(config)#mpls ip
RR(config)#mpls ldp
RR(config-ldp)#router-id 2.2.2.2
RR(config-ldp)#address-family ipv6
RR(config-ldp-af6)#transport-address 2:2:2::2
RR(config-ldp-af6)#exit
RR(config-ldp)#exit
RR(config)#interface gigabitethernet0
RR(config-if-gigabitethernet0)#mpls ip
RR(config-if-gigabitethernet0)#mpls ldp ipv6
RR(config-if-gigabitethernet0)#exit
RR(config)#interface gigabitethernet1
RR(config-if-gigabitethernet1)#mpls ip
RR(config-if-gigabitethernet1)#mpls ldp ipv6
RR(config-if-gigabitethernet1)#exit
```

#On PE2, enable the global MPLS IP and MPLS LDP. Meanwhile, enable MPLS IP and MPLS LDP on the interface.

```
PE2(config)#mpls ip
PE2(config)#mpls ldp
PE2(config-ldp)#router-id 3.3.3.3
PE2(config-ldp)#address-family ipv6
PE2(config-ldp-af6)#transport-address 3:3:3::3
PE2(config-ldp-af6)#exit
PE2(config-ldp)#exit
PE2(config)#interface gigabitethernet0
PE2(config-if-gigabitethernet0)#mpls ip
PE2(config-if-gigabitethernet0)#mpls ldp ipv6
PE2(config-if-gigabitethernet0)#exit
```

Note:

- router-id and transport-address can be configured manually and also can be generated automatically. Usually, they are configured the same. If not configuring router-id and transport-address manually, the device will select automatically. From the up interfaces, first select the Loopback interface with the maximum IP address. If the device does not

configure the Loopback interface address, select the common interface with the maximum IP address.

#After the configuration is complete, view the LDP session information on the device.

Take PE1 as an example:

```
PE1#show mpls ldp ipv6 session
Peer IPv6 Address                Peer Type     My Role   State         DS Cap
DeadTime
2:2:2::2                         Multicast     Passive   OPERATIONAL   Disabled
00:02:06
Statistics for ldp ipv6 sessions:
    Multicast sessions: 1
    Targeted sessions: 0
```

You can see that PE1 and RR set up the LDP session successfully.

#View the route label information on the device.

Take PE1 as an example:

```
PE1#show ipv6 route 2:2:2::2
Codes: C - Connected, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
    U - Per-user Static route
    O - OSPF, OE-OSPF External, M - Management

O   2:2:2::2/128 [110/1]
    via fe80::201:7aff:fe94:9a32 [1], label 3, 3d:00:02:50, gigabitethernet1
      fe80::201:7aff:fe94:9a32 [0], gigabitethernet1
PE1#show ipv6 route 3:3:3::3/128
Codes: C - Connected, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
    U - Per-user Static route
    O - OSPF, OE-OSPF External, M - Management

O   3:3:3::3/128 [110/2]
    via fe80::201:7aff:fe94:9a32 [1], label 24001, 3d:00:02:50, gigabitethernet1
      fe80::201:7aff:fe94:9a32 [0], gigabitethernet1
```

You can see that the loopback port route from PE1 to RR, PE2 has the label information.

Note:

- For the checking method of RR, PE2, refer to PE1.

Step 4: Configure the VPN instance and advertise the CE route to PE via IPv6 BGP.

#On PE1, configure the VPN instance and IPv6 BGP in VPN1.

```
PE1(config)#ip vrf 1
PE1(config-vrf)#rd 100:1
PE1(config-vrf)#route-target 100:1
PE1(config-vrf)#exit
PE1(config)#interface gigabitethernet0
PE1(config-if-gigabitethernet0)#ip vrf forwarding 1
PE1(config-if-gigabitethernet0)#ipv6 address 2001:1::1/64
PE1(config-if-gigabitethernet0)#exit
PE1(config-bgp)#address-family ipv6 vrf 1
PE1(config-bgp-af)#neighbor 2001:1::2 remote-as 65100
PE1(config-bgp-af)#exit-address-family
PE1(config-bgp)#exit
```

#On CE1, configure IPv6 BGP.

```
CE1#configure terminal
CE1(config)#router bgp 65100
CE1(config-bgp)#bgp router-id 11.11.11.11
CE1(config-bgp)#address-family ipv6
CE1(config-bgp-af)#neighbor 2001:1::1 remote-as 100
CE1(config-bgp-af)#network 1::1/128
CE1(config-bgp-af)#exit-address-family
CE1(config-bgp)#exit
```

#On PE2, configure the VPN instance and IPv6 BGP in VPN1.

```
PE2(config)#ip vrf 1
PE2(config-vrf)#rd 100:1
PE2(config-vrf)#route-target 100:1
PE2(config-vrf)#exit
PE2(config)#interface gigabitethernet1
PE2(config-if-gigabitethernet1)#ip vrf forwarding 1
PE2(config-if-gigabitethernet1)#ipv6 address 2001:2::1/64
PE2(config-if-gigabitethernet1)#exit
PE2(config-bgp)#address-family ipv6 vrf 1
PE2(config-bgp-af)#neighbor 2001:2::2 remote-as 65200
```

```
PE2(config-bgp-af)#exit-address-family
PE2(config-bgp)#exit
```

#On CE2, configure IPv6 BGP.

```
CE2#configure terminal
CE2(config)#router bgp 65200
CE2(config-bgp)#bgp router-id 33.33.33.33
CE2(config-bgp)#address-family ipv6
CE2(config-bgp-af)#neighbor 2001:2::1 remote-as 100
CE2(config-bgp-af)#network 2::2/128
CE2(config-bgp-af)#exit-address-family
CE2(config-bgp)#exit
```

#After configuration, view the IPv6 BGP neighbor information on the PE.

Take PE1 as an example:

```
PE1#show bgp vpnv6 unicast all summary
BGP router identifier 1.1.1.1, local AS number 100
BGP VRF 1 Route Distinguisher:
100:1
BGP table version is 1
2 BGP AS-PATH entries
0 BGP community entries

Neighbor        V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
2001:1::2       4 65100      27      27        1    0    0 00:21:15        1

Total number of neighbors 1
```

The content of the State/PfxRcd list is displayed as number (the number of the route prefixes received from the neighbor), and you can see that PE1 and CE1 set up the IPv6 BGP neighbor successfully.

#On PE, view the BGP VPNv6 route table and VPn route table.

Take PE1 as an example:

```
PE1#show bgp vpnv6 unicast vrf 1
BGP table version is 12, local router ID is 1.1.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network          Next Hop            Metric     LocPrf Weight Path
Route Distinguisher: 100:1 (Default for VRF 1)
```

```
[B]*> 1::1/128          2001:1::2              0             0 65100 i

PE1#show ipv6 route vrf 1
Codes: C - Connected, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management



B   1::1/128 [20/0]
    via 2001:1::2, 17:37:49, gigabitethernet0
C   2001:1::/64 [0/0]
    via ::, 18:24:27, gigabitethernet0
L   2001:1::1/128 [0/0]
    via ::, 18:24:27, gigabitethernet0
```

You can see that there is the route to CE1 in the VPN1 route table of PE1.

Note:

- For the checking method of PE2, refer to PE1.

Step 5: Configure MP-IBGP, and use the loopback interface as the peer address.

#On PE1, configure MP-IBGP, enable the VPNv6 address family.

```
PE1(config)#router bgp 100
PE1(config-bgp)#neighbor 2:2:2::2 remote-as 100
PE1(config-bgp)#neighbor 2:2:2::2 update-source loopback 0
PE1(config-bgp)#address-family vpnv6
PE1(config-bgp-af)#neighbor 2:2:2::2 activate
PE1(config-bgp-af)#exit-address-family
PE1(config-bgp)#exit
```

#On RR, configure MP-IBGP, enable the VPNv6 address family.

```
RR(config)#router bgp 100
RR(config-bgp)#neighbor 1:1:1::1 remote-as 100
RR(config-bgp)#neighbor 1:1:1::1 update-source loopback 0
RR(config-bgp)#neighbor 3:3:3::3 remote-as 100
RR(config-bgp)#neighbor 3:3:3::3 update-source loopback 0
RR(config-bgp)#address-family vpnv6
RR(config-bgp-af)#neighbor 1:1:1::1 activate
RR(config-bgp-af)#neighbor 3:3:3::3 activate
```

```
RR(config-bgp-af)#exit-address-family
RR(config-bgp)#exit
```

#On PE2, configure MP-IBGP, enable the VPNv6 address family.

```
PE2(config)#router bgp 100
PE2(config-bgp)#neighbor 2:2:2::2 remote-as 100
PE2(config-bgp)#neighbor 2:2:2::2 update-source loopback 0
PE2(config-bgp)#address-family vpnv6
PE2(config-bgp-af)#neighbor 2:2:2::2 activate
PE2(config-bgp-af)#exit-address-family
PE2(config-bgp)#exit
```

#After configuration, view the BGP neighbor information on the PE and RR.

Take PE1 as an example:

```
PE1#show bgp vpnv6 unicast all summary
BGP router identifier 1.1.1.1, local AS number 100
BGP table version is 12
2 BGP AS-PATH entries
0 BGP community entries

Neighbor      V      AS MsgRcvd MsgSent  TblVer  InQ OutQ Up/Down  State/PfxRcd
2:2:2::2      4      100     13     24      12    0    0 00:01:09        0

Total number of neighbors 1
BGP VRF 1 Route Distinguisher:
100:1
BGP table version is 1
2 BGP AS-PATH entries
0 BGP community entries

Neighbor      V      AS MsgRcvd MsgSent  TblVer  InQ OutQ Up/Down  State/PfxRcd
2001:2::2     4      200      3      4       1    0    0 00:00:18        1

Total number of neighbors 1
```

The content of the Up/Down list is displayed as specific time (the time of the neighbor UP), and you can see that PE1 and RR set up the BGP neighbor successfully.

Note:

- For the checking method of RR, PE2, refer to PE1.

Step 6: On RR, configure PE2, PE2 as the reflector client.

#On RR, configure PE2, PE2 as the reflector client.

```
RR(config)#router bgp 100
RR(config-bgp)#address-family vpnv6
RR(config-bgp-af)#neighbor 1:1:1::1 route-reflector-client
RR(config-bgp-af)#neighbor 3:3:3::3 route-reflector-client
RR(config-bgp-af)#exit-address-family
RR(config-bgp)#exit
```

Step 7: Check the result.

#On PE, view the BGP VPNv6 route table and VPn route table.

Take PE1 as an example:

```
PE1#show bgp vpnv6 unicast vrf 1
BGP table version is 13, local router ID is 1.1.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network          Next Hop            Metric     LocPrf Weight Path
Route Distinguisher: 100:1 (Default for VRF 1)
[B]*> 1::1/128           2001:1::2                0              0 65100 i
[B]*>i2::2/128           3:3:3::3                 0       100    0 65200 i

PE1#show ipv6 route vrf 1
Codes: C - Connected, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management



B   1::1/128 [20/0]
    via 2001:1::2, 17:54:59, gigabitethernet0
B   2::2/128 [200/0]
    via 3:3:3::3, 00:04:36, gigabitethernet1
C   2001:1::/64 [0/0]
    via ::, 18:41:37, gigabitethernet0
L   2001:1::1/128 [0/0]
    via ::, 18:41:37, gigabitethernet0
```

```
PE1#show ipv6 route vrf 1 2::2/128
Codes: C - Connected, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management



B   2::2/128 [200/0]
    via 3:3:3::3 [0], label 25120, 00:05:10, gigabitethernet1
      fe80::201:7aff:fe94:9a32 [3], label 24001, gigabitethernet1
```

You can see that there is the route information to the peer CE3 in the VPN1 route table of PE1, the VPN label of the route is 25120, and the global label is 24001.

You can see that there is the route information to the peer CE2 in the BGP VPNv6 route table of PE1 and VPN1 route table.

#On CE1, ping the loopback port of CE3, and view whether the ping can be connected.

```
CE1#ping ipv6 2::2 -s 1::1


Press key (ctrl + shift + 6) interrupt it.
Reply from  2::2: bytes = 76  time < 16 ms
Reply from  2::2: bytes = 76  time < 16 ms
Reply from  2::2: bytes = 76  time < 16 ms
Reply from  2::2: bytes = 76  time < 16 ms
Reply from  2::2: bytes = 76  time < 16 ms
Success rate is 100% (5/5). Round-trip min/avg/max = 0/0/0 ms.
```

You can see that CE1 can ping CE2.

7.3.9. Configure M-VRF

Network Requirements

- Deploy IPv4 LDP in the backbone network.
- MCE is the device used by the user for the VPN multi-instance exchange.
- Separate the routes of the user networks VPN1 and VPN2, the sites of the same VPN can communicate with each other, and the sites of different VPNs cannot communicate.
- CE1, CE3 are the sites of VPN1; CE2, CE4 are the sites of VPN2.
- PE1 and CE1 use IPv6 BGP to exchange the route information; PE1 and CE2 use OSPFv3 to exchange the route information.
- PEs use OSPF as IGP to communicate with each other, and configure MP-IBGP to exchange the VPNv6 route information.
- MCE and PE2 use OSPFv3 to exchange the route information; MCE and CE3, CE4 use the IPv6 static route to exchange the route information.

Network Topology

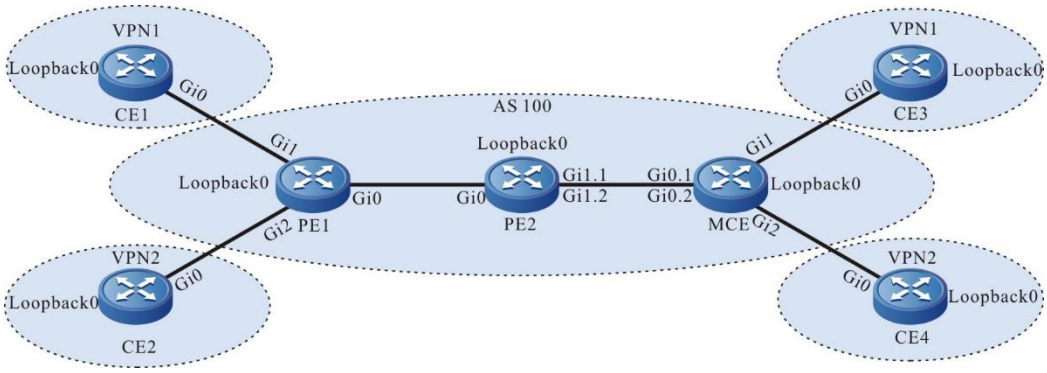

Figure 7-14 Networking of configuring M-VRF

Device	Interface	IP Address	Device	Interface	IP Address
CE1	Gi0	2001:1::2/64	PE2	Gi1.2	2001:4::1/64
	Loopback0	1::1/128		Loopback0	2.2.2.2/32
PE1	Gi0	10.0.0.1/24	MCE	Gi0.1	2001:3::2/64
	Gi1	2001:1::1/64		Gi0.2	2001:4::2/64
	Gi2	2001:2::1/64		Gi1	2001:5::1/64
	Loopback0	1.1.1.1/32		Gi2	2001:6::1/64
CE2	Gi0	2001:2::2/64	CE3	Gi0	2001:5::2/64
	Loopback0	2::2/128		Loopback0	3::3/128
PE2	Gi0	10.0.0.2/24	CE4	Gi0	2001:6::2/64
	Gi1.1	2001:3::1/64		Loopback0	4::4/128

Configuration Steps

Step 1: Configure the IP address of the interface (omitted).

Step 2: Configure the global OSPF and advertise the global route.

#Configure the global OSPF on PE1.

```
PE1#configure terminal
PE1(config)#router ospf 100
```

```
PE1(config-ospf)#network 10.0.0.0 0.0.0.255 area 0
PE1(config-ospf)#network 1.1.1.1 0.0.0.0 area 0
PE1(config-ospf)#exit
```

#Configure the global OSPF on PE2.

```
PE2#configure terminal
PE2(config)#router ospf 100
PE2(config-ospf)#network 10.0.0.0 0.0.0.255 area 0
PE2(config-ospf)#network 2.2.2.2 0.0.0.0 area 0
PE2(config-ospf)#exit
```

#After the configuration is complete, view the global route table on the device.

Take PE1 as an example:

```
PE1#show ip route
Codes: C - Connected, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
    U - Per-user Static route
    O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external



C   10.0.0.0/24 is directly connected, 00:04:27, gigabitethernet0
C   127.0.0.0/8 is directly connected, 1w3d:06:22:09, lo0
C   1.1.1.1/32 is directly connected, 00:01:06, loopback0
O   2.2.2.2/32 [110/2] via 10.0.0.2, 00:00:02, gigabitethernet0
```

You can see that there is the route information of the PE2 loopback port in the global route table of PE1.

Note:

- For the checking method of PE2, refer to PE1.

Step 3: Enable MPLS IP and MPLS LDP.

#On PE1, enable the global MPLS IP and MPLS LDP. Meanwhile, enable MPLS IP and MPLS LDP on the interface.

```
PE1(config)#mpls ip
PE1(config)#mpls ldp
PE1(config-ldp)#router-id 1.1.1.1
PE1(config-ldp)#address-family ipv4
PE1(config-ldp-af4)#transport-address 1.1.1.1
PE1(config-ldp-af4)#exit
PE1(config-ldp)#exit
PE1(config)#interface gigabitethernet0
```

```
PE1(config-if-gigabitethernet0)#mpls ip
PE1(config-if-gigabitethernet0)#mpls ldp
PE1(config-if-gigabitethernet0)#exit
```

#On PE2, enable the global MPLS IP and MPLS LDP. Meanwhile, enable MPLS IP and MPLS LDP on the interface.

```
PE2(config)#mpls ip
PE2(config)#mpls ldp
PE2(config-ldp)#router-id 2.2.2.2
PE2(config-ldp)#address-family ipv4
PE2(config-ldp-af4)#transport-address 2.2.2.2
PE2(config-ldp-af4)#exit
PE2(config-ldp)#exit
PE2(config)#interface gigabitethernet0
PE2(config-if-gigabitethernet0)#mpls ip
PE2(config-if-gigabitethernet0)#mpls ldp
PE2(config-if-gigabitethernet0)#exit
```

#After the configuration is complete, view the LDP session information on the device.

Take PE1 as an example:

```
PE1#show mpls ldp session
Peer IP Address    Peer Type    My Role   State        DS Cap   DeadTime
2.2.2.2            Multicast    Passive   OPERATIONAL  Disabled 00:02:20
Statistics for ldp sessions:
    Multicast sessions: 1
    Targeted sessions: 0
```

You can see that PE1 and PE2 set up the LDP session successfully.

#View the route label information on the device.

Take PE1 as an example:

```
PE1#show ip route 2.2.2.2 detail
Codes: C - Connected, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
    U - Per-user Static route
    O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external



O   2.2.2.2/32 [110/2] via 10.0.0.2, label 3, 00:5:23, gigabitethernet0
                       10.0.0.2 [0], gigabitethernet0
```

You can see that the loopback port route from PE1 to PE2 has the label information.

Note:

- For the checking method of PE2, refer to PE1.

Step 4: Configure the VPN instance, and advertise the CE1, CE2 route to PE1.

#On PE1, configure the VPN instance, configure IPv6 BGP in VPN1, and configure OSPFv3 in VPN2.

```
PE1(config)#ip vrf 1
PE1(config-vrf)#rd 100:1
PE1(config-vrf)#route-target 100:1
PE1(config-vrf)#exit
PE1(config)#ip vrf 2
PE1(config-vrf)#rd 200:1
PE1(config-vrf)#route-target 200:1
PE1(config-vrf)#exit
PE1(config)#interface gigabitethernet1
PE1(config-if-gigabitethernet1)#ip vrf forwarding 1
PE1(config-if-gigabitethernet1)#ipv6 address 2001:1::1/64
PE1(config-if-gigabitethernet1)#exit
PE1(config)#interface gigabitethernet2
PE1(config-if-gigabitethernet2)#ip vrf forwarding 2
PE1(config-if-gigabitethernet2)#ipv6 address 2001:2::1/64
PE1(config-if-gigabitethernet2)#exit
PE1(config)#router bgp 100
PE1(config-bgp)#address-family ipv6 vrf 1
PE1(config-bgp-af)#neighbor 2001:1::2 remote-as 65100
PE1(config-bgp-af)#exit-address-family
PE1(config-bgp)#exit
PE1(config)#ipv6 router ospf 100 vrf 2
PE1(config-ospf6)#router-id 1.1.1.1
PE1(config-ospf6)#exit
PE1(config)#interface gigabitethernet 2
PE1(config-if-gigabitethernet2)#ipv6 router ospf 100 area 0
PE1(config-if-gigabitethernet2)#exit
```

#On CE1, configure IPv6 BGP, and advertise the CE route to PE.

```
CE1#configure terminal
CE1(config)#router bgp 65100
CE1(config-bgp)#bgp router-id 11.11.11.11
CE1(config-bgp)#address-family ipv6
```

```
CE1(config-bgp-af)#neighbor 2001:1::1 remote-as 100
CE1(config-bgp-af)#network 1::1/128
CE1(config-bgp-af)#exit-address-family
CE1(config-bgp)#exit
```

#On CE2, configure OSPFv3, and advertise the CE route to PE.

```
CE2#configure terminal
CE2(config)#ipv6 router ospf 100
CE2(config-ospf6)#router-id 22.22.22.22
CE2(config-ospf6)#exit
CE2(config)#interface gigabitethernet 0
CE2(config-if-gigabitethernet0)#ipv6 router ospf 100 area 0
CE2(config-if-gigabitethernet0)#exit
CE2(config)#interface loopback 0
CE2(config-if-loopback0)#ipv6 router ospf 100 area 0
CE2(config-if-loopback0)#exit
```

#After the configuration is complete, view the route tables of VPN1 and VPN2 on PE1.

```
PE1#show ipv6 route vrf 1
Codes: C - Connected, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management



B   1::1/128 [20/0]
    via 2001:1::2, 00:00:19, gigabitethernet1
C   2001:1::/64 [0/0]
    via ::, 00:03:46, gigabitethernet1
L   2001:1::1/128 [0/0]
    via ::, 00:03:46, gigabitethernet1

PE1#show ipv6 route vrf 2
Codes: C - Connected, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management
```

```
O   2::2/128 [110/2]
    via fe80::201:7aff:fe5e:6d2f, 00:00:18, gigabitethernet2
C   2001:2::/64 [0/0]
    via ::, 00:21:40, gigabitethernet2
L   2001:2::1/128 [0/0]
    via ::, 00:21:40, gigabitethernet2
```

You can see that there is the route information of CE1 and CE2 in the VPN1 and VPN2 route tables of PE1.

Step 5: On PE2 and MCE, configure the VPN instance; on CE3, CE4, configure the default route to MCE.

#On PE2, configure the VPN instance, and configure OSPFv3 in VPN1 and VPN2.

```
PE2(config)#ip vrf 1
PE2(config-vrf)#rd 100:1
PE2(config-vrf)#route-target 100:1
PE2(config-vrf)#exit
PE2(config)#ip vrf 2
PE2(config-vrf)#rd 200:1
PE2(config-vrf)#route-target 200:1
PE2(config-vrf)#exit
PE2(config)#interface gigabitethernet1.1
PE2(config-if-gigabitethernet1.1)#ip vrf forwarding 1
PE2(config-if-gigabitethernet1.1)#encapsulation dot1q 1
PE2(config-if-gigabitethernet1.1)#ipv6 address 2001:3::1/64
PE2(config-if-gigabitethernet1.1)#exit
PE2(config)#interface gigabitethernet1.2
PE2(config-if-gigabitethernet1.2)#ip vrf forwarding 2
PE2(config-if-gigabitethernet1.2)#encapsulation dot1q 2
PE2(config-if-gigabitethernet1.2)#ipv6 address 2001:4::1/64
PE2(config-if-gigabitethernet1.2)#exit
PE2(config)#router ospf 100 vrf 1
PE2(config-ospf6)#router-id 2.2.2.2
PE2(config-ospf6)#exit
PE2(config)#router ospf 200 vrf 2
PE2(config-ospf6)#router-id 2.2.2.3
PE2(config-ospf6)#exit
PE2(config)#interface gigabitethernet1.1
PE2(config-if-gigabitethernet1.1)#ipv6 router ospf 100 area 0
```

```
PE2(config-if-gigabitethernet1.1)#exit
PE2(config)#interface gigabitethernet1.2
PE2(config-if-gigabitethernet1.2)#ipv6 router ospf 200 area 0
PE2(config-if-gigabitethernet1.2)#exit
```

#On MCE, configure the VPN instance; configure OSPFv3 in VPN1 and VPN2, configure the IPv6 static route to the CE loopback port, and re-distribute to OSPFv3.

```
MCE#configure terminal
MCE(config)#ip vrf 1
MCE(config-vrf)#rd 100:1
MCE(config-vrf)#exit
MCE(config)#ip vrf 2
MCE(config-vrf)#rd 200:1
MCE(config-vrf)#exit
MCE(config)#interface gigabitethernet0.1
MCE(config-if-gigabitethernet0.1)#ip vrf forwarding 1
MCE(config-if-gigabitethernet0.1)# encapsulation dot1q 1
MCE(config-if-gigabitethernet0.1)#ipv6 address 2001:3::2/64
MCE(config-if-gigabitethernet0.1)#exit
MCE(config)#interface gigabitethernet0.2
MCE(config-if-gigabitethernet0.2)#ip vrf forwarding 2
MCE(config-if-gigabitethernet0.2)#encapsulation dot1q 2
MCE(config-if-gigabitethernet0.2)#ipv6 address 2001:4::2/64
MCE(config-if-gigabitethernet0.2)#exit
MCE(config)#interface gigabitethernet1
MCE(config-if-gigabitethernet1)#ip vrf forwarding 1
MCE(config-if-gigabitethernet1)#ipv6 address 2001:5::1/64
MCE(config-if-gigabitethernet1)#exit
MCE(config)#interface gigabitethernet2
MCE(config-if-gigabitethernet2)#ip vrf forwarding 2
MCE(config-if-gigabitethernet2)#ipv6 address 2001:6::1/64
MCE(config-if-gigabitethernet2)#exit
MCE(config)#ipv6 route vrf 1 3::3/128 2001:5::2
MCE(config)#ipv6 route vrf 2 4::4/128 2001:6::2
MCE(config)#ipv6 router ospf 100 vrf 1
MCE(config-ospf6)#router-id 55.55.55.55
MCE(config-ospf6)#redistribute static
MCE(config)#ipv6 router ospf 200 vrf 2
```

```
MCE(config-ospf6)#router-id 55.55.55.56
MCE(config-ospf6)#redistribute static
MCE(config-ospf6)#exit
MCE(config)#interface gigabitethernet 0.1
MCE(config-if-gigabitethernet0.1)#ipv6 router ospf 100 area 0
MCE(config-if-gigabitethernet0.1)#exit
MCE(config)#interface gigabitethernet 0.2
MCE(config-if-gigabitethernet0.2)#ipv6 router ospf 200 area 0
MCE(config-if-gigabitethernet0.2)#exit
```

#On CE3, configure the default route, and the egress interface points to MCE.

```
CE3#configure terminal
CE3(config)#ipv6 route ::/0 2001:5::1
```

#On CE4, configure the default route, and the egress interface points to MCE.

```
CE4#configure terminal
CE4(config)#ipv6 route ::/0 2001:6::1
```

Note:

- On CE3 and CE4, you just need to configure one default route and the egress interface points to MCE.

#After the configuration is complete, view the route tables of VPN1 and VPN2 on the MCE.

```
MCE#show ipv6 route vrf 1
Codes: C - Connected, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management



S   3::3/128 [1/0]
    via 2001:5::2, 00:14:17, gigabitethernet1
C   2001:3::/64 [0/0]
    via ::, 00:17:08, gigabitethernet0.1
L   2001:3::2/128 [0/0]
    via ::, 00:17:08, gigabitethernet0.1
C   2001:5::/64 [0/0]
    via ::, 00:15:49, gigabitethernet1
L   2001:5::1/128 [0/0]
    via ::, 00:15:49, gigabitethernet1
```

```
MCE#show ipv6 route vrf 2
Codes: C - Connected, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management



S   4::4/128 [1/0]
    via 2001:6::2, 00:10:30, gigabitethernet2
C   2001:4::/64 [0/0]
    via ::, 00:16:51, gigabitethernet0.2
L   2001:4::2/128 [0/0]
    via ::, 00:16:51, gigabitethernet0.2
C   2001:6::/64 [0/0]
    via ::, 00:10:31, gigabitethernet2
L   2001:6::1/128 [0/0]
    via ::, 00:10:31, gigabitethernet2
```

You can see that there is the IPv6 static route information of CE3 and CE4 on the route tables of VPN1 and VPN2 of the MCE.

#View the route tables of VPN1 and VPN2 on PE2.

```
PE2#show ipv6 route vrf 1
Codes: C - Connected, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management



OE  3::3/128 [150/20]
    via fe80::201:7aff:fec8:2ce0, 00:04:38, gigabitethernet1.1
C   2001:3::/64 [0/0]
    via ::, 00:25:59, gigabitethernet1.1
L   2001:3::1/128 [0/0]
    via ::, 00:25:59, gigabitethernet1.1

PE2#show ipv6 route vrf 2
Codes: C - Connected, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
       U - Per-user Static route
```

```
O - OSPF, OE-OSPF External, M - Management

OE  4::4/128 [150/20]
    via fe80::201:7aff:fec8:2ce0, 00:04:06, gigabitethernet1.2
C   2001:4::/64 [0/0]
    via ::, 00:25:48, gigabitethernet1.2
L   2001:4::1/128 [0/0]
    via ::, 00:25:48, gigabitethernet1.2
```

You can see that there is the route information of CE3 and CE4 on the route tables of VPN1 and VPN2 of PE2.

Step 6: Configure MP-IBGP, use the loopback interface as the peer address, and re-distribute the route with the OSPFv3 protocol in the VPN instance.

#On PE1, configure MP-IBGP, enable VPNv6 address family, and re-distribute the route with the OSPFv3 protocol in the VPN2 instance.

```
PE1(config)#router bgp 100
PE1(config-bgp)#neighbor 2.2.2.2 remote-as 100
PE1(config-bgp)#neighbor 2.2.2.2 update-source loopback0
PE1(config-bgp)#address-family vpnv6
PE1(config-bgp-af)#neighbor 2.2.2.2 activate
PE1(config-bgp-af)#exit-address-family
PE1(config-bgp)#address-family ipv6 vrf 2
PE1(config-bgp-af)#redistribute ospf 100
PE1(config-bgp-af)#exit-address-family
PE1(config-bgp)#exit
PE1(config)#ipv6 router ospf 100 vrf 2
PE1(config-ospf6)#redistribute bgp 100
PE1(config-ospf6)#exit
```

#On PE2, configure MP-IBGP, enable VPNv6 address family, and re-distribute the route with the OSPFv3 protocol in the VPN1 and VPN2 instances.

```
PE2(config)#router bgp 100
PE2(config-bgp)#neighbor 1.1.1.1 remote-as 100
PE2(config-bgp)#neighbor 1.1.1.1 update-source loopback 0
PE2(config-bgp)#address-family vpnv6
PE2(config-bgp-af)#neighbor 1.1.1.1 activate
PE2(config-bgp-af)#exit-address-family
PE2(config-bgp)#address-family ipv6 vrf 1
```

```
PE2(config-bgp-af)#redistribute ospf 100
PE2(config-bgp-af)#exit-address-family
PE2(config-bgp)#address-family ipv6 vrf 2
PE2(config-bgp-af)#redistribute ospf 200
PE2(config-bgp-af)#exit-address-family
PE2(config-bgp)#exit
PE2(config)#ipv6 router ospf 100 vrf 1
PE2(config-ospf6)#redistribute bgp 100
PE2(config-ospf6)#exit
PE2(config)#ipv6 router ospf 200 vrf 2
PE2(config-ospf6)#redistribute bgp 100
PE2(config-ospf6)#exit
```

Step 7: Check the result.

#After the configuration is complete, view the BGP neighbor information on the PE.

Take PE1 as an example:

```
PE1#show bgp vpnv6 unicast all summary
BGP router identifier 1.1.1.1, local AS number 100
BGP table version is 4
2 BGP AS-PATH entries
0 BGP community entries

Neighbor        V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
2.2.2.2         4   100      11       8        4    0    0 00:04:02        4

Total number of neighbors 1
BGP VRF 1 Route Distinguisher:
100:1
BGP table version is 1
2 BGP AS-PATH entries
0 BGP community entries

Neighbor        V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
2001:1::2       4 65100      16       17        1    0    0 00:11:50        1

Total number of neighbors 1
```

The content of the State/PfxRcd list is displayed as number (the number of the route prefixes received from the neighbor), and you can see that PE1 and PE2, CE1 set up the BGP neighbor successfully.

#View the BGP VPNv6 route table and VPN route table on the PE.

Take PE1 as an example:

```
PE1#show bgp vpnv6 unicast vrf 1
BGP table version is 4, local router ID is 1.1.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network          Next Hop            Metric     LocPrf Weight Path
Route Distinguisher: 100:1 (Default for VRF 1)
[B]*> 1::1/128          2001:1::2             0              0 65100 i
[B]*>i3::3/128          ::ffff:2.2.2.2        20       100      0 ?
[B]*>i2001:3::/64       ::ffff:2.2.2.2         1       100      0 ?

PE1#show bgp vpnv6 unicast vrf 2
BGP table version is 4, local router ID is 1.1.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network          Next Hop            Metric     LocPrf Weight Path
Route Distinguisher: 200:1 (Default for VRF 2)
[O]*> 2::2/128          ::                    2          32768 ?
[B]*>i4::4/128          ::ffff:2.2.2.2        20       100      0 ?
[O]*> 2001:2::/64       ::                    1          32768 ?
[B]*>i2001:4::/64       ::ffff:2.2.2.2         1       100      0 ?
```

You can see that there is the route information to the peer CE3 and CE4 in the BGP VPNv6 route table of PE1.

```
PE1#show ipv6 route vrf 1
Codes: C - Connected, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management



B   1::1/128 [20/0]
```

```
    via 2001:1::2, 00:11:14, gigabitethernet1
B   3::3/128 [200/20]
    via ::ffff:2.2.2.2, 00:02:39, gigabitethernet0
C   2001:1::/64 [0/0]
    via ::, 00:57:52, gigabitethernet1
L   2001:1::1/128 [0/0]
    via ::, 00:57:52, gigabitethernet1
B   2001:3::/64 [200/1]
    via ::ffff:2.2.2.2, 00:02:39, gigabitethernet0

PE1#show ipv6 route vrf 1 3::3/128
Codes: C - Connected, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management

B   3::3/128 [200/20]
    via ::ffff:2.2.2.2 [0], label 16, 00:03:10, gigabitethernet0
        ::ffff:10.0.0.2 [2], label 3, gigabitethernet0
```

You can see that there is the route information ot the peer CE3 in the VPN1 route table of PE1, the VPN label of the route is 24000, and the global label is 3.

```
PE1#show ipv6 route vrf 2
Codes: C - Connected, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management

O   2::2/128 [110/2]
    via fe80::201:7aff:fe5e:6d2f, 00:54:26, gigabitethernet2
B   4::4/128 [200/20]
    via ::ffff:2.2.2.2, 00:03:11, gigabitethernet0
C   2001:2::/64 [0/0]
    via ::, 01:15:48, gigabitethernet2
L   2001:2::1/128 [0/0]
    via ::, 01:15:48, gigabitethernet2
```

```
B   2001:4::/64 [200/1]
    via ::ffff:2.2.2.2, 00:03:11, gigabitethernet0
```

```
PE1#show ipv6 route vrf 2 4::4/128
Codes: C - Connected, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management
```

```
B   4::4/128 [200/20]
    via ::ffff:2.2.2.2 [0], label 24001, 00:03:20, gigabitethernet0
        ::ffff:10.0.0.2 [2], label 3, gigabitethernet0
```

You can see that there is the route information ot the peer CE4 in the VPN2 route table of PE1, the VPN label of the route is 24001, and the global label is 3.

#View the MPLS forwarding table on the PE.

Take PE1 as an example:

```
PE1#show mpls forwarding-table
Pro: L - LDP, O - OSPF, B - MP-BGP, R - RSVP, M - Mapped-Route, S - Static
Label,ML - mLDP (ML FEC: Root address/OT/OV), RM - RSVP P2MP (RM FEC: P2MP
ID/TID)
```

Pro	Ident	FEC	Inlabel	Outlabel	Outgoing	Next hop
B	1	::/0	24000	/	/	::
B	2	::/0	24001	/	/	::

You can see that there is the route label information of VPN1 and VPN2 in the MPLS forwarding table of PE1.

Note:

- For the checking method of PE2, refer to PE1.

#Ping the loopback port of CE3 at CE1 and view whether the ping can be connected.

```
CE1#ping ipv6 3::3 -s 1::1

Press key (ctrl + shift + 6) interrupt it.
Reply from  3::3: bytes = 76  time < 16 ms
Reply from  3::3: bytes = 76  time < 16 ms
Reply from  3::3: bytes = 76  time < 16 ms
Reply from  3::3: bytes = 76  time < 16 ms
```

```
Reply from  3::3: bytes = 76  time < 16 ms
Success rate is 100% (5/5). Round-trip min/avg/max = 0/0/0 ms.
```

#Ping the loopback port of CE4 at CE1 and view whether the ping can be connected.

```
CE1#ping ipv6 4::4 -s 1::1

Press key (ctrl + shift + 6) interrupt it.
Send a packet to 4::4, request timed out.
Send a packet to 4::4, request timed out.
Send a packet to 4::4, request timed out.
Send a packet to 4::4, request timed out.
Send a packet to 4::4, request timed out.
Success rate is 0% (0/5).
```

You can see that the devices in one VPN can communicate normally, the devices of different VPNs cannot communicate, and the routes are separated.

Note:

- In the actual application, if there are more than two AS edge devices, it is suggested not to re-distribute the route between different routing protocols directly. If you have to configure, it is necessary to configure the filter, summary and other route control policies on the AS edge device, preventing the route loop.

7.3.10. Configure BGP AS Replacing

Network Requirements

- Deploy IPV4 LDP in the backbone network.
- CE1 and CE2 belong VPN1.
- CE1 and CE2 both belong to AS65100, and use IPv6 BGP to exchange the route information with PE.
- PEs adopt OSPF as OSPF to intercommunicate with each other, and configure MP-IBGP to exchange the VPNv6 route information.
- Configure the AS replacing on PE1 and PE2, ensuring that CE1 and CE2 can receive the route from the peer normally.

Network Topology

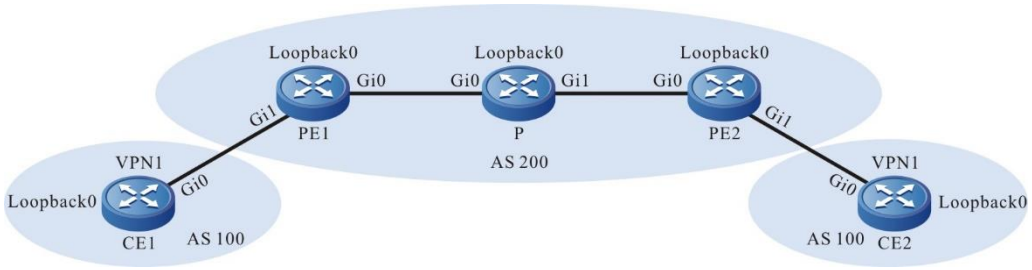

Figure 7-15 Networking of configuring BGP AS replacing

Device	Interface	IP Address	Device	Interface	IP Address
CE1	Gi0	2001:1::2/64	P	Loopback0	3.3.3.3/32
	Loopback0	1::1/128	CE2	Gi0	2001:2::2/64
PE1	Gi0	10.0.0.1/24		Loopback0	2::2/128
	Gi1	2001:1::1/64	PE2	Gi0	20.0.0.1/24
	Loopback0	1.1.1.1/32		Gi1	2001:2::1/64
P	Gi0	10.0.0.2/24		Loopback0	2.2.2.2/32
	Gi1	20.0.0.2/24			

Configuration Steps

Step 1: Configure the IP address of the interface (omitted).

Step 2: Configure the global OSPF and advertise the global route.

#Configure the global OSPF on PE1.

```
PE1#configure terminal
PE1(config)#router ospf 100
PE1(config-ospf)#network 1.1.1.1 0.0.0.0 area 0
PE1(config-ospf)#network 10.0.0.0 0.0.0.255 area 0
PE1(config-ospf)#exit
```

#Configure the global OSPF on P.

```
P#configure terminal
P(config)#router ospf 100
P(config-ospf)#network 3.3.3.3 0.0.0.0 area 0
P(config-ospf)#network 10.0.0.0 0.0.0.255 area 0
P(config-ospf)#network 20.0.0.0 0.0.0.255 area 0
P(config-ospf)#exit
```

#Configure the global OSPF on PE2.

```
PE2#configure terminal
PE2(config)#router ospf 100
PE2(config-ospf)#network 2.2.2.2 0.0.0.0 area 0
PE2(config-ospf)#network 20.0.0.0 0.0.0.255 area 0
```

```
PE2(config-ospf)#exit
```

#After the configuration is complete, view the global route table on the device.

Take PE1 as an example:

```
PE1#show ip route
Codes: C - Connected, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
    U - Per-user Static route
    O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external

Gateway of last resort is not set

C   10.0.0.0/24 is directly connected, 00:39:30, gigabitethernet0
O   20.0.0.0/24 [110/2] via 10.0.0.2, 00:11:15, gigabitethernet0
C   127.0.0.0/8 is directly connected, 1w2d:07:04:57, lo0
C   1.1.1.1/32 is directly connected, 00:39:09, loopback0
O   2.2.2.2/32 [110/3] via 10.0.0.2, 00:00:03, gigabitethernet0
O   3.3.3.3/32 [110/2] via 10.0.0.2, 00:00:44, gigabitethernet0
```

You can see that there is the route information of P and PE2 loopback ports in the global route table of PE1.

Note:

- For the checking method of P, PE2, refer to PE1.

Step 3: Enable MPLS IP and MPLS LDP.

#On PE1, enable the global MPLS IP and MPLS LDP. Meanwhile, enable MPLS IP and MPLS LDP on the interface.

```
PE1(config)#mpls ip
PE1(config)#mpls ldp
PE1(config-ldp)#router-id 1.1.1.1
PE1(config-ldp)#address-family ipv4
PE1(config-ldp-af4)#transport-address 1.1.1.1
PE1(config-ldp-af4)#exit
PE1(config-ldp)#exit
PE1(config)#interface gigabitethernet0
PE1(config-if-gigabitethernet0)#mpls ip
PE1(config-if-gigabitethernet0)#mpls ldp
PE1(config-if-gigabitethernet0)#exit
```

#On P, enable the global MPLS IP and MPLS LDP. Meanwhile, enable MPLS IP and MPLS LDP on the interface.

```
P(config)#mpls ip
```

```
P(config)#mpls ldp
P(config-ldp)#router-id 3.3.3.3
P(config-ldp)#address-family ipv4
P(config-ldp-af4)#transport-address 3.3.3.3
P(config-ldp-af4)#exit
P(config-ldp)#exit
P(config)#interface gigabitethernet0
P(config-if-gigabitethernet0)#mpls ip
P(config-if-gigabitethernet0)#mpls ldp
P(config-if-gigabitethernet0)#exit
P(config)#interface gigabitethernet1
P(config-if-gigabitethernet1)#mpls ip
P(config-if-gigabitethernet1)#mpls ldp
P(config-if-gigabitethernet1)#exit
```

#On PE2, enable the global MPLS IP and MPLS LDP. Meanwhile, enable MPLS IP and MPLS LDP on the interface.

```
PE2(config)#mpls ip
PE2(config)#mpls ldp
PE2(config-ldp)#router-id 2.2.2.2
PE2(config-ldp)#address-family ipv4
PE2(config-ldp-af4)#transport-address 2.2.2.2
PE2(config-ldp-af4)#exit
PE2(config-ldp)#exit
PE2(config)#interface gigabitethernet0
PE2(config-if-gigabitethernet0)#mpls ip
PE2(config-if-gigabitethernet0)#mpls ldp
PE2(config-if-gigabitethernet0)#exit
```

Note:

- router-id and transport-address can be configured manually and also can be generated automatically. Usually, they are configured the same. If not configuring router-id and transport-address manually, the device will select automatically. From the up interfaces, first select the Loopback interface with the maximum IP address. If the device does not configure the Loopback interface address, select the common interface with the maximum IP address.

#After the configuration is complete, view the LDP session information on the device.

Take PE1 as an example:

```
PE1#show mpls ldp session
Peer IP Address   Peer Type    My Role  State        DS Cap   DeadTime
3.3.3.3           Multicast    Passive  OPERATIONAL  Disabled 00:02:20
```

```
Statistics for ldp sessions:
    Multicast sessions: 1
    Targeted sessions: 0
```

You can see that PE1 and P set up the LDP session successfully.

#View the route label information on the device.

Take PE1 as an example:

```
PE1#show ip route 2.2.2.2 detail
Codes: C - Connected, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
    U - Per-user Static route
    O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external



O   2.2.2.2/32 [110/2] via 10.0.0.2, label 24000, 00:5:23, gigabitethernet0
                10.0.0.2 [0], gigabitethernet0

PE1#show ip route 3.3.3.3 detail
Codes: C - Connected, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
    U - Per-user Static route
    O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external



O   3.3.3.3/32 [110/2] via 10.0.0.2, label 3, 00:5:23, gigabitethernet0
                10.0.0.2 [0], gigabitethernet0
```

You can see that there is the route label information of P and PE2 loopback ports on PE1.

Note:

- For the checking method ofP, PE2, refer to PE1.

Step 4: On the PE, configure the VPN instance, and configure IPv6 BGP between PE and CE.

#On PE1, configure the VPN instance and configure the IPv6 BGP in VPN1.

```
PE1(config)#ip vrf 1
PE1(config-vrf)#rd 100:1
PE1(config-vrf)#route-target 100:1
PE1(config-vrf)#exit
PE1(config)#interface gigabitethernet1
```

```
PE1(config-if-gigabitethernet1)#ip vrf forwarding 1
PE1(config-if-gigabitethernet1)#ipv6 address 2001:1::1/64
PE1(config-if-gigabitethernet1)#exit
PE1(config)#router bgp 100
PE1(config-bgp)#address-family ipv6 vrf 1
PE1(config-bgp-af)#neighbor 2001:1::2 remote-as 65100
PE1(config-bgp-af)#exit-address-family
PE1(config-bgp)#exit
```

#On CE1, configure the IPv6 BGP with PE.

```
CE1#configure terminal
CE1(config)#router bgp 65100
CE1(config-bgp)#bgp router-id 11.11.11.11
CE1(config-bgp)#address-family ipv6
CE1(config-bgp-af)#neighbor 2001:1::1 remote-as 100
CE1(config-bgp-af)#network 1::1/128
CE1(config-bgp-af)#exit-address-family
CE1(config-bgp)#exit
```

#On PE2, configure the VPN instance and configure IPv6 BGP in VPN1.

```
PE2(config)#ip vrf 1
PE2(config-vrf)#rd 100:1
PE2(config-vrf)#route-target 100:1
PE2(config-vrf)#exit
PE2(config)#interface gigabitethernet1
PE2(config-if-gigabitethernet1)#ip vrf forwarding 1
PE2(config-if-gigabitethernet1)#ipv6 address 2001:2::1/64
PE2(config-if-gigabitethernet1)#exit
PE2(config)#router bgp 100
PE2(config-bgp)#address-family ipv6 vrf 1
PE2(config-bgp-af)#neighbor 2001:2::2 remote-as 65100
PE2(config-bgp-af)#exit-address-family
PE2(config-bgp)#exit
```

#On CE2, configure IPv6 BGP.

```
CE3#configure terminal
CE3(config)#router bgp 65100
CE3(config-bgp)#bgp router-id 22.22.22.22
CE3(config-bgp)#address-family ipv6
CE3(config-bgp-af)#neighbor 2001:2::1 remote-as 100
```

```
CE3(config-bgp-af)#network 2::2/128
CE3(config-bgp-af)#exit-address-family
CE3(config-bgp)#exit
```

#After the configuration is complete, view the IPv6 BGP neighbor information on the PE.

Take PE1 as an example:

```
PE1#show bgp vpnv6 unicast all summary
BGP router identifier 1.1.1.1, local AS number 100
BGP VRF 1 Route Distinguisher:
100:1
BGP table version is 1
2 BGP AS-PATH entries
0 BGP community entries

Neighbor        V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
2001:1::2       4 65100     125     126        1    0    0 01:45:00        1

Total number of neighbors 1
```

The content of the State/PfxRcd list is displayed as number (the number of the route prefixes received from the neighbor), and you can see that PE1 and CE1 set up the IPv6 BGP neighbor successfully.

#View the BGP VPNv6 route table and VPN route table on the PE.

```
PE1#show bgp vpnv6 unicast vrf 1
BGP table version is 7, local router ID is 1.1.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network          Next Hop            Metric     LocPrf Weight Path
Route Distinguisher: 100:1 (Default for VRF 1)
[B]*> 1::1/128          2001:1::2                0             0 65100 i

PE1#show ipv6 route vrf 1
Codes: C - Connected, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management



B   1::1/128 [20/0]
```

```
    via 2001:1::2, 01:46:06, gigabitethernet1
C   2001:1::/64 [0/0]
    via ::, 01:53:42, gigabitethernet1
L   2001:1::1/128 [0/0]
    via ::, 01:53:42, gigabitethernet1
```

You can see that there is the route information to CE1 in the BGP route table and VPN route table of PE1.

Note:

- For the checking method of PE2, refer to PE1..

Step 5: Configure MP-IBGP, and use the loopback interface as the peer address.

#On PE1, configure MP-IBGP and enable the VPNv6 address family.

```
PE1(config)#router bgp 100
PE1(config-bgp)#neighbor 2.2.2.2 remote-as 100
PE1(config-bgp)#neighbor 2.2.2.2 update-source loopback 0
PE1(config-bgp)#address-family vpnv6
PE1(config-bgp-af)#neighbor 2.2.2.2 activate
PE1(config-bgp-af)#exit-address-family
PE1(config-bgp)#exit
```

#On PE2, configure MP-IBGP and enable the VPNv6 address family.

```
PE2(config)#router bgp 100
PE2(config-bgp)#neighbor 1.1.1.1 remote-as 100
PE2(config-bgp)#neighbor 1.1.1.1 update-source loopback 0
PE2(config-bgp)#address-family vpnv6
PE2(config-bgp-af)#neighbor 1.1.1.1 activate
PE2(config-bgp-af)#exit-address-family
PE2(config-bgp)#exit
```

#After the configuration is complete, view the BGP neighbor information on the PE.

Take PE1 as an example:

```
PE1#show bgp vpnv6 unicast all summary
BGP router identifier 1.1.1.1, local AS number 100
BGP table version is 8
2 BGP AS-PATH entries
0 BGP community entries

Neighbor        V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
2.2.2.2         4   100      40      40        8    0    0 00:32:03        1
```

```
Total number of neighbors 1
BGP VRF 1 Route Distinguisher:
100:1
BGP table version is 1
2 BGP AS-PATH entries
0 BGP community entries

Neighbor        V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
2001:1::2       4 65100     171     170        1    0    0 02:23:52        1

Total number of neighbors 1
```

The content of the State/PfxRcd list is displayed as number (the number of the route prefixes received from the neighbor), and you can see that PE1 and PE2, CE1 set up the BGP neighbor successfully.

#View the BGP VPNv6 route table and VPN route table on the PE.

Take PE1 as an example:

```
PE1#show bgp vpnv6 unicast vrf 1
BGP table version is 8, local router ID is 1.1.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network          Next Hop            Metric     LocPrf Weight Path
Route Distinguisher: 100:1 (Default for VRF 1)
[B]*> 1::1/128           2001:1::2                0             0 65100 i
[B]*>i2::2/128           ::ffff:2.2.2.2           0       100   0 65100 i

PE1#show ipv6 route vrf 1
Codes: C - Connected, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management



B   1::1/128 [20/0]
    via 2001:1::2, 02:25:39, gigabitethernet1
B   2::2/128 [200/0]
    via ::ffff:2.2.2.2, 00:33:51, gigabitethernet0
C   2001:1::/64 [0/0]
```

```
    via ::, 02:33:15, gigabitethernet1
L   2001:1::1/128 [0/0]
    via ::, 02:33:15, gigabitethernet1
```

You can see that there is the route information to CE2 in the BGP VPNv6 route table of PE1. AS-PATH is displayed as 65100 and there is also the route information to CE2 in the VPN1 route table of PE1.

Note:

- For the checking method of PE2, refer to PE1..

#View the IPv6 BGP route table on the CE.

Take CE1 as an example:

```
CE1#show bgp ipv6 unicast
BGP table version is 3, local router ID is 11.11.11.11
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network          Next Hop            Metric     LocPrf Weight Path
[B]*> 1::1/128      ::                  0          32768 i
```

You can see that there is no route information to CE2 in the IPv6 BGP route table of CE1.

Note:

- CE discovers that the AS PATH attribute of the received peer route contains the same AS number 65100, so refuses the BGP route. After configuring the AS cover on the PE, CE can learn the peer route.

Step 6: On the PE, configure the AS coverage.

#In the BGP IPv6 VRF address family of PE1, configure the AS cover for the EBGP neighbor, so as to cover the same AS number with its own local AS number and transmit to the CE.

```
PE1(config)#router bgp 100
PE1(config-bgp)#address-family ipv6 vrf 1
PE1(config-bgp-af)#neighbor 2001:1::2 as-override
PE1(config-bgp-af)#exit-address-family
PE1(config-bgp)#exit
```

#In the BGP IPv6 VRF address family of PE2, configure the AS cover for the EBGP neighbor, so as to cover the same AS number with its own local AS number and transmit to the CE.

```
PE2(config)#router bgp 100
PE2(config-bgp)#address-family ipv6 vrf 1
PE2(config-bgp-af)#neighbor 2001:2::2 as-override
PE2(config-bgp-af)#exit-address-family
PE2(config-bgp)#exit
```

Step 7: Check the result.

#After the configuration is complete, view the BGP VPNv4 route table and VPN route table on the PE.

Take PE1 as an example:

```
PE1#show bgp vpnv6 unicast vrf 1
BGP table version is 10, local router ID is 1.1.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network          Next Hop          Metric     LocPrf Weight Path
Route Distinguisher: 100:1 (Default for VRF 1)
[B]*> 1::1/128          2001:1::2              0              0 65100 i
[B]*>i2::2/128          ::ffff:2.2.2.2         0       100    0 65100 i
```

You can see that there is the route information to CE2 in the BGP VPNv6 route table of PE1 and AS-PATH is displayed as 65100.

```
PE1#show ipv6 route vrf 1
Codes: C - Connected, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management



B   1::1/128 [20/0]
    via 2001:1::2, 01:31:42, gigabitethernet1
B   2::2/128 [200/0]
    via ::ffff:2.2.2.2, 02:09:55, gigabitethernet0
C   2001:1::/64 [0/0]
    via ::, 04:09:18, gigabitethernet1
L   2001:1::1/128 [0/0]
    via ::, 04:09:18, gigabitethernet1

PE1#show ipv6 route vrf 1 2::2/128
Codes: C - Connected, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management
```

```
B   2::2/128 [200/0]
    via ::ffff:2.2.2.2 [0], label 25120, 02:10:10, gigabitethernet0
        ::ffff:10.0.0.2 [3], label 24000, gigabitethernet0
```

You can see that there is the route information to the peer CE2 in the VPN1 route table of PE1, the VPN label of the route is 25120, and the global label is 24000.

#View the MPLS forwarding table on the PE.

Take PE1 as an example:

```
PE1#show mpls forwarding-table
Pro: L - LDP, O - OSPF, B - MP-BGP, R - RSVP, M - Mapped-Route, S - Static
Label,ML - mLDP (ML FEC: Root address/OT/OV), RM - RSVP P2MP (RM FEC: P2MP
ID/TID)

Pro Ident       FEC             Inlabel Outlabel Outgoing           Next hop
B   1           ::/0            25120   /        /                  ::
```

You can see that there is the route label information of VPN1 in the MPLS forwarding table of PE1.

Note:

- For the checking method of PE2, refer to PE1..

#View the IPv6 BGP route bale again on the CE.

```
CE1#show bgp ipv6 unicast
BGP table version is 5, local router ID is 11.11.11.11
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network          Next Hop          Metric     LocPrf Weight Path
[B]*> 1::1/128      ::                0          32768 i
[B]*> 2::2/128      2001:1::1         0          0 100 100 i
```

```
CE1#show ipv6 route
Codes: C - Connected, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management
```

```
L   ::1/128 [0/0]
    via ::, 1w3d:04:25:16, lo0
LC  1::1/128 [0/0]
    via ::, 04:25:09, loopback0
B   2::2/128 [20/0]
    via 2001:1::1, 01:49:27, gigabitethernet0
C   2001:1::/64 [0/0]
    via ::, 04:27:09, gigabitethernet0
L   2001:1::2/128 [0/0]
    via ::, 04:27:09, gigabitethernet0
```

You can see that there is the route information to CE2 in the IPv6 BGP route table of the CE1 and the global route table, and the AS-PATH of CE2 route is modified to 100 100 in the IPv6 BGP route table.

On CE1, ping the loopback port of CE2 and view whether the ping can be connected.

```
CE1#ping ipv6 2::2 -s 1::1

Press key (ctrl + shift + 6) interrupt it.
Reply from  2::2: bytes = 76  time < 16 ms
Reply from  2::2: bytes = 76  time < 16 ms
Reply from  2::2: bytes = 76  time < 16 ms
Reply from  2::2: bytes = 76  time < 16 ms
Reply from  2::2: bytes = 76  time < 16 ms
Success rate is 100% (5/5). Round-trip min/avg/max = 0/0/0 ms.
```

You can see that CE1 can ping CE2.

7.3.11. Configure Share VPN

Network Requirements

- Deploy IPv4 LDP in the backbone network.
- The whole MPLS network includes three VPNs, VPN1, VPN2, and VPN-share.
- CE1 belongs to the user network of VPN1, CE2 belongs to the user network of VPN2, VPN1 and VPN2 are not share VPN.
- CE3 belongs to the user network of the VPN-Share, and VPN-Share is the share VPN.
- Import RT of non-share VPN contains the Export RT of the share VPN, but does not contain the Export RT of other non-share VPN; meanwhile, Import RT of the share VPN contains the Export RT of other non-share VPN, so as to ensure that the share VPN sites can communicate with any shate VPN site. The non-share VPN sites cannot communicate with each other.

Network Topology

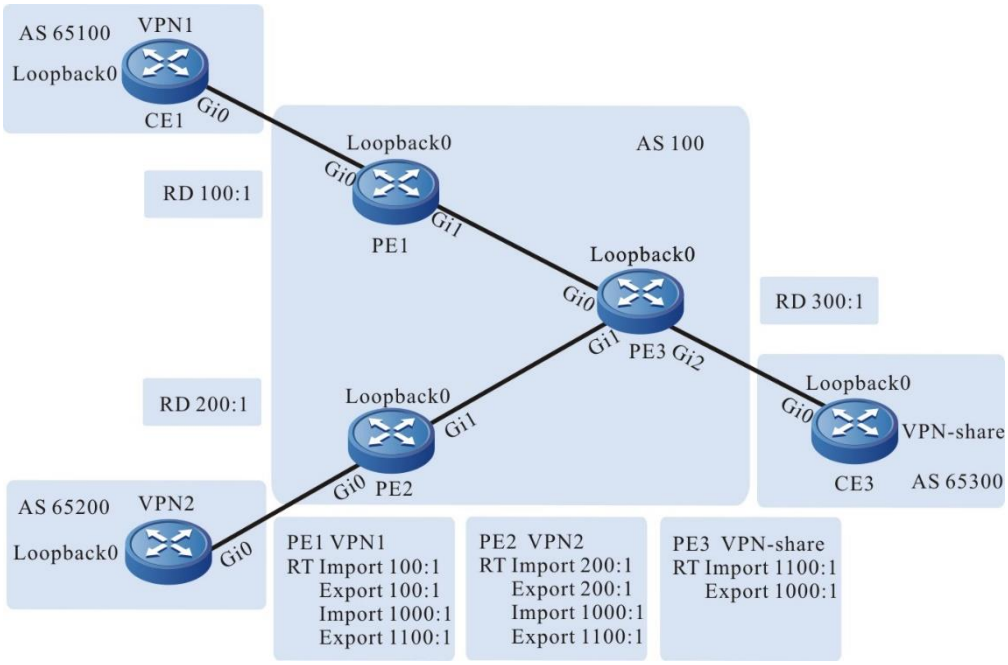

Figure 7-16 Configure the share VPN

Device	Interface	IP Address	Device	Interface	IP Address
CE1	Gi0	2001:1::2/64	CE3	Gi0	2001:3::2/64
	Loopback0	1::1/128		Loopback0	3::3/128
PE1	Gi0	2001:1::1/64	PE2	Gi0	20.0.0.2/24
	Gi1	10.0.0.1/24		Gi1	2001:2::1/64
	Loopback0	1.1.1.1/32		Loopback0	3.3.3.3/32
PE3	Gi0	10.0.0.2/24	CE2	Gi0	2001:2::2/64
	Gi1	20.0.0.1/24		Loopback0	2::2/128
	Gi2	2001:3::1/64			
	Loopback0	2.2.2.2/32			

Configuration Steps

Step 1: Configure the IP address of the interface (omitted).

Step 2: Configure the global OSPF and advertise the global route.

#Configure the global OSPF on PE1.

```
PE1#configure terminal
PE1(config)#router ospf 100
PE1(config-ospf)#network 1.1.1.1 0.0.0.0 area 0
PE1(config-ospf)#network 10.0.0.0 0.0.0.255 area 0
PE1(config-ospf)#exit
```

#Configure the global OSPF on PE2.

```
PE2#configure terminal
PE2(config)#router ospf 100
PE2(config-ospf)#network 3.3.3.3 0.0.0.0 area 0
PE2(config-ospf)#network 20.0.0.0 0.0.0.255 area 0
PE2(config-ospf)#exit
```

#Configure the global OSPF on PE3.

```
PE3#configure terminal
PE3(config)#router ospf 100
PE3(config-ospf)# network 2.2.2.2 0.0.0.0 area 0
PE3(config-ospf)#network 10.0.0.0 0.0.0.255 area 0
PE3(config-ospf)#network 20.0.0.0 0.0.0.255 area 0
PE3(config-ospf)#exit
```

#After the configuration is complete, view the global route table on the device.

Take PE1 as an example:

```
PE1#show ip route
Codes: C - Connected, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external



C   10.0.0.0/24 is directly connected, 1d:00:35:09, gigabitethernet1
O   20.0.0.0/24 [110/2] via 10.0.0.2, 1d:00:34:23, gigabitethernet1
C   127.0.0.0/8 is directly connected, 1w6d:04:09:13, lo0
C   1.1.1.1/32 is directly connected, 2d:21:48:10, loopback0
O   2.2.2.2/32 [110/2] via 10.0.0.2, 1d:00:34:23, gigabitethernet1
O   3.3.3.3/32 [110/3] via 10.0.0.2, 1d:00:34:23, gigabitethernet1
```

You can see that there is the route information og PE2 and PE3 loopback ports in the global route table of PE1.

Note:

- For the checking method of PE3, PE2, refer to PE1..

Step 3: Enable MPLS IP and MPLS LDP.

#On PE1, enable the global MPLS IP and MPLS LDP. Meanwhile, enable MPLS IP and MPLS LDP on the interface.

```
PE1(config)#mpls ip
PE1(config)#mpls ldp
PE1(config-ldp)#router-id 1.1.1.1
PE1(config-ldp)#address-family ipv4
PE1(config-ldp-af4)#transport-address 1.1.1.1
PE1(config-ldp-af4)#exit
PE1(config-ldp)#exit
PE1(config)#interface gigabitethernet1
PE1(config-if-gigabitethernet1)#mpls ip
PE1(config-if-gigabitethernet1)#mpls ldp
PE1(config-if-gigabitethernet1)#exit
```

#On PE2, enable the global MPLS IP and MPLS LDP. Meanwhile, enable MPLS IP and MPLS LDP on the interface.

```
PE2(config)#mpls ip
PE2(config)#mpls ldp
PE2(config-ldp)#router-id 3.3.3.3
PE2(config-ldp)#address-family ipv4
PE2(config-ldp-af4)#transport-address 3.3.3.3
PE2(config-ldp-af4)#exit
PE2(config-ldp)#exit
PE2(config)#interface gigabitethernet1
PE2(config-if-gigabitethernet1)#mpls ip
PE2(config-if-gigabitethernet1)#mpls ldp
PE2(config-if-gigabitethernet1)#exit
```

#On PE3, enable the global MPLS IP and MPLS LDP. Meanwhile, enable MPLS IP and MPLS LDP on the interface.

```
PE3(config)#mpls ip
PE3(config)#mpls ldp
PE3(config-ldp)#router-id 2.2.2.2
PE3(config-ldp)#address-family ipv4
PE3(config-ldp-af4)#transport-address 2.2.2.2
```

```
PE3(config-ldp-af4)#exit
PE3(config-ldp)#exit
PE3(config)#interface gigabitethernet0
PE3(config-if-gigabitethernet0)#mpls ip
PE3(config-if-gigabitethernet0)#mpls ldp
PE3(config-if-gigabitethernet0)#exit
PE3(config)#interface gigabitethernet1
PE3(config-if-gigabitethernet1)#mpls ip
PE3(config-if-gigabitethernet1)#mpls ldp
PE3(config-if-gigabitethernet1)#exit
```

#After the configuration is complete, view the LDP session information on the device.

Take PE1 as an example:

```
PE1#show mpls ldp session
Peer IP Address    Peer Type    My Role   State        DS Cap   DeadTime
2.2.2.2            Multicast    Passive   OPERATIONAL  Disabled 00:02:20
Statistics for ldp sessions:
    Multicast sessions: 1
    Targeted sessions: 0
```

You can see that PE1 and PE3 set up the LDP session successfully.

#View the route label information on the device.

Take PE1 as an example:

```
PE1#show ip route 2.2.2.2 detail
Codes: C - Connected, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
    U - Per-user Static route
    O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external



O   2.2.2.2/32 [110/2] via 10.0.0.2, label 3, 00:5:23, gigabitethernet0
                       10.0.0.2 [0], gigabitethernet0

PE1#show ip route 3.3.3.3 detail
Codes: C - Connected, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
    U - Per-user Static route
    O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external
```

```
O   3.3.3.3/32 [110/2] via 10.0.0.2, label 24001, 00:5:23, gigabitethernet0
                       10.0.0.2 [0], gigabitethernet0
```

You can see that the loopback port route from PE1 to PE2, PE3 has the label information.

Note:

- For the checking method of PE2 and PE3, refer to PE1.

Step 4: Configure the VPN instance and advertise the CE route to the PE via IPv6 BGP.

#On PE1, configure the VPN instance and IPv6 BGP in the VPN instance.

```
PE1(config)#ip vrf 1
PE1(config-vrf)#rd 100:1
PE1(config-vrf)#route-target export 100:1
PE1(config-vrf)#route-target import 100:1
PE1(config-vrf)#route-target export 1100:1
PE1(config-vrf)#route-target import 1000:1
PE1(config-vrf)#exit
PE1(config)#interface gigabitethernet0
PE1(config-if-gigabitethernet0)#ip vrf forwarding 1
PE1(config-if-gigabitethernet0)#ipv6 address 2001:1::1/64
PE1(config-if-gigabitethernet0)#exit
PE1(config)#router bgp 100
PE1(config-bgp)#address-family ipv6 vrf 1
PE1(config-bgp-af)#neighbor 2001:1::2 remote-as 65100
PE1(config-bgp-af)#exit-address-family
PE1(config-bgp)#exit
```

Note:

import-target and export-target in the Rt attribute of PE1 is 100:1, which is used to import and export the VPN internal route. export-target is 1100:1, which is used to export the VPN internal route to the share VPN; import-target is 1000:1, which is used to import the route from the share-VPN.

#Configure IPv6 BGP on CE1.

```
CE1#configure terminal
CE1(config)#router bgp 65100
CE1(config-bgp)#bgp router-id 11.11.11.11
CE1(config-bgp)#address-family ipv6
CE1(config-bgp-af)#neighbor 2001:1::1 remote-as 100
CE1(config-bgp-af)#network 1::1/128
CE1(config-bgp-af)#exit-address-family
```

```
CE1(config-bgp)#exit
```

#On PE2, configure the VPN instance and IPv6 BGP in the VPN instance.

```
PE2(config)#ip vrf 2
PE2(config-vrf)#rd 200:1
PE2(config-vrf)#route-target export 200:1
PE2(config-vrf)#route-target export 1100:1
PE2(config-vrf)#route-target import 200:1
PE2(config-vrf)#route-target import 1000:1
PE2(config-vrf)#exit
PE2(config)#interface gigabitethernet 0
PE2(config-if-gigabitethernet0)#ip vrf forwarding 2
PE2(config-if-gigabitethernet0)#ipv6 address 2001:2::1/64
PE2(config-if-gigabitethernet0)#exit
PE2(config)#router bgp 100
PE2(config-bgp)#address-family ipv6 vrf 2
PE2(config-bgp-af)#neighbor 2001:2::2 remote-as 65200
PE2(config-bgp-af)#exit-address-family
PE2(config-bgp)#exit
```

Note:

- import-target and export-target in the Rt attribute of PE2 is 100:1, which is used to import and export the VPN internal route. export-target is 1100:1, which is used to export the VPN internal route to the share VPN; import-target is 1000:1, which is used to import the route from the share-VPN.

#Configure IPv6 BGP on CE2.

```
CE2#configure terminal
CE2(config)#router bgp 65200
CE2(config-bgp)#bgp router-id 33.33.33.33
CE2(config-bgp)#address-family ipv6
CE2(config-bgp-af)#neighbor 2001:2::1 remote-as 100
CE2(config-bgp-af)#network 2::2/128
CE2(config-bgp-af)#exit-address-family
CE2(config-bgp)#exit
```

#On PE3, configure the VPN instance and IPv6 BGP in the VPN instance.

```
PE3(config)#ip vrf vpn-share
PE3(config-vrf)#rd 300:1
PE3(config-vrf)#route-target export 1000:1
PE3(config-vrf)#route-target import 1100:1
PE3(config-vrf)#exit
```

```
PE3(config)#interface gigabitethernet 2
PE3(config-if-gigabitethernet2)#ip vrf forwarding vpn-share
PE3(config-if-gigabitethernet2)#ipv6 address 2001:3::1/64
PE3(config-if-gigabitethernet2)#exit
PE3(config)#router bgp 100
PE3(config-bgp)#address-family ipv6 vrf vpn-share
PE3(config-bgp-af)#neighbor 2001:3::2 remote-as 65300
PE3(config-bgp-af)#exit-address-family
PE3(config-bgp)#exit
```

Note:

- export-target in the Rt attribute of PE3 is 1000:1, which is used to export the local VPN route to the other VPN; import-target is 1100:1, which is used to import the route from the other VPN.

#On CE3, configure IPv6 BGP.

```
CE3#configure terminal
CE3(config)#router bgp 65300
CE3(config-bgp)#bgp router-id 22.22.22.22
CE3(config-bgp)#address-family ipv6
CE3(config-bgp-af)#neighbor 2001:3::1 remote-as 100
CE3(config-bgp-af)#network 3::3/128
CE3(config-bgp-af)#exit-address-family
CE3(config-bgp)#exit
```

#After the configuration is complete, view the VPN route table on the PE.

Take PE1 as an example:

```
PE1#show ipv6 route vrf 1
Codes: C - Connected, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management




B   1::1/128 [20/0]
    via 2001:1::2, 00:17:34, gigabitethernet0
C   2001:1::/64 [0/0]
    via ::, 2d:21:38:58, gigabitethernet0
L   2001:1::1/128 [0/0]
    via ::, 2d:21:38:58, gigabitethernet0
```

You can see that there is the route information to CE1 loopback port in the VPN route table of PE1.

Note:

- For the checking method of PE2 and PE3, refer to PE1.

Step 5: Configure MP-IBGP, and use the loopback interface as the peer address.

#On PE1, configure MP-IBGP, set up the BGP neighbor with PE2, PE3, and enable the VPNv6 address family.

```
PE1(config)#router bgp 100
PE1(config-bgp)#neighbor 2.2.2.2 remote-as 100
PE1(config-bgp)#neighbor 2.2.2.2 update-source loopback 0
PE1(config-bgp)#neighbor 3.3.3.3 remote-as 100
PE1(config-bgp)#neighbor 3.3.3.3 update-source loopback 0
PE1(config-bgp)#address-family vpnv6
PE1(config-bgp-af)#neighbor 2.2.2.2 activate
PE1(config-bgp-af)#neighbor 3.3.3.3 activate
PE1(config-bgp-af)#exit-address-family
PE1(config-bgp)#exit
```

#On PE2, configure MP-IBGP, set up the BGP neighbor with PE1, PE3, and enable the VPNv6 address family.

```
PE2(config)#router bgp 100
PE2(config-bgp)#neighbor 1.1.1.1 remote-as 100
PE2(config-bgp)#neighbor 1.1.1.1 update-source loopback 0
PE2(config-bgp)#neighbor 2.2.2.2 remote-as 100
PE2(config-bgp)#neighbor 2.2.2.2 update-source loopback 0
PE2(config-bgp)#address-family vpnv6
PE2(config-bgp-af)#neighbor 1.1.1.1 activate
PE2(config-bgp-af)#neighbor 2.2.2.2 activate
PE2(config-bgp-af)#exit-address-family
PE2(config-bgp)#exit
```

#On PE3, configure MP-IBGP, set up the BGP neighbor with PE1, PE2, and enable the VPNv6 address family.

```
PE3(config)#router bgp 100
PE3(config-bgp)#neighbor 1.1.1.1 remote-as 100
PE3(config-bgp)#neighbor 1.1.1.1 update-source loopback 0
PE3(config-bgp)#neighbor 3.3.3.3 remote-as 100
PE3(config-bgp)#neighbor 3.3.3.3 update-source loopback 0
PE3(config-bgp)#address-family vpnv6
PE3(config-bgp-af)#neighbor 1.1.1.1 activate
```

```
PE3(config-bgp-af)#neighbor 3.3.3.3 activate
PE3(config-bgp-af)#exit-address-family
PE3(config-bgp)#exit
```

Step 6: Check the result.

#On the PE, view the BGP neighbor information.

Take PE1 as an example:

```
PE1#show bgp vpnv6 unicast all summary
BGP router identifier 1.1.1.1, local AS number 100
BGP table version is 3
3 BGP AS-PATH entries
0 BGP community entries

Neighbor        V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
2.2.2.2         4   100      24      24        3    0    0 00:19:46        1
3.3.3.3         4   100      23      23        3    0    0 00:18:00        0

Total number of neighbors 2
BGP VRF 1 Route Distinguisher:
100:1
BGP table version is 1
3 BGP AS-PATH entries
0 BGP community entries

Neighbor        V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
2001:1::2       4 65100      53      53        1    0    0 00:43:08        1

Total number of neighbors 1
```

The content of the Up/Down list is displayed as specific time (the time of the neighbor UP), and you can see that PE1 andPE2, PE3 set up the BGP neighbor successfully.

#View the BGP VPNv6 route table and VPN1 route table on the PE.

Take PE1 as an example:

```
PE1#show bgp vpnv6 unicast vrf 1
BGP table version is 3, local router ID is 1.1.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network          Next Hop            Metric     LocPrf Weight Path
```

```
Route Distinguisher: 100:1 (Default for VRF 1)
[B]*> 1::1/128          2001:1::2            0             0 65100 i
[B]*>i3::3/128          ::ffff:2.2.2.2       0      100    0 65300 i
```

You can see that there is the route information to CE3 in the BGP VPNv6 route table of PE1, but there is not the route information to CE2.

```
PE1#show ipv6 route vrf 1
Codes: C - Connected, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management



B   1::1/128 [20/0]
     via 2001:1::2, 00:45:03, gigabitethernet0
B   3::3/128 [200/0]
     via ::ffff:2.2.2.2, 00:10:24, gigabitethernet1
C   2001:1::/64 [0/0]
     via ::, 2d:22:06:27, gigabitethernet0
L   2001:1::1/128 [0/0]
     via ::, 2d:22:06:27, gigabitethernet0

PE1#show ipv6 route vrf 1 3::3/128
Codes: C - Connected, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management



B  3::3/128 [200/0]
     via ::ffff:2.2.2.2 [0], label 5120, 0:11:30, gigabitethernet1
         ::ffff:10.0.0.2 [2], label 3, gigabitethernet1
```

You can see that there is the route information to CE3 in the VPNv1 route table of PE1, the VPN label of the route is 25120, and the global label is 3, but there is not the route information to CE2.

#View the MPLS forwarding table on the PE.

Take PE1 as an example:

```
PE1#show mpls forwarding-table
```

```
Pro: L - LDP, O - OSPF, B - MP-BGP, R - RSVP, M - Mapped-Route, S - Static
Label,ML - mLDP (ML FEC: Root address/OT/OV), RM - RSVP P2MP (RM FEC: P2MP
ID/TID)


Pro Ident       FEC             Inlabel Outlabel Outgoing           Next hop
B  1            ::/0            25120   /       /                   ::
```

You can see that there is the route label information of VPN1 in the MPLS forwarding table of PE1.

Note:

- For the checking method of PE2 and PE3, refer to PE1.

#On CE3, ping the loopback ports of CE1 and CE2.

```
CE3#ping ipv6 1::1 -s 3::3

Press key (ctrl + shift + 6) interrupt it.
Reply from  1::1: bytes = 76  time < 16 ms
Reply from  1::1: bytes = 76  time < 16 ms
Reply from  1::1: bytes = 76  time < 16 ms
Reply from  1::1: bytes = 76  time < 16 ms
Reply from  1::1: bytes = 76  time < 16 ms
Success rate is 100% (5/5). Round-trip min/avg/max = 0/0/0 ms.

CE3#ping ipv6 2::2 -s 3::3

Press key (ctrl + shift + 6) interrupt it.
Reply from  2::2: bytes = 76  time < 16 ms
Reply from  2::2: bytes = 76  time < 16 ms
Reply from  2::2: bytes = 76  time < 16 ms
Reply from  2::2: bytes = 76  time < 16 ms
Reply from  2::2: bytes = 76  time < 16 ms
Success rate is 100% (5/5). Round-trip min/avg/max = 0/0/0 ms.
```

You can see that CE3 can ping the loopback ports of CE1 and CE2.

#On CE1, ping the loopback ports of CE2.

```
CE1#ping ipv6 2::2 -s 1::1

Press key (ctrl + shift + 6) interrupt it.
Send a packet to 2::2, request timed out.
Send a packet to 2::2, request timed out.
```

```
Send a packet to 2::2, request timed out.
Send a packet to 2::2, request timed out.
Send a packet to 2::2, request timed out.
Success rate is 0% (0/5).
```

You can see that CE1 cannot ping the loopback port of CE2.

8. MPLS VPLS

8.1. Overview

MPLS VPLS (Virtual Private LAN Service) is one point-to-multipoint L2VPN (Layer 2 Virtual Private Network) technology provided in the Ethernet LAN. The technology can connect the access points validly, and realize the point-to-point, point-to-multipoint, and multipoint-to-multipoint Ethernet service on the network topology.

The MPLS VPLS technology includes two layers, that is, signaling control layer and data forwarding layer.

- Signaling control layer: The VPLS technology uses the signaling protocol to set up the PW (Pseudo Wire) across the core network between the PEs (Provider Edge). With the PW, the Ethernet data unit can be transmitted on the core network. Most of the core networks are PSN (Packet Switch Network), like IP/MPLS. The PW in VPLS is set up by setting up one pair of uni-directional MPLS VC-LSP(Virtual Circuit-Label Switching Path) between two PEs. The setup PSN tunnel can bear multiple MPLS VPLS services, and meanwhile, shield the transmitted data and protect the security of the data across the core network. Besides, the VPLS technology adopts the signaling protocol to dynamically discover the added and logout PE node, updating the network topology information in real time.
- Data forwarding layer: One VPLS domain corresponds to one VPN user. PE maintains one bridge MAC address table of containing the corresponding relation of the MAC address and the forwarding path for each MPLS VPLS domain. MPLS VPLS creates the table via the source MAC learning, and forwards data based on the bridge MAC address table.

The VPLS technology simulates one LAN, similar to connect the user branch LAN to one switch, and inevitably, there are loops. To solve the loop topology problem, the VPLS technology puts forward the hierarchical VPLS, that is, H-VPLS (Hierarchy of VPLS) technology.

The L2 transparent transmission service provided by MPLS VPLS is different from the traditional L2VPN service. The traditional L2VPN service is the point-to-point connection service, while MPLS VPLS simulates one virtual switch on the PE device for the VPN users to use. The virtual switch has the same functions as the traditional switch. In this way, the VPN user can realize the interconnection in the VPN groups via the MPLS VPLS, realizing the multipoint connection. Besides, the MPLS VPLS technology has one advantage that after configuring the PE device with the multipoint connectivity and when adding, deleting or re-deploying the CE device in the VPN, you just need to re-configure the direct-connected PE device. If using the traditional point-to-point L2VPN, you need to re-configure each PE device. QTECH supports Martini MPLS VPLS, which can make the LDP protocol distribute the label for the VC FEC by expanding the LDP protocol.

8.2. MPLS VPLS Function Configuration

Table 8-1 MPLS VPLS function configuration list

Configuration task	
Configure the VPLS instance	Configure the VPLS instance
Bind the VPLS instance	Bind the VPLS instance
Configure the VPLS instance attributes	Configure MTU
Configure H-VPLS	Configure SVC H-VPLS

8.2.1. Configure the VPLS Instance

Configuration Condition

When configuring the VPLS instance, first complete the following tasks:

- Ensure the IGP connectivity on the MPLS core network
- Enable LDP and set up the global LSP on the MPLS core network

Configure the VPLS Instance

When configuring the VPLS instance, specify the VPN ID and peer PE address. VPN ID is used to distinguish different VPLS domains. LDP creates the VC FEC according to VPN ID, distributes the label for the VC FEC, and sets up the LDP target session according to the peer PE address. LDP negotiates the PW parameters and exchanges the label information via the target session.

Table 8-2 Configure the VPLS instance

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Create one VPLS instance	**mpls vpls** *vsi-name* [**manual**]	Mandatory By default, do not create the VPLS instance.
Configure VPN ID	**vpn-id** *value*	Mandatory By default, do not create the VPN ID.
Configure the peer PE	**peer** *peer-address* [**preferred-path tunnel** *tunnel-id* [**disable-fallback**]]	Mandatory By default, do not create the peer PE.

Note:

- If the VPLS forwarding path prefers tunnel, and then, configure the disable-fallback parameter, it indicates that you can only use the specified tunnel to forward the packets of the VPLS instance.
- VPN ID should be unique globally, and cannot repeat with VPN ID and VC ID of other VPLS instance and the VC ID in VPWS.
- The peer PE address should be the LDP transmission address of the peer PE, and the address is used to set up the target session between PEs.

8.2.2. Bind the VPLS Instance

Configuration Condition

Before the interface binds the MPLS VPLS instance, first complete the following tasks:

- Configure the VPLS instance
- Enable the MPLS forwarding capability on the desired interface, and do not configure the IP address

Bind the VPLS Instance

On the PE device, the interface connecting the CE binds the corresponding VPLS instance, and the packet received from the interface enters the VPLS instance for forwarding.

When binding the VPLS instance, you can specify the packet encapsulation mode between CE and PE as ethernet or vlan mode. By default, both L3 Ethernet main interface and L3 Ethernet sub interface are ethernet mode.

The meanings of the two modes are as follows:

- ethernet mode: The packet received from the CE is forwarded to the peer PE via PW. No matter whether the packet carries the service delimiter, PE directly presses the label, and then, forwards. After receiving the packet, the peer PE device directly pops up the label, and then, forwards the packet to CE.
- vlan mode: When the packet received from CE is forwarded to the peer PE via PW and if the packet carries the service delimiter, PE removes the service delimiter, presses the label, and forwards the packet. After the peer PE receives the popup label of the packet, add the corresponding service delimiter according to the AC interface type. If the packet does not carry the service delimiter, PE directly presses the label, and then, forwards the packet. After the peer PD receives the popup label of the packet, add the corresponding service delimiter according to the AC interface type.

Table 8-3 Bind the VPLS instance

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the interface configuration mode	**interface** *interface-name*	-
Bind the VPLS instance	**mpls vpls** *vsi-name* [**ethernet** | **vlan**]	Mandatory By default, do not bind the VPLS instance on the interface.

8.2.3. Configure the VPLS Instance Attribute

Configuration Condition

None

Configure MTU

The MTU in the VPLS instance is the maximum transmission unit of the VPLS instance. The MTUs of the VPLS instances on the peer PE devices should be consistent. Otherwise, the PW connection cannot be set up.

Table 8-4 Configure MTU

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the VPLS configuration mode	**mpls vpls** *vsi-name*	--
Configure MTU	**mtu** *value*	Optional By default, the MTU value of the VPLS instance is 1500 bytes.

Note:

- The configure MTU value is used only when the LDP protocol negotiates the PW parameter, not affecting the VPLS instance forwarding the packet.

8.2.4. Configure H-VPLS

Configuration Condition

When configuring H-VPLS, first complete the following tasks:

- Ensure the IGP connectivity on the MPLS core network
- Enable LDP and set up the global LSP on the MPLS core network

Configure SVC H-VPLS

H-VPLS (Hierarchical VPLS) uses a centralized star layout to build the hierarchical MPLS L2VPN network. The PE devices are divided to two kinds: One is the PE on the MPLS core network, called NPE, and the other is the PE device connecting the user, called UPE. UPE can be the L2 device only supporting the switching function, and also can be the L3 device supporting the switching function and the routing function. One end of it sets up PW to connect NPE, and the other end can connect one or multiple user CE devices. The PEs on the MPLS core network still remains a fully-meshed topology.

The PW between the NPE and UPE in the SVC H-VPLS is created via the Spoke VC function of LDP. When configuring the SVC H-VPLS, it is necessary to specify the UPE and VCID on the NPE.

Table 8-5 Configure the SVC H-VPLS

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the VPLS configuration mode	**mpls vpls** *vsi-name*	Mandatory By default, do not create the VPLS instance.
Configure VPN ID	**vpn-id** *value*	Mandatory By default, do not configure the VPN ID.
Configure the peer PE of SVC	**peer** *peer-address* **vc** *vc-id* [**raw | taged**] [**preferred-path tunnel** *tunnel-id* [**disable-fallback**]]	Mandatory By default, do not configure the peer PE.

8.2.5. MPLS VPLS Monitoring and Maintaining

Table 8-6 MPLS VPLS monitoring and maintaining

Command	Description
show mpls ldp vpls [*vpn-id* | **detail** | **peer** *peer-address* | **statistics**]	Display the PW information of the VPLS instance in the LDP protocol
show mpls forwarding-table vpls	Display the forwarding entry information of the VPLS instance

8.3. MPLS VPLS Typical Configuration Example

8.3.1. Configure Ethernet to Access Martini VPLS

Network Requirements

- PE and P adopt OSPF as IGP to realize the intercommunication within the PEs
- On the PE, enable the VPLS function, and adopt LDP as the VPLS signaling to set up PW.
- Three CEs belong to one VPN, and are connected via Ethernet, realizing the intercommunication between CEs.

Network Topology

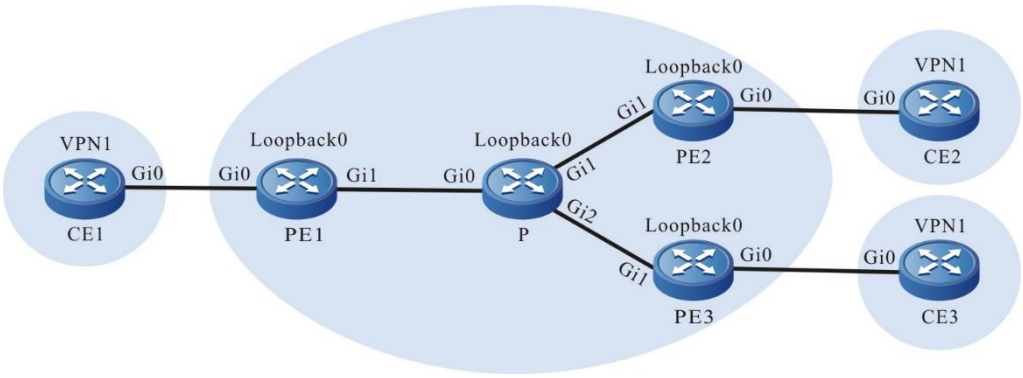

Figure 8-1 Configure Ethernet to access Martini VPLS

Device	Interface	IP Address	Device	Interface	IP Address
CE1	Gi0	1.0.0.1/24	PE1	Gi1	3.0.0.2/24
CE2	Gi0	1.0.0.2/24		Loopback0	11.0.0.1/32
CE3	Gi0	1.0.0.3/24	PE2	Gi1	4.0.0.2/24
P	Gi0	3.0.0.1/24		Loopback0	12.0.0.1/32
	Gi1	4.0.0.1/24	PE3	Gi1	5.0.0.2/24
	Gi2	5.0.0.1/24		Loopback0	13.0.0.1/32
	Loopback0	10.0.0.1/32			

Configuration Steps

Step 1: Configure the IP address of the interface. (omitted)

Step 2: Configure the global OSPF, and advertise the global route.

#On PE1, configure the global OSPF.

```
PE1#configure terminal
PE1(config)#router ospf 100
PE1(config-ospf)#network 11.0.0.1 0.0.0.0 area 0
PE1(config-ospf)#network 3.0.0.0 0.0.0.255 area 0
PE1(config-ospf)#exit
```

#On P, configure the global OSPF.

```
P#configure terminal
P(config)#router ospf 100
P(config-ospf)#network 10.0.0.1 0.0.0.0 area 0
P(config-ospf)#network 3.0.0.0 0.0.0.255 area 0
P(config-ospf)#network 4.0.0.0 0.0.0.255 area 0
P(config-ospf)#network 5.0.0.0 0.0.0.255 area 0
P(config-ospf)#exit
```

#On PE2, configure the global OSPF.

```
PE2#configure terminal
PE2(config)#router ospf 100
PE2(config-ospf)#network 12.0.0.1 0.0.0.0 area 0
```

```
PE2(config-ospf)#network 4.0.0.0 0.0.0.255 area 0
PE2(config-ospf)#exit
```

#On PE3, configure the global OSPF.

```
PE3#configure terminal
PE3(config)#router ospf 100
PE3(config-ospf)#network 13.0.0.1 0.0.0.0 area 0
PE3(config-ospf)#network 5.0.0.0 0.0.0.255 area 0
PE3(config-ospf)#exit
```

#After configuration, view the core route table on PE and P.

Take PE1 as an example:

```
PE1#show ip route
Codes: C - Connected, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
    U - Per-user Static route
    O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external
```

```
C   3.0.0.0/24 is directly connected, 00:35:39, gigabitethernet1
O   4.0.0.0/24 [110/2] via 3.0.0.1, 00:30:20, gigabitethernet1
O   5.0.0.0/24 [110/2] via 3.0.0.1, 00:30:20, gigabitethernet1
C   127.0.0.0/8 is directly connected, 00:48:18, lo0
O   10.0.0.1/32 [110/2] via 3.0.0.1, 00:29:44, gigabitethernet1
C   11.0.0.1/32 is directly connected, 00:31:06, loopback0
O   12.0.0.1/32 [110/3] via 3.0.0.1, 00:04:00, gigabitethernet1
O   13.0.0.1/32 [110/3] via 3.0.0.1, 00:27:58, gigabitethernet1
```

You can see that there is the information of the route to loopback0 segment of P, PE2, and PE3 in the route table of PE1.

Note:

- For the checking method of P, PE2, PE3, refer to PE1.

Step 3: Enable MPLS IP and MPLS LDP.

#On PE1, enable the global MPLS IP and MPLS LDP, and meanwhile, enable MPLS IP and MPLS LDP on the interface.

```
PE1(config)#mpls ip
PE1(config)#mpls ldp
PE1(config-ldp)#router-id 11.0.0.1
PE1(config-ldp)#address-family ipv4
```

```
PE1(config-ldp-af4)#transport-address 11.0.0.1
PE1(config-ldp-af4)#exit
PE1(config-ldp)#exit
PE1(config)#interface gigabitethernet1
PE1(config-if-gigabitethernet1)#mpls ip
PE1(config-if-gigabitethernet1)#mpls ldp
PE1(config-if-gigabitethernet1)#exit
```

#On P, enable the global MPLS IP and MPLS LDP, and meanwhile, enable MPLS IP and MPLS LDP on the interface.

```
P(config)#mpls ip
P(config)#mpls ldp
P(config-ldp)#router-id 10.0.0.1
P(config-ldp)#address-family ipv4
P(config-ldp-af4)#transport-address 10.0.0.1
P(config-ldp-af4)#exit
P(config-ldp)#exit
P(config)#interface gigabitethernet0
P(config-if-gigabitethernet0)#mpls ip
P(config-if-gigabitethernet0)#mpls ldp
P(config-if-gigabitethernet0)#exit
P(config)#interface gigabitethernet1
P(config-if-gigabitethernet1)#mpls ip
P(config-if-gigabitethernet1)#mpls ldp
P(config-if-gigabitethernet1)#exit
P(config)#interface gigabitethernet2
P(config-if-gigabitethernet2)#mpls ip
P(config-if-gigabitethernet2)#mpls ldp
P(config-if-gigabitethernet2)#exit
```

#On PE2, enable the global MPLS IP and MPLS LDP, and meanwhile, enable MPLS IP and MPLS LDP on the interface.

```
PE2(config)#mpls ip
PE2(config)#mpls ldp
PE2(config-ldp)#router-id 12.0.0.1
PE2(config-ldp)#address-family ipv4
PE2(config-ldp-af4)#transport-address 12.0.0.1
PE2(config-ldp-af4)#exit
PE2(config-ldp)#exit
PE2(config)#interface gigabitethernet1
```

```
PE2(config-if-gigabitethernet1)#mpls ip
PE2(config-if-gigabitethernet1)#mpls ldp
PE2(config-if-gigabitethernet1)#exit
```

#On PE3, enable the global MPLS IP and MPLS LDP, and meanwhile, enable MPLS IP and MPLS LDP on the interface.

```
PE3(config)#mpls ip
PE3(config)#mpls ldp
PE3(config-ldp)#router-id 13.0.0.1
PE3(config-ldp)#address-family ipv4
PE3(config-ldp-af4)#transport-address 13.0.0.1
PE3(config-ldp-af4)#exit
PE3(config-ldp)#exit
PE3(config)#interface gigabitethernet1
PE3(config-if-gigabitethernet1)#mpls ip
PE3(config-if-gigabitethernet1)#mpls ldp
PE3(config-if-gigabitethernet1)#exit
```

Note:

- router-id and transport-address can be configured manually and also can be generated automatically. Usually, they are configured to be the same. If not manually configuring router-id and transport-address, the device automatically select: from the up interfaces, first select the maximum IP address in the Loopback interfaces; if the device is not configured with the Loopback interface address, select the maximum IP address in the common interfaces.

#After configuration, view the LDP session information on PE and P.

Take PE1 as an example:

```
PE1#show mpls ldp session
Peer IP Address   Peer Type    My Role  State        DS Cap   DeadTime
10.0.0.1          Multicast    Active   OPERATIONAL  Disabled 00:02:43
Statistics for ldp sessions:
    Multicast sessions: 1
    Targeted sessions: 0
```

State is displayed as OPERATIONAL indicating that PE1 and P set up the LDP session successfully.

#On the device, view the route label information.

Take PE1 as an example:

```
PE1#show ip route 10.0.0.1 detail
Codes: C - Connected, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
    U - Per-user Static route
    O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external
```

```
O   10.0.0.1/32 [110/2] via 3.0.0.1, label 3, 00:35:17, gigabitethernet1
                        3.0.0.1 [0], gigabitethernet1

PE1#show ip route 12.0.0.1 detail
Codes: C - Connected, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external

O   12.0.0.1/32 [110/3] via 3.0.0.1, label 24018, 00:35:17, gigabitethernet1
                        3.0.0.1 [0], gigabitethernet1

PE1#show ip route 13.0.0.1 detail
Codes: C - Connected, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external

O   13.0.0.1/32 [110/3] via 3.0.0.1, label 24017, 00:35:17, gigabitethernet1
                        3.0.0.1 [0], gigabitethernet1
```

You can see that PE1 has the route label information of the loopback interface address of P,PE2, and PE3 in the MPLS forwarding table of PE1.

Note:

- For the checking method of P, PE2, PE3, refer to PE1.

Step 4: Configure the VPLS instance and bind the VPLS instance on the AC interface.

#On PE1, configure the VPLS instance 100 and specify the remote PE, and meanwhile, bind the VPLS instance on gigabitethernet0.

```
PE1(config)#mpls vpls 100
PE1(config-vpls)#vpn-id 1
PE1(config-vpls)#peer 12.0.0.1
PE1(config-vpls)#peer 13.0.0.1
PE1(config-vpls)#exit
```

```
PE1(config)#interface gigabitethernet0
PE1(config-if-gigabitethernet0)#mpls ip
PE1(config-if-gigabitethernet0)#mpls vpls 100 ethernet
PE1(config-if-gigabitethernet0)#exit
```

#On PE2, configure the VPLS instance 100 and specify the remote PE, and meanwhile, bind the VPLS instance on gigabitethernet0.

```
PE2(config)#mpls vpls 100
PE2(config-vpls)#vpn-id 1
PE2(config-vpls)#peer 11.0.0.1
PE2(config-vpls)#peer 13.0.0.1
PE2(config-vpls)#exit
PE2(config)#interface gigabitethernet0
PE2(config-if-gigabitethernet0)#mpls ip
PE2(config-if-gigabitethernet0)#mpls vpls 100 ethernet
PE2(config-if-gigabitethernet0)#exit
```

#On PE3, configure the VPLS instance 100 and specify the remote PE, and meanwhile, bind the VPLS instance on gigabitethernet0.

```
PE3(config)#mpls vpls 100
PE3(config-vpls)#vpn-id 1
PE3(config-vpls)#peer 11.0.0.1
PE3(config-vpls)#peer 12.0.0.1
PE3(config-vpls)#exit
PE3(config)#interface gigabitethernet0
PE3(config-if-gigabitethernet0)#mpls ip
PE3(config-if-gigabitethernet0)#mpls vpls 100 ethernet
PE3(config-if-gigabitethernet0)#exit
```

#On the PE, view the VPLS setup status.

Take PE1 as an example:

```
PE1#show mpls ldp vpls
VPLS-ID  Peer Address  State  Type  Local-MTU  Remote-MTU  Label-Sent  Label-Rcvd
1        12.0.0.1      Up     tag   1500       1500        24016       24016
1        13.0.0.1      Up     tag   1500       1500        24020       24020
Statistics for ldp vpls:
  LDP VPLS up: 2
  LDP VPLS down: 0
```

State is displayed as UP, indicating that VPLS is set up on PE1 successfully.

Note:

- For the checking method of PE2, PE3, refer to PE1.
- On the AC interface to be bound with the VPLS instance, enable the MPLS forwarding capability, and you cannot configure the IP address.

Step 5: Check the result.

#On the PE, view the MPLS forwarding table.

Take PE1 as an example:

```
PE1#show mpls forwarding-table
Pro: L - LDP, O - OSPF, B - MP-BGP, R - RSVP, M - Mapped-Route, S - Static Label,ML - mLDP (ML FEC: Root address/OT/OV), RM - RSVP P2MP (RM FEC: P2MP ID/TID)

Pro Ident       FEC             Inlabel Outlabel Outgoing          Next hop
L   -VPLS-      1               /       24016    gigabitethernet1  12.0.0.1
L   -VPLS-      1               /       24020    gigabitethernet1  13.0.0.1
L   -VPLS-      12.0.0.1/32     24016   /        VPLS 1            /
L   global      10.0.0.1/32     24017   3        gigabitethernet1  3.0.0.1
L   global      12.0.0.1/32     24018   24018    gigabitethernet1  3.0.0.1
L   global      13.0.0.1/32     24019   24017    gigabitethernet1  3.0.0.1
L   -VPLS-      13.0.0.1/32     24020   /        VPLS 1            /
```

You can see that there are the VPLS entries in the MPLS forwarding table of PE1.

Note:

- For the checking method of PE2, PE3, refer to PE1.

#On CE1, ping the gigabitethernet0 address of CE2 and CE3, and the ping can be connected.

```
CE1#ping 1.0.0.2

Press key (ctrl + shift + 6) interrupt it.
Sending 5, 76-byte ICMP Echos to 1.0.0.2 , timeout is 2 seconds:
!!!!!
Success rate is 100% (5/5). Round-trip min/avg/max = 0/3/16 ms.

CE1#ping 1.0.0.3

Press key (ctrl + shift + 6) interrupt it.
```

```
Sending 5, 76-byte ICMP Echos to 1.0.0.3 , timeout is 2 seconds:
!!!!!
Success rate is 100% (5/5). Round-trip min/avg/max = 0/3/16 ms.
```

You can see that the CE devices in the same VPNs can communicate with each other.

8.3.2. Configure Vlan to Access Martini VPLS

Network Requirements

- PE and P adopt OSPF as IGP to realize the intercommunication within the PEs.
- In the whole MPLS network, there are two VPNs, VPN1 and VPN2; CE1 and CE3 belong VPN1; CE2 and CE4 belong to VPN2.
- On the PE, enable the VPLS function, and adopt LDP as the VPLS signaling to set up PW.
- CE is connected via VLAN, realizing the communication between CEs in the same VPN. The CEs in different VPNs cannot communicate with each other.

Network Topology

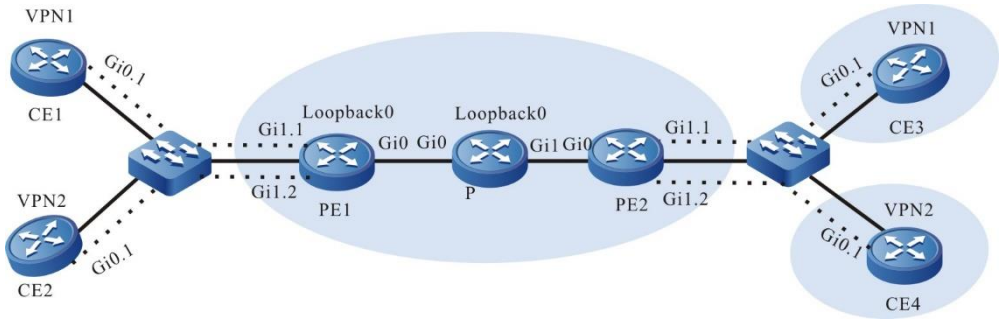

Figure 8-2 Configure Vlan to access Martini VPLS

Device	Interface	IP Address	Device	Interface	IP Address
CE1	Gi0.1	1.0.0.1/24	P	Gi0	3.0.0.2/24
CE2	Gi0.1	1.0.0.2/24		Gi1	4.0.0.1/24
CE3	Gi0.1	1.0.0.3/24		Loopback0	11.0.0.1/32
CE4	Gi0.1	1.0.0.4/24	PE2	Gi0	4.0.0.2/24
PE1	Gi0	3.0.0.1/24		Loopback0	12.0.0.1/32
	Loopback0	10.0.0.1/32			

Configuration Steps

Step 1: Configure the IP address of the interface. (omitted)

Step 2: Configure the global OSPF, and advertise the global route.

#On PE1, configure the global OSPF.

```
PE1#configure terminal
PE1(config)#router ospf 100
PE1(config-ospf)#network 10.0.0.1 0.0.0.0 area 0
PE1(config-ospf)#network 3.0.0.0 0.0.0.255 area 0
PE1(config-ospf)#exit
```

#On P, configure the global OSPF.

```
P#configure terminal
P(config)#router ospf 100
P(config-ospf)#network 11.0.0.1 0.0.0.0 area 0
P(config-ospf)#network 3.0.0.0 0.0.0.255 area 0
P(config-ospf)#network 4.0.0.0 0.0.0.255 area 0
P(config-ospf)#exit
```

#On PE2, configure the global OSPF.

```
PE2#configure terminal
PE2(config)#router ospf 100
PE2(config-ospf)#network 12.0.0.1 0.0.0.0 area 0
PE2(config-ospf)#network 4.0.0.0 0.0.0.255 area 0
PE2(config-ospf)#exit
```

#After configuration, view the core route table on PE and P.

Take PE1 as an example:

```
PE1#show ip route
Codes: C - Connected, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external



C   3.0.0.0/24 is directly connected, 00:17:14, gigabitethernet0
O   4.0.0.0/24 [110/2] via 3.0.0.2, 00:01:44, gigabitethernet0
C   127.0.0.0/8 is directly connected, 2860:10:17, lo0
C   10.0.0.1/32 is directly connected, 00:30:04, loopback0
O   11.0.0.1/32 [110/2] via 3.0.0.2, 00:01:22, gigabitethernet0
O   12.0.0.1/32 [110/3] via 3.0.0.2, 00:00:49, gigabitethernet0
```

You can see that there is the information about the route to the loopback0 segment of P, PE2 in the route table of PE1.

Note:

- For the checking method of P, PE2, refer to PE1.

Step 3: Enable MPLS IP and MPLS LDP.

#On PE1, enable the global MPLS IP and MPLS LDP, and meanwhile, enable MPLS IP and MPLS LDP on the interface.

```
PE1(config)#mpls ip
PE1(config)#mpls ldp
PE1(config-ldp)#router-id 10.0.0.1
PE1(config-ldp)#address-family ipv4
PE1(config-ldp-af4)#transport-address 10.0.0.1
PE1(config-ldp-af4)#exit
PE1(config-ldp)#exit
PE1(config)#interface gigabitethernet0
PE1(config-if-gigabitethernet0)#mpls ip
PE1(config-if-gigabitethernet0)#mpls ldp
PE1(config-if-gigabitethernet0)#exit
```

#On P, enable the global MPLS IP and MPLS LDP, and meanwhile, enable MPLS IP and MPLS LDP on the interface.

```
P(config)#mpls ip
P(config)#mpls ldp
P(config-ldp)#router-id 11.0.0.1
P(config-ldp)#address-family ipv4
P(config-ldp-af4)#transport-address 11.0.0.1
P(config-ldp-af4)#exit
P(config-ldp)#exit
P(config)#interface gigabitethernet0
P(config-if-gigabitethernet0)#mpls ip
P(config-if-gigabitethernet0)#mpls ldp
P(config-if-gigabitethernet0)#exit
P(config)#interface gigabitethernet1
P(config-if-gigabitethernet1)#mpls ip
P(config-if-gigabitethernet1)#mpls ldp
P(config-if-gigabitethernet1)#exit
```

#On PE2, enable the global MPLS IP and MPLS LDP, and meanwhile, enable MPLS IP and MPLS LDP on the interface.

```
PE2(config)#mpls ip
```

```
PE2(config)#mpls ldp
PE2(config-ldp)#router-id 12.0.0.1
PE2(config-ldp)#address-family ipv4
PE2(config-ldp-af4)#transport-address 12.0.0.1
PE2(config-ldp-af4)#exit
PE2(config-ldp)#exit
PE2(config)#interface gigabitethernet0
PE2(config-if-gigabitethernet0)#mpls ip
PE2(config-if-gigabitethernet0)#mpls ldp
PE2(config-if-gigabitethernet0)#exit
```

Note:

- router-id and transport-address can be configured manually and also can be generated automatically. Usually, they are configured to be the same. If not manually configuring router-id and transport-address, the device automatically select: from the up interfaces, first select the maximum IP address in the Loopback interfaces; if the device is not configured with the Loopback interface address, select the maximum IP address in the common interfaces

#After configuration, view the LDP session information on PE and P.

Take PE1 as an example:

```
PE1#show mpls ldp session
Peer IP Address   Peer Type    My Role  State        DS Cap   DeadTime
10.0.0.1          Multicast    Active   OPERATIONAL  Disabled 00:02:43
Statistics for ldp sessions:
    Multicast sessions: 1
    Targeted sessions: 0
```

State is displayed as OPERATIONAL, indicating that PE1 and P set up the LDP session successfully.

#On the device, view the route label information.

Take PE1 as an example:

```
PE1#show ip route 11.0.0.1 detail
Codes: C - Connected, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
    U - Per-user Static route
    O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external
```

```
O   11.0.0.1/32 [110/2] via 3.0.0.1, label 3, 00:35:17, gigabitethernet0
                        3.0.0.1 [0], gigabitethernet0
```

```
PE1#show ip route 12.0.0.1 detail
Codes: C - Connected, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external




O   12.0.0.1/32 [110/3] via 3.0.0.1, label 24020, 00:35:17, gigabitethernet0
                        3.0.0.1 [0], gigabitethernet0
```

You can see that PE1 has the route label information of the route to the loopback interface address of P and PE2.

Note:

- For the checking method of P, PE2, refer to PE1

Step 4: Configure the VPLS instance and bind the VPLS instance on the AC interface.

#On PE1, configure the VPLS instance 100 and instance 200, and specify the remote PE, and meanwhile, bind the VPLS instance 100 on gigabitethernet1.1, and bind VPLS instance 200 on gigabitethernet1.2.

```
PE1(config)#mpls vpls 100
PE1(config-vpls)#vpn-id 1
PE1(config-vpls)#peer 12.0.0.1
PE1(config-vpls)#exit
PE1(config)#mpls vpls 200
PE1(config-vpls)#vpn-id 2
PE1(config-vpls)#peer 12.0.0.1
PE1(config-vpls)#exit
PE1(config)#interface gigabitethernet1.1
PE1(config-if-gigabitethernet1.1)#encapsulation dot1q 100
PE1(config-if-gigabitethernet1.1)#mpls ip
PE1(config-if-gigabitethernet1.1)#mpls vpls 100 vlan
PE1(config-if-gigabitethernet1.1)#exit
PE1(config)#interface gigabitethernet1.2
PE1(config-if-gigabitethernet1.2)#encapsulation dot1q 200
PE1(config-if-gigabitethernet1.2)#mpls ip
PE1(config-if-gigabitethernet1.2)#mpls vpls 200 vlan
PE1(config-if-gigabitethernet1.2)#exit
```

#On PE2, configure the VPLS instance 100 and instance 200, and specify the remote PE, and meanwhile, bind the VPLS instance 100 on gigabitethernet1.1, and bind VPLS instance 200 on gigabitethernet1.2.

```
PE2(config)#mpls vpls 100
PE2(config-vpls)#vpn-id 1
PE2(config-vpls)#peer 10.0.0.1
PE2(config-vpls)#exit
PE2(config)#mpls vpls 200
PE2(config-vpls)#vpn-id 2
PE2(config-vpls)#peer 10.0.0.1
PE2(config-vpls)#exit
PE2(config)#interface gigabitethernet1.1
PE2(config-if-gigabitethernet1.1)#encapsulation dot1q 100
PE2 (config-if-gigabitethernet1.1)#mpls ip
PE2(config-if-gigabitethernet1.1)#mpls vpls 100 vlan
PE2(config-if-gigabitethernet1.1)#exit
PE2(config)#interface gigabitethernet1.2
PE2(config-if-gigabitethernet1.2)#encapsulation dot1q 200
PE2(config-if-gigabitethernet1.2)#mpls ip
PE2(config-if-gigabitethernet1.2)#mpls vpls 200 vlan
PE2(config-if-gigabitethernet1.2)#exit
```

#On the PE, view the VPLS setup status.

Take PE1 as an example:

```
PE1#show mpls ldp vpls
VPLS-ID  Peer Address  State  Type  Local-MTU  Remote-MTU  Label-Sent  Label-Rcvd
1        12.0.0.1      Up     tag   1500       1500        24016       24016
2        12.0.0.1      Up     tag   1500       1500        24017       24017
Statistics for ldp vpls
  LDP VPLS up: 2
  LDP VPLS down: 0
```

State is displayed as UP, indicating that VPLS is set up on PE1 successfully.

Note:

- For the checking method of PE2, refer to PE1.
- On the AC interface to be bound with the VPLS instance, enable the MPLS forwarding capability, and you cannot configure the IP address.

Step 5: Check the result.

#On the PE, view the MPLS forwarding table.

Take PE1 as an example:

```
PE1#show mpls forwarding-table
```

```
PE1#show mpls forwarding-table
Pro: L - LDP, O - OSPF, B - MP-BGP, R - RSVP, M - Mapped-Route, S - Static
Label,ML - mLDP (ML FEC: Root address/OT/OV), RM - RSVP P2MP (RM FEC: P2MP
ID/TID)

Pro Ident       FEC             Inlabel Outlabel Outgoing          Next hop
L  -VPLS-       1/vc:0          /       24016    /                 12.0.0.1
L  -VPLS-       2/vc:0          /       24017    /                 12.0.0.1
L  -VPLS-       12.0.0.1/32       24016  /       VPLS 1            /
L  -VPLS-       12.0.0.1/32       24017  /       VPLS 2            /
L  global       11.0.0.1/32     24018  3       gigabitethernet0    3.0.0.2
L  global       12.0.0.1/32       24019  24020   gigabitethernet0    3.0.0.2
```

You can see that there are the VPLS entries in the MPLS forwarding table of PE1.

Note:

- For the checking method of PE2, refer to PE1

#On CE1, ping the gigabitethernet0.1 address of CE3, and the ping can be connected.

```
CE1#ping 1.0.0.3

Press key (ctrl + shift + 6) interrupt it.
Sending 5, 76-byte ICMP Echos to 1.0.0.3 , timeout is 2 seconds:
!!!!!
Success rate is 100% (5/5). Round-trip min/avg/max = 0/3/16 ms.
```

#On CE1, ping the gigabitethernet0.1 address of CE4, and the ping cannot be connected.

```
CE1#ping 1.0.0.4

Press key (ctrl + shift + 6) interrupt it.
Sending 5, 76-byte ICMP Echos to 1.0.0.4 , timeout is 2 seconds:
.....
Success rate is 0% (0/5).
```

#On CE2, ping the gigabitethernet0.1 address of CE4, and the ping can be connected.

```
CE2#ping 1.0.0.4

Press key (ctrl + shift + 6) interrupt it.
Sending 5, 76-byte ICMP Echos to 1.0.0.4 , timeout is 2 seconds:
```

```
!!!!!
Success rate is 100% (5/5). Round-trip min/avg/max = 0/3/16 ms.
```

#On CE2, ping the gigabitethernet0.1 address of CE3, and the ping cannot be connected.

```
CE2#ping 1.0.0.3


Press key (ctrl + shift + 6) interrupt it.
Sending 5, 76-byte ICMP Echos to 1.0.0.3 , timeout is 2 seconds:
.....
Success rate is 0% (0/5).
```

You can see that the CE devices in the same VPN can communicate with each other, and the CE devices in different VPNs cannot communicate with each other.

Note:

- When CEs are connected via vlan, the CEs with different vlan IDs in the same VPN also can communicate with each other.

8.3.3. Configure LSP to Access Martini H-VPLS

Network Requirements

- In the whole MPLS network, there are two VPNs, VPN1 and VPN2, the CEs in the same VPN can communicate with each other, and the CEs in different VPNs cannot communicate with each other.
- On the PE, enable the VPLS function, and adopt LDP as the VPLS signaling to set up PW.
- UPE and NPE set up the virtual connection via SVC.

Network Topology

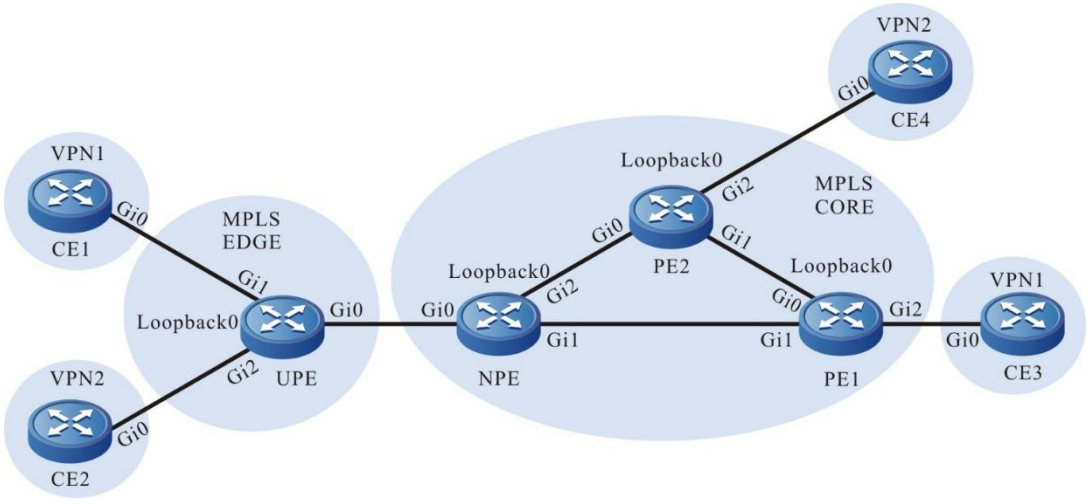

Figure 8-3 Configure LSP to access Martini H-VPLS

Device	Interface	IP Address	Device	Interface	IP Address
CE1	Gi0	1.0.0.1/24	PE1	Gi1	4.0.0.1/24
CE2	Gi0	1.0.0.2/24		Gi0	6.0.0.2/24
CE3	Gi0	1.0.0.3/24		Loopback0	12.0.0.1/32
CE4	Gi0	1.0.0.4/24	PE2	Gi0	5.0.0.1/24
NPE	Gi0	3.0.0.2/24		Gi1	6.0.0.1/24
	Gi1	4.0.0.2/24		Loopback0	13.0.0.1/32
	Gi2	5.0.0.2/24	UPE	Gi0	3.0.0.1/24
	Loopback0	11.0.0.1/32		Loopback0	10.0.0.1/32

Configuration Steps

Step 1: Configure the IP address of the interface. (omitted)

Step 2: Configure the global OSPF, and advertise the global route.

On the UPE, configure the global OSPF.

```
UPE#configure terminal
UPE(config)#router ospf 100
UPE(config-ospf)#network 10.0.0.1 0.0.0.0 area 0
UPE(config-ospf)#network 3.0.0.0 0.0.0.255 area 0
UPE(config-ospf)#exit
```

#On the NPE, configure the global OSPF.

```
NPE#configure terminal
NPE(config)#router ospf 100
NPE(config-ospf)#network 11.0.0.1 0.0.0.0 area 0
NPE(config-ospf)#network 3.0.0.0 0.0.0.255 area 0
NPE(config-ospf)#network 4.0.0.0 0.0.0.255 area 0
NPE(config-ospf)#network 5.0.0.0 0.0.0.255 area 0
NPE(config-ospf)#exit
```

#On PE1, configure the global OSPF.

```
PE1#configure terminal
```

```
PE1(config)#router ospf 100
PE1(config-ospf)#network 12.0.0.1 0.0.0.0 area 0
PE1(config-ospf)#network 4.0.0.0 0.0.0.255 area 0
PE1(config-ospf)#network 6.0.0.0 0.0.0.255 area 0
PE1(config-ospf)#exit
```

#On PE2, configure the global OSPF.

```
PE2#configure terminal
PE2(config)#router ospf 100
PE2(config-ospf)#network 13.0.0.1 0.0.0.0 area 0
PE2(config-ospf)#network 5.0.0.0 0.0.0.255 area 0
PE2(config-ospf)#network 6.0.0.0 0.0.0.255 area 0
PE2(config-ospf)#exit
```

#After configuration, view the core route table on the PE.

Take NPE as an example:

```
NPE#show ip route
Codes: C - Connected, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
    U - Per-user Static route
    O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external

C   3.0.0.0/24 is directly connected, 88:26:40, gigabitethernet0
C   4.0.0.0/24 is directly connected, 88:26:30, gigabitethernet1
C   5.0.0.0/24 is directly connected, 88:26:24, gigabitethernet2
O   6.0.0.0/24 [110/2] via 4.0.0.1, 88:12:10, gigabitethernet1
          [110/2] via 5.0.0.1, 88:09:45, gigabitethernet2
C   127.0.0.0/8 is directly connected, 278:36:42, lo0
O   10.0.0.1/32 [110/2] via 3.0.0.1, 88:24:04, gigabitethernet0
C   11.0.0.1/32 is directly connected, 88:25:07, loopback0
O   12.0.0.1/32 [110/2] via 4.0.0.1, 88:11:59, gigabitethernet1
O   13.0.0.1/32 [110/2] via 5.0.0.1, 88:09:35, gigabitethernet2
```

You can see that there is the information about the route to the loopback0 segment of UPE, PE1, PE2 in the route table of NPE.

Note:

- For the checking method of UPE, PE1, PE2, refer to NPE.

Step 3: Enable MPLS IP and MPLS LDP.

#On the UPE, enable the global MPLS IP and MPLS LDP, and meanwhile, enable MPLS IP and MPLS LDP on the interface.

```
UPE(config)#mpls ip
UPE(config)#mpls ldp
UPE(config-ldp)#router-id 10.0.0.1
UPE(config-ldp)#address-family ipv4
UPE(config-ldp-af4)#transport-address 10.0.0.1
UPE(config-ldp-af4)#exit
UPE(config-ldp)#exit
UPE(config)#interface gigabitethernet0
UPE(config-if-gigabitethernet0)#mpls ip
UPE(config-if-gigabitethernet0)#mpls ldp
UPE(config-if-gigabitethernet0)#exit
```

#On the NPE, enable the global MPLS IP and MPLS LDP, and meanwhile, enable MPLS IP and MPLS LDP on the interface.

```
NPE(config)#mpls ip
NPE(config)#mpls ldp
NPE(config-ldp)#router-id 11.0.0.1
NPE(config-ldp)#address-family ipv4
NPE(config-ldp-af4)#transport-address 11.0.0.1
NPE(config-ldp-af4)#exit
NPE(config-ldp)#exit
NPE(config)#interface gigabitethernet0
NPE(config-if-gigabitethernet0)#mpls ip
NPE(config-if-gigabitethernet0)#mpls ldp
NPE(config-if-gigabitethernet0)#exit
NPE(config)#interface gigabitethernet1
NPE(config-if-gigabitethernet1)#mpls ip
NPE(config-if-gigabitethernet1)#mpls ldp
NPE(config-if-gigabitethernet1)#exit
NPE(config)#interface gigabitethernet2
NPE(config-if-gigabitethernet2)#mpls ip
NPE(config-if-gigabitethernet2)#mpls ldp
NPE(config-if-gigabitethernet2)#exit
```

#On PE1, enable the global MPLS IP and MPLS LDP, and meanwhile, enable MPLS IP and MPLS LDP on the interface.

```
PE1(config)#mpls ip
PE1(config)#mpls ldp
```

```
PE1(config-ldp)#router-id 12.0.0.1
PE1(config-ldp)#address-family ipv4
PE1(config-ldp-af4)#transport-address 12.0.0.1
PE1(config-ldp-af4)#exit
PE1(config-ldp)#exit
PE1(config)#interface gigabitethernet0
PE1(config-if-gigabitethernet0)#mpls ip
PE1(config-if-gigabitethernet0)#mpls ldp
PE1(config-if-gigabitethernet0)#exit
PE1(config)#interface gigabitethernet1
PE1(config-if-gigabitethernet1)#mpls ip
PE1(config-if-gigabitethernet1)#mpls ldp
PE1(config-if-gigabitethernet1)#exit
```

#On PE2, enable the global MPLS IP and MPLS LDP, and meanwhile, enable MPLS IP and MPLS LDP on the interface.

```
PE2(config)#mpls ip
PE2(config)#mpls ldp
PE2(config-ldp)#router-id 13.0.0.1
PE2(config-ldp)#address-family ipv4
PE2(config-ldp-af4)#transport-address 13.0.0.1
PE2(config-ldp-af4)#exit
PE2(config-ldp)#exit
PE2(config)#interface gigabitethernet0
PE2(config-if-gigabitethernet0)#mpls ip
PE2(config-if-gigabitethernet0)#mpls ldp
PE2(config-if-gigabitethernet0)#exit
PE2(config)#interface gigabitethernet1
PE2(config-if-gigabitethernet1)#mpls ip
PE2(config-if-gigabitethernet1)#mpls ldp
PE2(config-if-gigabitethernet1)#exit
```

#After configuration, view the LDP session information on the PE.

Take NPE as an example:

```
NPE#show mpls ldp session
Peer IP Address   Peer Type    My Role   State        DS Cap    DeadTime
10.0.0.1          Multicast    Active    OPERATIONAL  Disabled  00:02:51
12.0.0.1          Multicast    Passive   OPERATIONAL  Disabled  00:02:32
13.0.0.1          Multicast    Passive   OPERATIONAL  Disabled  00:02:00
```

```
Statistics for ldp sessions:
    Multicast sessions: 3
    Targeted sessions: 0
```

State is displayed as OPERATIONAL, indicating that the PE1 and P set up the LDP session successfully.

#On the device, view the MPLS forwarding table.

Take NPE as an example:

```
NPE#show mpls forwarding-table
Pro: L - LDP, O - OSPF, B - MP-BGP, R - RSVP, M - Mapped-Route, S - Static Label,ML - mLDP (ML FEC: Root address/OT/OV), RM - RSVP P2MP (RM FEC: P2MP ID/TID)

Pro Ident       FEC             Inlabel Outlabel Outgoing          Next hop
L   global      10.0.0.1/32      24016   3       gigabitethernet0   3.0.0.1
L   global      12.0.0.1/32      24017   3       gigabitethernet1   4.0.0.1
L   global      13.0.0.1/32      24018   3       gigabitethernet2   5.0.0.1
```

You can see that there is the corresponding FEC label information of the route to the loopback interface address segment of UPE, PE1, PE2 in the MPLS forwarding table of NPE.

#View the route label information on the device.

Take NPE as an example:

```
NPE#show ip route 10.0.0.1 detail
Codes: C - Connected, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
    U - Per-user Static route
    O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external

O   10.0.0.1/32 [110/2] via 3.0.0.1, label 3, 00:35:17, gigabitethernet0
                        3.0.0.1 [0], gigabitethernet10

NPE#show ip route 12.0.0.1 detail
Codes: C - Connected, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
    U - Per-user Static route
    O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external
```

```
O   12.0.0.1/32 [110/3] via 4.0.0.1, label 3, 00:35:17, gigabitethernet1
                        4.0.0.1 [0], gigabitethernet1


NPE#show ip route 13.0.0.1 detail
Codes: C - Connected, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
    U - Per-user Static route
    O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external




O   13.0.0.1/32 [110/3] via 5.0.0.1, label 3, 00:35:17, gigabitethernet3
                        5.0.0.1 [0], gigabitethernet3
```

You can see that NPE has the route label information of the loopback interface address to UPE, PE1, and PE2.

Note:

- For the checking method of UPE, PE1, PE2, refer to NPE.

Step 4: Configure the VPLS instance and bind the VPLS instance on the AC interface.

#On PE1, configure the VPLS instance and specify the remote PE, and meanwhile, bind the VPLS instance 100 on gigabitethernet2.

```
PE1(config)#mpls vpls 100
PE1(config-vpls)#vpn-id 1
PE1(config-vpls)#peer 11.0.0.1
PE1(config-vpls)#peer 13.0.0.1
PE1(config-vpls)#exit
PE1(config)#interface gigabitethernet2
PE1(config-if-gigabitethernet2)#mpls ip
PE1(config-if-gigabitethernet2)#mpls vpls 100
PE1(config-if-gigabitethernet2)#exit
```

#On PE2, configure the VPLS instance and specify the remote PE, and meanwhile, bind the VPLS instance 200 on gigabitethernet2.

```
PE2(config)#mpls vpls 200
PE2(config-vpls)#vpn-id 2
PE2(config-vpls)#peer 11.0.0.1
PE2(config-vpls)#peer 12.0.0.1
PE2(config-vpls)#exit
PE2(config)#interface gigabitethernet2
PE2(config-if-gigabitethernet2)#mpls ip
```

```
PE2(config-if-gigabitethernet2)#mpls vpls 200
PE2(config-if-gigabitethernet2)#exit
```

#On the NPE, configure the VPLS instance and specify the remote PE, and meanwhile, configure the SVC peer.

```
NPE(config)#mpls vpls 100
NPE(config-vpls)#vpn-id 1
NPE(config-vpls)#peer 12.0.0.1
NPE(config-vpls)#peer 13.0.0.1
NPE(config-vpls)#peer 10.0.0.1 vc 10
NPE(config-vpls)#exit
NPE(config)#mpls vpls 200
NPE(config-vpls)#vpn-id 2
NPE(config-vpls)#peer 12.0.0.1
NPE(config-vpls)#peer 13.0.0.1
NPE(config-vpls)#peer 10.0.0.1 vc 20
NPE(config-vpls)#exit
```

#On UPE, configure the VPLS instance and configure the SVC peer, and meanwhile, bind the VPLS instance 100 on gigabitethernet1, and bind VPLS instance 200 on gigabitethernet2.

```
UPE(config)#mpls vpls 100
UPE(config-vpls)#vpn-id 1
UPE(config-vpls)#peer 11.0.0.1 vc 10
UPE(config-vpls)#exit
UPE(config)#mpls vpls 200
UPE(config-vpls)#vpn-id 2
UPE(config-vpls)#peer 11.0.0.1 vc 20
UPE(config-vpls)#exit
UPE(config)#interface gigabitethernet1
UPE(config-if-gigabitethernet1)#mpls ip
UPE(config-if-gigabitethernet1)#mpls vpls 100
UPE(config-if-gigabitethernet1)#exit
UPE(config)#interface gigabitethernet2
UPE(config-if-gigabitethernet2)#mpls ip
UPE(config-if-gigabitethernet2)#mpls vpls 200
UPE(config-if-gigabitethernet2)#exit
```

#On the PE, view the VPLS setup status.

Take NPE as an example:

```
NPE#show mpls ldp vpls
```

```
VPLS-ID    Peer Address   State    Type    Local-MTU   Remote-MTU  Label-Sent
Label-Rcvd
1          12.0.0.1       Up       tag     1500        1500        24019
24019
2          13.0.0.1       Up       tag     1500        1500        24023
24019
Statistics for ldp vpls:
   LDP VPLS up: 2
   LDP VPLS down: 0
```

State is displayed as UP, indicating that VPLS is set up on NPE successfully.

#On the NPE and UPE, view the SVC setup status.

Take UPE as an example:

```
UPE#show mpls ldp vpls svc
VC-ID      VPLS-ID   State   Type    Local-Label   Remote-Label   Destination-
Address
10         1         UP      tag     24016         24021          11.0.0.1
20         2         UP      tag     24017         24024          11.0.0.1
Statistics for L2-circuit:
    L2-circuit up: 2
    L2-circuit down: 0
```

State is displayed as UP, indicating that the SVC is set up between UPE and NPE successfully.

Step 5: Check the result.

#On the UPE, view the MPLS forwarding table.

```
UPE#show mpls forwarding-table
Pro: L - LDP, O - OSPF, B - MP-BGP, R - RSVP, M - Mapped-Route, S - Static
Label,ML - mLDP (ML FEC: Root address/OT/OV), RM - RSVP P2MP (RM FEC: P2MP
ID/TID)

Pro Ident      FEC            Inlabel Outlabel Outgoing          Next hop
L   -VPLS-     1/vc:10        /       24021    gigabitethernet0  11.0.0.1
L   -VPLS-     2/vc:20        /       24024    gigabitethernet0  11.0.0.1
L   -VPLS-     11.0.0.1/32    24016   /        VPLS 1            /
L   -VPLS-     11.0.0.1/32    24017   /        VPLS 2            /
```

#On the NPE, view the MPLS forwarding table.

```
NPE#show mpls forwarding-table
Pro: L - LDP, O - OSPF, B - MP-BGP, R - RSVP, M - Mapped-Route, S - Static
Label,ML - mLDP (ML FEC: Root address/OT/OV), RM - RSVP P2MP (RM FEC: P2MP
ID/TID)
```

Pro	Ident	FEC	Inlabel	Outlabel	Outgoing	Next hop
L	-VPLS-	1	/	24019	gigabitethernet1	12.0.0.1
L	-VPLS-	1/vc:10	/	24016	gigabitethernet0	10.0.0.1
L	-VPLS-	2	/	24019	gigabitethernet2	13.0.0.1
L	-VPLS-	2/vc:20	/	24017	gigabitethernet0	10.0.0.1
L	global	10.0.0.1/32	24016	3	gigabitethernet0	3.0.0.1
L	global	12.0.0.1/32	24017	3	gigabitethernet1	4.0.0.1
L	global	13.0.0.1/32	24018	3	gigabitethernet2	5.0.0.1
L	-VPLS-	12.0.0.1/32	24019	/	VPLS 1	/
L	-VPLS-	10.0.0.1/32	24021	/	VPLS 1	/
L	-VPLS-	13.0.0.1/32	24023	/	VPLS 2	/
L	-VPLS-	10.0.0.1/32	24024	/	VPLS 2	/

#On PE1, view the MPLS forwarding table.

```
PE1#show mpls forwarding-table
```

```
Pro: L - LDP, O - OSPF, B - MP-BGP, R - RSVP, M - Mapped-Route, S - Static
Label,ML - mLDP (ML FEC: Root address/OT/OV), RM - RSVP P2MP (RM FEC: P2MP
ID/TID)
```

Pro	Ident	FEC	Inlabel	Outlabel	Outgoing	Next hop
L	-VPLS-	1	/	24019	gigabitethernet1	11.0.0.1
L	global	10.0.0.1/32	24016	24016	gigabitethernet1	4.0.0.2
L	global	11.0.0.1/32	24017	3	gigabitethernet1	4.0.0.2
L	global	13.0.0.1/32	24018	3	gigabitethernet0	6.0.0.1
L	-VPLS-	11.0.0.1/32	24019	/	VPLS 1	/

You can see that there is the VPLS entry in the MPLS forwarding table of the device.

Note:

- For the checking method of PE2, refer to PE1.

#On CE1, ping the gigabitethernet0 address of CE3, and the ping can be connected.

```
CE1#ping 1.0.0.3
```

```
Press key (ctrl + shift + 6) interrupt it.
Sending 5, 76-byte ICMP Echos to 1.0.0.3 , timeout is 2 seconds:
!!!!!
Success rate is 100% (5/5). Round-trip min/avg/max = 0/3/16 ms.
```

#On CE1, ping the gigabitethernet0 address of CE4, and the ping cannot be connected.

```
CE1#ping 1.0.0.4

Press key (ctrl + shift + 6) interrupt it.
Sending 5, 76-byte ICMP Echos to 1.0.0.4 , timeout is 2 seconds:
.....
Success rate is 0% (0/5).
```

#On CE2, ping the gigabitethernet0 address of CE4, and the ping can be connected.

```
CE2#ping 1.0.0.4

Press key (ctrl + shift + 6) interrupt it.
Sending 5, 76-byte ICMP Echos to 1.0.0.4 , timeout is 2 seconds:
!!!!!
Success rate is 100% (5/5). Round-trip min/avg/max = 0/3/16 ms.
```

#On CE2, ping the gigabitethernet0 address of CE3, and the ping cannot be connected.

```
CE2#ping 1.0.0.3

Press key (ctrl + shift + 6) interrupt it.
Sending 5, 76-byte ICMP Echos to 1.0.0.3 , timeout is 2 seconds:
.....
Success rate is 0% (0/5).
```

You can see that the CE devices in the same VPN can communicate with each other, and the CE devices in different VPNs cannot communicate with each other.

8.3.4. Configure VPLS to Connect over L2TPv2 Tunnel

Network Requirements

- There are two network sites LAC and one central end LNS in the whole network. The central end PC3 is in the same IP network segment with nodes PC1 (LAC1 side) and PC2 (LAC2 side).
- The network sites and centers are configured with public network addresses to enable routes interworking through the operator network.
- The L2TPv2 tunnel is established in the network site and center, and the public network address is used as the source address and destination address of the tunnel.
- The network site and center establish the OSPF neighbor through the L2TPv2 tunnel to realize internal routing interworking.
- The network site and the center establish an LDP session through the L2TPv2 tunnel.
- The network site and center enable the VPLS function and use LDP as VPLS signaling to establish PW.

- PC1 and PC3, PC2 and PC3 realize the L2 communication across L3 network through the VPLS over L2TPv2 tunnel.

Network Topology

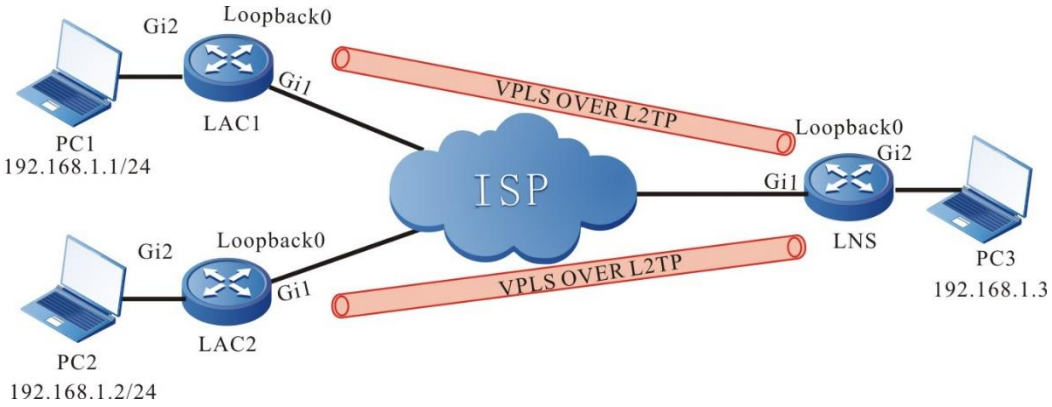

Figure 8-4 Networking of configuring VPLS over L2TPv2

Device	Interface	IP Address	Device	Interface	IP Address
LAC1	Gi1	1.100.1.1/24	LNS	Gi1	1.100.3.1/24
	Loopback0	10.1.1.1/32		Loopback0	10.3.1.1/32
PC1		192.168.1.1/24		Loopback1	10.3.2.1/32
LAC2	Gi1	1.100.2.1/24	PC3		192.168.1.3/24
	Loopback0	10.2.1.1/32			
PC2		192.168.1.2/24			

Configuration Steps

Step 1: Configure the IP address of the interface. (omitted)

Step 2: Configure the static or dynamic route, making the public network address routes of the network site and central interwork with each other (omitted).

#On LNS, you can ping the public network address of LAC1 and LAC2.

```
LNS#ping 1.100.1.1

Press key (ctrl + shift + 6) interrupt it.
Sending 5, 76-byte ICMP Echos to 1.100.1.1 , timeout is 2 seconds:
!!!!!
```

```
Success rate is 100% (5/5). Round-trip min/avg/max = 0/1/4 ms.


LNS#ping 1.100.2.1



Press key (ctrl + shift + 6) interrupt it.
Sending 5, 76-byte ICMP Echos to 1.100.2.1 , timeout is 2 seconds:
!!!!!
Success rate is 100% (5/5). Round-trip min/avg/max = 1/3/4 ms.
```

Note:

- For the checking method of LAC1 and LAC2, refer to LNS.

Step 3: Configure the L2TPv2 tunnel.

#On LAC1, configure the pseudowire template name as vpls_l2tp, encapsulation protocol type as L2TPv2, the key as admin123, and local device name as lac1, and borrow gigabitethernet1.

```
LAC1(config)#pseudowire-class vpls_l2tp
LAC1(config-pw-class)#encapsulation l2tpv2
LAC1(config-pw-class)#password 0 admin123
LAC1(config-pw-class)#hostname lac1
LAC1(config-pw-class)#ip local interface gigabitethernet1
LAC1(config-pw-class)#exit
```

#On LAC1, configure the virtual PPP interface virtual ppp0, encapsulate the PPP protocol, use the PAP authentication mode to send, the user name is admin, the password is admin123, and use the pseudo wire template vpls_l2tp to establish the L2TP tunnel with LNS.

```
LAC1(config)#interface virtual-ppp0
LAC1(config-if-virtual-ppp0)#encapsulation ppp
LAC1(config-if-virtual-ppp0)#ip address 10.1.2.1 255.255.255.0
LAC1(config-if-virtual-ppp0)#ppp pap sent-username admin password 0 admin123
LAC1(config-if-virtual-ppp0)#pseudowire 1.100.3.1 1 pw-class vpls_l2tp
LAC1(config-if-virtual-ppp0)#exit
```

#On LAC2, configure the pseudo wire template with the name vpls_l2tp, the encapsulation protocol type is L2TPv2, the key is admin123, the local device name is lac2, and borrow gigabitethernet1.

```
LAC2(config)#pseudowire-class vpls_l2tp
LAC2(config-pw-class)#encapsulation l2tpv2
LAC2(config-pw-class)#password 0 admin123
LAC2(config-pw-class)#hostname lac2
LAC2(config-pw-class)#ip local interface gigabitethernet1
LAC2(config-pw-class)#exit
```

#On LAC2, configure the virtual PPP interface virtual-ppp0, encapsulate the PPP protocol, use the PAP authentication mode to send, the user name is admin, the password is admin123, and use the pseudo wire template vpls_l2tp to establish the L2TP tunnel with LNS.

```
LAC2(config)#interface virtual-ppp0
LAC2(config-if-virtual-ppp0)#encapsulation ppp
LAC2(config-if-virtual-ppp0)#ip address 10.2.2.1 255.255.255.0
LAC2(config-if-virtual-ppp0)#ppp pap sent-username admin password 0 admin123
LAC2(config-if-virtual-ppp0)#pseudowire 1.100.3.1 1 pw-class vpls_l2tp
LAC2(config-if-virtual-ppp0)#exit
```

#On LNS, configure the user name of PPP authentication as admin, and password as admin123.

```
LNS(config)#local-user admin class network
LNS(config-user-network-admin)#service-type ppp
LNS(config-user-network-admin)#password 0 admin123
LNS(config-user-network-admin)#exit
```

#On LNS, configure the virtual template virtual-template 0, and use the PAP authentication mode.

```
LNS(config)#interface virtual-template 0
LNS(config-if-virtual-template0)#encapsulation ppp
LNS(config-if-virtual-template0)#ip unnumbered loopback1
LNS(config-if-virtual-template0)#ppp authentication pap
LNS(config-if-virtual-template0)#exit
```

#On LNS, enable VPDN, create VPDN group vpls_lns, which is configured to accept dial-in request, apply the L2TP protocol, borrow virtual template virtual-template0, and configures the shared key between LAC and LNS as admin123.

```
LNS(config)#vpdn enable
LNS(config)#vpdn-group vpls_lns
LNS(config-vpdn)#accept-dialin
LNS(config-vpdn-acc-in)#protocol l2tp
LNS(config-vpdn-acc-in)#virtual-template 0
LNS(config-vpdn-acc-in)#exit
LNS(config-vpdn)#local name lns
LNS(config-vpdn)#l2tp tunnel password 0 admin123
LNS(config-vpdn)#exit
```

Note:

- For more about the L2TP configuration, refer to IP protocol and services-L2TP chapter in te manual.

Step 4: Check the setup result of the L2TP tunnel.

#View the virtual-ppp0 interface information of LAC1.

```
LAC1#show interface virtual-ppp 0
```

```
virtual-ppp0:
line protocol is up
 Flags: (0x81080f1) POINT-TO-POINT MULTICAST RUNNING
 Type: PPP
Internet address: 10.1.2.1/24
    Destination Internet address: 10.3.2.1
    Metric: 0, MTU: 1500, BW: 64 Kbps, DLY: 20000 usec, VRF: global
    Reliability 255/255, Txload 3/255, Rxload 1/255
    Last clearing of "show interface" counters never
    input peak rate 86021 bits/sec,  0 hour 11 minutes 4 seconds ago
    output peak rate 143778 bits/sec,  0 hour 11 minutes 4 seconds ago
    5 minutes input rate 315 bits/sec, 0 packet/sec, bandwidth utilization -
    5 minutes output rate 1002 bits/sec, 1 packet/sec, bandwidth utilization -
    2170 packets received; 4238 packets sent
    407116 bytes received; 1126619 bytes sent
    378 multicast packets received
    388 multicast packets sent
    0 input errors; 0 output errors
    0 collisions; 0 dropped
     encap-type: simply PPP
     LCP:OPENED
     IPCP:OPENED   MPLSCP:OPENED
```

#On the LAC1 device, view the L2TP information.

```
LAC1#show vpdn detail

 L2tp MaxTun 12000, MaxSes 12000:

 tunnel free num: 11999
TUNNELS:
 LOCAL-ID REM-ID   LOCAL-NAME   REM-NAME  VPDN-GROUP   PORT   SES-CNT
STATE       REM-ADDR
1429    736     vpls_lac      lns            1701     1     ESTABLISHED     1.100.3.1

session free num: 11999
SESSIONS:
LOCAL-ID REM-ID   TUN-ID   IF-NAME      SYSTEMID          MSI/CALLING-NUM
STATE
188     86      1429  virtual-ppp0   --------    ----------------      ESTABLISHED
```

L2tp total Tunnel and Session Information. Tunnel 1 Session 1

It can be observed that the L2TP tunnel is successfully established between LAC1 and LNS.

#On LAC, you can ping the virtual-template0 interface address of LNS.

LAC1#ping 10.3.2.1

Press key (ctrl + shift + 6) interrupt it.

Sending 5, 76-byte ICMP Echos to 10.3.2.1 , timeout is 2 seconds:

!!!!!

Success rate is 100% (5/5). Round-trip min/avg/max = 2/4/8 ms.

Note:

- For the checking method of LAC2, refer to LAC1.

Step 5: On LAC and LNS, configure the global OSPF, and advertise the internal route.

#On LAC1, configure the global OSPF.

LAC1(config)#router ospf 100

LAC1(config-ospf)#router-id 10.1.1.1

LAC1(config-ospf)#network 10.1.0.0 0.0.255.255 area 0

LAC1(config-ospf)#exit

#On LAC2, configure the global OSPF.

LAC2(config)#router ospf 100

LAC2(config-ospf)#router-id 10.2.1.1

LAC2(config-ospf)#network 10.2.0.0 0.0.255.255 area 0

LAC2(config-ospf)#exit

#On LNS, configure the global OSPF.

LNS(config)#router ospf 100

LNS(config-ospf)#router-id 10.3.1.1

LNS(config-ospf)#network 10.3.0.0 0.0.255.255 area 0

LNS(config-ospf)#exit

#After configuration, view the core route table on LNS.

LNS#show ip route

Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS

U - Per-user Static route

O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external

```
S   1.100.1.1/32 [1/10] is directly connected, 2d:19:54:00, gigabitethernet1
S   1.100.2.1/32 [1/10] is directly connected, 2d:19:54:00, gigabitethernet1
C   1.100.3.0/24 is directly connected, 2d:19:54:01, gigabitethernet1
L   1.100.3.1/32 is directly connected, 2d:19:54:01, gigabitethernet1
O   10.1.1.1/32 [110/1563] via 10.1.2.1, 02:02:15, virtual-access0
C   10.1.2.1/32 is directly connected, 2d:19:53:47, virtual-access0
O   10.2.1.1/32 [110/1563] via 10.2.2.1, 02:01:59, virtual-access1
C   10.2.2.1/32 is directly connected, 2d:19:53:35, virtual-access1
LC  10.3.1.1/32 is directly connected, 2d:20:04:02, loopback0
C   10.3.2.0/24 is directly connected, 2d:19:53:35, virtual-access1
                is directly connected, 2d:19:53:47, virtual-access0
LC  10.3.2.1/32 is directly connected, 02:54:55, loopback0
```

You can see that the route information to loopback0 segments of LAC1 and LAC2 exists in the route table of LNS.

Note:

- For the checking methods of LAC1 and LAC2, refer to LNS.

Step 6: Enable MPLS IP and MPLS LDP.

#On LAC1, enable the global MPLS IP and MPLS LDP, and enable MPLS IP and MPLS LDP on the interface.

```
LAC1(config)#mpls ip
LAC1(config)#mpls ldp
LAC1(config-ldp)#router-id 10.1.1.1
LAC1(config-ldp)#address-family ipv4
LAC1(config-ldp-af4)#transport-address 10.1.1.1
LAC1(config-ldp-af4)#exit
LAC1(config-ldp)#exit
LAC1(config)#interface virtual-ppp 0
LAC1(config-if-virtual-ppp0)#mpls ip
LAC1(config-if-virtual-ppp0)#mpls ldp
LAC1(config-if-virtual-ppp0)#exit
```

#On LAC2, enable the global MPLS IP and MPLS LDP, and enable MPLS IP and MPLS LDP on the interface.

```
LAC2(config)#mpls ip
LAC2(config)#mpls ldp
LAC2(config-ldp)#router-id 10.2.1.1
LAC2(config-ldp)#address-family ipv4
LAC2(config-ldp-af4)#transport-address 10.2.1.1
```

```
LAC2(config-ldp-af4)#exit
LAC2(config-ldp)#exit
LAC2(config-if-virtual-ppp0)#interface virtual-ppp 0
LAC2(config-if-virtual-ppp0)#mpls ip
LAC2(config-if-virtual-ppp0)#mpls ldp
LAC2(config-if-virtual-ppp0)#exit
```

#On LNS, enable the global MPLS IP and MPLS LDP, and enable MPLS IP and MPLS LDP on the interface.

```
LNS(config)#mpls ip
LNS(config)#mpls ldp
LNS(config-ldp)#router-id 10.3.1.1
LNS(config-ldp)#address-family ipv4
LNS(config-ldp-af4)#transport-address 10.3.1.1
LNS(config-ldp-af4)#exit
LNS(config-ldp)#exit
LNS(config)#interface virtual-template 0
LNS(config-if-virtual-template0)#mpls ip
LNS(config-if-virtual-template0)#mpls ldp
LNS(config-if-virtual-template0)#exit
```

#Take LNS as an example to view the LDP session information.

```
LNS#show mpls ldp session
Peer IP Address    Peer Type     My Role    State        DS Cap    DeadTime
10.1.1.1           Multicast     Active     OPERATIONAL  Disabled  00:02:05
10.2.1.1           Multicast     Active     OPERATIONAL  Disabled  00:02:15
Statistics for ldp sessions:
    Multicast sessions: 2
    Targeted sessions: 0
```

State is displayed as operational, indicating that LNS and LAC successfully established LDP session.

#Take LNS as an example to view the route label information.

```
LNS#show ip route 10.1.1.1 detail
Codes: C - Connected, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
    U - Per-user Static route
    O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external
```

```
O   10.1.1.1/32 [110/1563] via 10.1.2.1, label 3, 00:35:17, virtual-access1
```

```
                    10.1.2.1 [0], virtual-access1

LNS#show ip route 10.2.1.1 detail
Codes: C - Connected, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external

O   10.2.1.1/32 [110/1563] via 10.2.2.1, label 3, 00:35:26, virtual-access0
                    10.2.2.1 [0], virtual-access0
```

It can be seen that the MPLS forwarding table and routing label information table of LNs contain the FEC label information corresponding to the loopback interface address network segment route to LAC.

Note:

- For the checking methods of LAC1 and LAC2, refer to LNS.

Step 7: Configure the VPLS instance, and bind the VPLS instance on the AC interface.

#On LNS, configure VPLS instance 100, and specify the remote LAC. Meanwhile, on gigabitethernet2, bind the VPLS instance.

```
LNS(config)#mpls vpls 100
LNS(config-vpls)#vpn-id 1
LNS(config-vpls)#peer 10.1.1.1
LNS(config-vpls)#peer 10.2.1.1
LNS(config-vpls)#exit
LNS(config)#interface gigabitethernet2
LNS(config-if-gigabitethernet2)#mpls ip
LNS(config-if-gigabitethernet2)#mpls vpls 100 ethernet
LNS(config-if-gigabitethernet2)#exit
```

#On LAC1, configure VPLS instance 100, and specify the remote LNS. Meanwhile, on gigabitethernet2, bind the VPLS instance.

```
LAC1(config)#mpls vpls 100
LAC1(config-vpls)#vpn-id 1
LAC1(config-vpls)#peer 10.3.1.1
LAC1(config-vpls)#exit
LAC1(config)#interface gigabitethernet2
LAC1(config-if-gigabitethernet2)#mpls ip
LAC1(config-if-gigabitethernet2)#mpls vpls 100 ethernet
LAC1(config-if-gigabitethernet2)#exit
```

#On LAC2, configure VPLS instance 100, and specify the remote LNS. Meanwhile, on gigabitethernet2, bind the VPLS instance.

```
LAC2(config)#mpls vpls 100
LAC2(config-vpls)#vpn-id 1
LAC2(config-vpls)#peer 10.3.1.1
LAC2(config-vpls)#exit
LAC2(config)#interface gigabitethernet2
LAC2(config-if-gigabitethernet2)#mpls ip
LAC2(config-if-gigabitethernet2)#mpls vpls 100 ethernet
LAC2(config-if-gigabitethernet2)#exit
```

Note:

- When specifying peer, it can be configured as raw mode and tagged mode. The default mode is tagged mode. For details, please refer to MPLS VPLS in the MPLS chapter of the command manual.
- The interface can be configured as VLAN mode and Ethernet mode when binding VPLS instances. The default mode is Ethernet mode. For details, please refer to MPLS VPLS in the MPLS chapter of the command manual.

In this configuration, LACs cannot communicate with each other through LNS. If LACs need to communicate with each other, the peer configuration of LNS is replaced with peer 10.1.1.1 vc 101 and peer 10.2.1.1 vc 102, the peer configuration of LAC1 is replaced with peer 10.3.1.1 vc 101, and the peer configuration of LAC2 is replaced with peer 10.3.1.1 vc 102.

Step 8: Verify the VPLS configuration result.

#Take LNS as an example to view the VPLS setup status.

```
LNS#show mpls ldp vpls
VPLS-ID    Peer Address  State   Type     Local-MTU  Remote-MTU  Label-Sent
Label-Rcvd
1          10.1.1.1      Up      tag      1500       1500        20247       21340
1          10.2.1.1      Up      tag      1500       1500        20248       25147
Statistics for ldp vpls:
LDP VPLS up: 2
LDP VPLS down: 0
```

State is displayed as up, indicating that VPLS on LNS is successfully established.

#Take LNS as an example to view VPLS forwarding.

```
LNS#show mpls forwarding-table
Pro: L - LDP, O - OSPF, B - MP-BGP, R - RSVP, M - Mapped-Route, S - Static
Label,ML - mLDP (ML FEC: Root address/OT/OV), RM - RSVP P2MP (RM FEC: P2MP
ID/TID)

Pro Ident       FEC             Inlabel Outlabel Outgoing       Next hop
```

```
L  -VPLS-      1/vc:0          /     25340   /              10.1.1.1
L  -VPLS-      1/vc:0          /     25147   /              10.2.1.1
L  global      10.1.1.1/32     24240  3      virtual-access1      10.1.2.1
L  global      10.2.1.1/32     24241  3      virtual-access0      10.2.2.1
L  -VPLS-      10.1.1.1/32     24247  /      VPLS 1               /
L  -VPLS-      10.2.1.1/32     24248  /      VPLS 1               /
```

You can see that there are VPLS table entries in the MPLS forwarding table of LNS.

Note:

- For the checking methods of LAC1 and LAC2, refer to LNS.
- When using the configuration mode of interworking between LACs, check the VPLS establishment status by using **show mpls ldp vpls svc**.

Step 9: Check whether LNS can communicate with the PC of LAC normally.

#On PC3, you can ping PC1.

```
PC3>ping 192.168.1.1

Ping 192.168.1.1: 32 data bytes, Press Ctrl_C to break
From 192.168.1.1: bytes=32 seq=1 ttl=128 time<1 ms
From 192.168.1.1: bytes=32 seq=2 ttl=128 time=15 ms
From 192.168.1.1: bytes=32 seq=3 ttl=128 time<1 ms
From 192.168.1.1: bytes=32 seq=4 ttl=128 time=16 ms
From 192.168.1.1: bytes=32 seq=5 ttl=128 time<1 ms

--- 192.168.1.1 ping statistics ---
5 packet(s) transmitted
5 packet(s) received
0.00% packet loss
round-trip min/avg/max = 0/6/16 ms
#On PC3, you can ping PC2.
PC3>ping 192.168.1.2

Ping 192.168.1.2: 32 data bytes, Press Ctrl_C to break
From 192.168.1.2: bytes=32 seq=1 ttl=128 time<1 ms
From 192.168.1.2: bytes=32 seq=2 ttl=128 time<1 ms
From 192.168.1.2: bytes=32 seq=3 ttl=128 time=15 ms
From 192.168.1.2: bytes=32 seq=4 ttl=128 time<1 ms
From 192.168.1.2: bytes=32 seq=5 ttl=128 time=16 ms
```

```
--- 192.168.1.2 ping statistics ---
 5 packet(s) transmitted
 5 packet(s) received
 0.00% packet loss
 round-trip min/avg/max = 0/6/16 ms
```

It can be seen that PCs between LNS and LAC can communicate with each other.

9. MPLS VPWS

9.1. Overview

MPLS VPWS (Virtual Private Wire Service) is one point-to-point virtual private wire technology, used to provide the L2 VPN service of different media for the user via the MPLS network, supporting ATM, FR, VLAN, Ethernet, PPP, HDLC and other L2 media. Meanwhile, the MPLS network still can provide the common IP, L3 VPN, traffic engineering, QoS and other services, greatly saving the investment of the carrier in the network construction.

MPLS VPWS encapsulates the label stack before the L2 packet to transmit the L2 data transparently on the MPLS network. The outer label is called the tunnel label, mainly used to transmit the packet from one PE to another PE; the inner label is called VC label, used to distinguish the different connections in different L2VPN. After receiving the packet with the VC label, the PE decides to which VPN user the packet is transmitted according to the VC label.

With the MPLS VPWS network, you can set up the L2 connection between different sites. The carrier just needs to provide the L2 connectivity for the user, while does not need to take part in the route calculation of the VPN user. Because of this feature, MPLS VPWS has better scalability than MPLS L3VPN. QTECH supports Martini MPLS VPWS, that is, make the LDP protocol distribute the label for the VC FEC via the expanded LDP protocol.

9.2. MPLS VPWS Function Configuration

Table 9-1 MPLS VPWS function configuration list

Configuration task	
Configure MPLS VPWS	Configure MPLS VPWS

9.2.1. Configure MPLS VPWS

Configuration Condition

Before configuring MPLS VPWS, first complete the following tasks:

- On the MPLS core network, ensure the IGP connectivity.
- On the MPLS core network, enable the label signaling protocol, and set up the global LSP.
- Enable the MPLS forwarding basic capability on the desired interface.

Configure MPLS VPWS

Martini expands the LDP protocol, and adds the VC FEC type in the LDP protocol, making the LDP distribute the VC label for the VC FEC. Besides, the two PE devices exchanging the VC label may be not directly connected, so LDP should use the peer PE address of the VPWS VC connection to set up the target session, and transmits the VC label on the session. When the label exchanging and binding between two PEs are complete, and the parameters are negotiated to be consistent, the PW between the two PEs is set up, and the CEs can transmit the L2 data via the PW. The MPLS VPWS realized by expanding the LDP signaling protocol can bear various link-layer protocols, but it is required that the link layer protocols of each site of the VPN are the same.

When MPLS VPWS bears the Ethernet link data, the MPLS VPWS VC connection created on the L3 interface can specify the **ethernet** or **vlan** mode:

- By default, the L3 Ethernet sub interface is **vlan** mode, and the parameter can be configured as the **ethernet** mode or **vlan** mode.
- By default, the L3 Ethernet main interface is the **ethernet** mode, and the parameter can only be specified as the **ethernet** mode.

Table 9-2 Configure MPLS VPWS

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the interface configuration mode	**interface** *interface-name*	Mandatory
Create the VPWS connection	**xconnect** *peer-address vc-id* **encapsulation mpls** [**ethernet** | **vlan**] [**preferred-path tunnel** *tunnel-id* [**disable-fallback**]]	Mandatory By default, do not create the VPWS connection on the interface.

Note:

- When configuring MPLS VPWS, it is necessary to confirm the interface type of the peer PE connecting CE, and ensure that the interface types of the two sides are consistent.
- It is necessary to plan VC ID, and ensure that the VC ID is unique globally, and cannot repeat with VPN ID or VC ID in the VPLS instance.
- For the meaning of the **ethernet** and **vlan** parameters when creating VPWS, refer to MPLS VPWS command manual.

9.2.2. Configure MPLS VPWS across Domain

Configuration Condition

Before configuring the MPLS VPWS across domain, first complete the following tasks:

- On the MPLS core network, ensure the IGP connectivity.
- On the MPLS core network, enable the label signaling protocol, and set up the global LSP.
- Enable the MPLS forwarding basic capability on the desired interface.

Configure Option-A across Domain

Option-A, also known as VRF-to-VRF, is the simplest way to realize VPN mutual access between ASs. VRF-to-VRF handles VPWS connectivity between ASs simply by regarding another ASBR as a CE device. The following figure describes an example of VRF-to-VRF VPWS across domain.

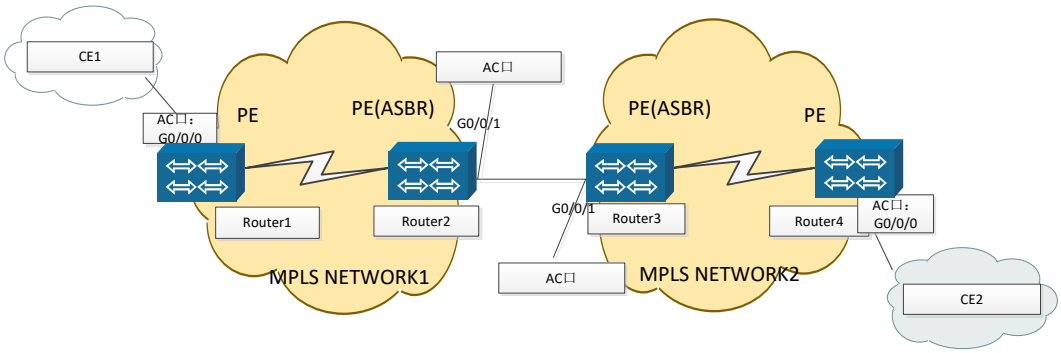

Figure 9-1 Configure VPWS Option-A across domain (VRF-to-VRF)

In the figure above, VPN A site 1 and site 2 are connected to two different service providers: AS1 and AS2, respectively. The service providers are connected through ASBR. Two AS regions configure the MPLS VPWS network. The VPN across AS needs the local ASBR to act as the PE device of VPN and the peer ASBR to act as the CE device of VPN. At the same time, the direct-connected interfaces of the two ASBR devices are the AC interfaces of the two AS regions, and their corresponding VPN IDs are different. The packets sent from CE1 to CE2 are transmitted transparently through the AS area 1, then through AS area 2, and at last, reach CE2, so as to realize the connection between site 1 and site 2.

The advantage of Option-A cross-domain mode is that there is no need to run MPLS between ASBRs. The disadvantage is that it allocates interfaces and links for each cross-domain VPN, and its scalability is poor.

Configure Option-B across Domain

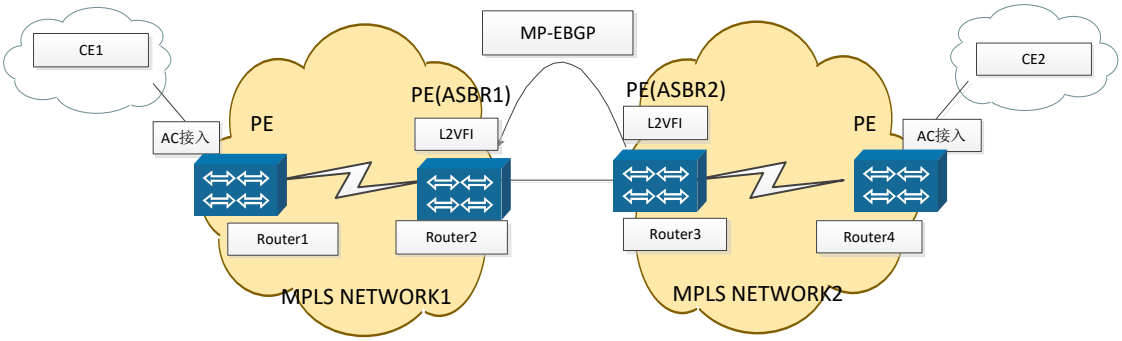

Figure 9-2 Configure Option-B across domain

Option-B across domain needs to run MP-EBGP between ASBRs, and you need to configure L2VFI on ASBR to build PW between ASBR and PE, and between ASBR and peer ASBR. EBGP is used to learn global routing between ASBRs and advertise global labels. LDP establishes PW between ASBRs to distribute labels for VC. At last, form two PWs on ASBR, one with PE and the other with ASBR. Finally, the packets sent by CE1 reach CE2 through AS1 and AS2.

The advantage of Option-B cross-domain mode is that it does not need ASBR to allocate interfaces for each VPN, but it needs to run MP-EBGP on ASRB and keep the routes advertised between the domains.

Table 9-3 Configure Option-B across domain

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enable the MPLS forwarding globally	**mpls ip**	Mandatory By default, do not enable the MPLS forwarding.
Enable the MPLS LDP globally	**mpls ldp**	Mandatory By default, do not enable MPLS LDP.
Configure L2VFI globally	**l2 vfi *vfi-name* point-to-point**	Mandatory By default, do not enable L2VFI.
Configure the PW with the PE or ASBR	**peer** *ip-address vcid* **encapsulation mpls**	Mandatory By default, do not enable function of setting up PW.
Enter the interface configuration mode	**interface** *interface_name*	-
Enable the MPLS forwarding on the interface	**mpls ip**	Mandatory Configure on the interconnection interface of two ASBRs. By default, do not enable the MPLS forwarding on the interface.
Return to the global configuration mode	**exit**	-

Step	Command	Description
Enable the BGP protocol and enter the BGP configuration mode	**router bgp** *autonomous-system*	-
Configure the peer ASBR as the EBGP neighbor	**neighbor** { *ipv4-address* | *peer-group-name* } **remote-as** *as-number*	Mandatory By default, do not configure any EBGP neighbor.
Configure advertising the label to the peer ASBR	**neighbor** *neighbor-address* **send-label**	Mandatory By default, do not configure advertising the label to the neighbor.

Note:

- The above only lists the basic configuration of Option-B across domain on ASBR. For the configuration between ASBR and the PE, P device in the local AS, refer to the chapter of “MPLS VPWS Typical Configuration Example”.

9.2.3. MPLS VPWS Monitoring and Maintaining

Table 9-4 MPLS VPWS monitoring and maintaining

Command	Description
show mpls forwarding-table l2-circuit [**ftn** [*vc-id*] **| ilm**] [**detail**]	Display the VPWS MPLS forwarding information
show mpls ldp l2-circuit [*vc-id*] [**detail**]	Display the VPWS information in the LDP protocol
show mpls ldp l2-circuit statistics	Display the VPWS statistics information in the LDP protocol
show ip bgp labels	Display the labels received from the peer and distributed for the IPv4 route

9.3. MPLS VPWS Typical Configuration Example

9.3.1. Configure Ethernet to Access Martini VPWS

Network Requirements

- In the whole MPLS network, there are two VPNs, VPN1 and VPN2; CE1 and CE3 belong VPN1; CE2 and CE4 belong to VPN2.
- On the PE, enable the VPWS function, and adopt LDP as the VPWS signaling to set up PW.
- CE is connected via Ethernet, realizing the communication between CEs in the same VPN. The CEs in different VPNs cannot communicate with each other.

Network Topology

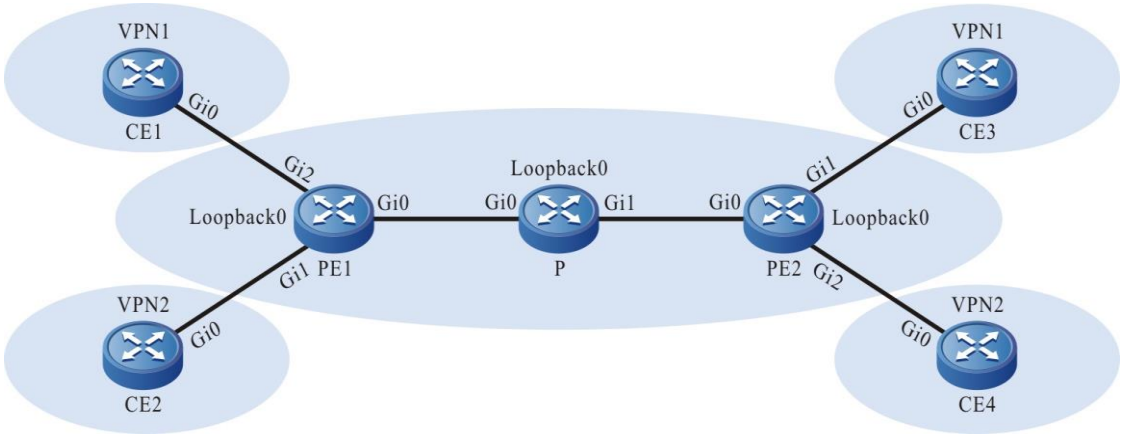

Figure 9-3 Configure Ethernet to access Martini VPWS

Device	Interface	IP Address	Device	Interface	IP Address
CE1	Gi0	1.0.0.1/24	P	Gi0	3.0.0.2/24
CE2	Gi0	1.0.0.2/24		Gi1	4.0.0.1/24
CE3	Gi0	1.0.0.3/24		Loopback0	11.0.0.1/32
CE4	Gi0	1.0.0.4/24	PE2	Gi0	4.0.0.2/24
PE1	Gi0	3.0.0.1/24		Loopback0	12.0.0.1/32
	Loopback0	10.0.0.1/32			

Configuration Steps

Step 1: Configure the IP address of the interface. (omitted)

Step 2: Configure the global OSPF, and advertise the global route.

##On PE1, configure the global OSPF.

```
PE1#configure terminal
PE1(config)#router ospf 100
PE1(config-ospf)#network 10.0.0.1 0.0.0.0 area 0
PE1(config-ospf)#network 3.0.0.0 0.0.0.255 area 0
PE1(config-ospf)#exit
```

##On P, configure the global OSPF.

```
P#configure terminal
P(config)#router ospf 100
P(config-ospf)#network 11.0.0.1 0.0.0.0 area 0
P(config-ospf)#network 3.0.0.0 0.0.0.255 area 0
P(config-ospf)#network 4.0.0.0 0.0.0.255 area 0
P(config-ospf)#exit
```

##On PE2, configure the global OSPF.

```
PE2#configure terminal
PE2(config)#router ospf 100
PE2(config-ospf)#network 12.0.0.1 0.0.0.0 area 0
PE2(config-ospf)#network 4.0.0.0 0.0.0.255 area 0
PE2(config-ospf)#exit
```

#After configuration, view the core route table on PE and P.

Take PE1 as an example:

```
PE1#show ip route
Codes: C - connected, S - static, R - RIP,  O - OSPF, OE-OSPF External, M - Management
    D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-ISIS

C   3.0.0.0/24 is directly connected, 00:17:14, gigabitethernet0
O   4.0.0.0/24 [110/2] via 3.0.0.2, 00:01:44, gigabitethernet0
C   127.0.0.0/8 is directly connected, 2860:10:17, lo0
C   10.0.0.1/32 is directly connected, 00:30:04, loopback0
O   11.0.0.1/32 [110/2] via 3.0.0.2, 00:01:22, gigabitethernet0
O   12.0.0.1/32 [110/3] via 3.0.0.2, 00:00:49, gigabitethernet0
```

You can see that there is the information of the route to loopback0 segment of P, PE2 in the route table of PE1.

Note:

- For the checking methods of P, PE2, refer to PE1.

Step 3: Enable MPLS IP and MPLS LDP.

#On PE1, enable the global MPLS IP and MPLS LDP, and meanwhile, enable MPLS IP and MPLS LDP on the interface.

```
PE1(config)#mpls ip
PE1(config)#mpls ldp
PE1(config-ldp)#router-id 10.0.0.1
PE1(config-ldp)#address-family ipv4
PE1(config-ldp-af4)#transport-address 10.0.0.1
PE1(config-ldp-af4)#exit
PE1(config-ldp)#exit
PE1(config)#interface gigabitethernet0
PE1(config-if-gigabitethernet0)#mpls ip
PE1(config-if-gigabitethernet0)#mpls ldp
PE1(config-if-gigabitethernet0)#exit
```

#On P, enable the global MPLS IP and MPLS LDP, and meanwhile, enable MPLS IP and MPLS LDP on the interface.

```
P(config)#mpls ip
P(config)#mpls ldp
P(config-ldp)#router-id 11.0.0.1
P(config-ldp)#address-family ipv4
P(config-ldp-af4)#transport-address 11.0.0.1
P(config-ldp-af4)#exit
P(config-ldp)#exit
P(config)#interface gigabitethernet0
P(config-if-gigabitethernet0)#mpls ip
P(config-if-gigabitethernet0)#mpls ldp
P(config-if-gigabitethernet0)#exit
P(config)#interface gigabitethernet1
P(config-if-gigabitethernet1)#mpls ip
P(config-if-gigabitethernet1)#mpls ldp
P(config-if-gigabitethernet1)#exit
```

#On PE2, enable the global MPLS IP and MPLS LDP, and meanwhile, enable MPLS IP and MPLS LDP on the interface.

```
PE2(config)#mpls ip
PE2(config)#mpls ldp
PE2(config-ldp)#router-id 12.0.0.1
PE2(config-ldp)#address-family ipv4
PE2(config-ldp-af4)#transport-address 12.0.0.1
PE2(config-ldp-af4)#exit
PE2(config-ldp)#exit
PE2(config)#interface gigabitethernet0
PE2(config-if-gigabitethernet0)#mpls ip
PE2(config-if-gigabitethernet0)#mpls ldp
PE2(config-if-gigabitethernet0)#exit
```

Note:

- router-id and transport-address can be configured manually and also can be generated automatically. Usually, they are configured to be the same. If not manually configuring router-id and transport-address, the device automatically select: from the up interfaces, first select the maximum IP address in the Loopback interfaces; if the device is not configured with the Loopback interface address, select the maximum IP address in the common interfaces.

#After configuration, view the LDP session information on PE and P.

Take PE1 as an example:

```
PE1#show mpls ldp session
Peer IP Address    Peer Type     My Role   State        DS Cap    DeadTime
11.0.0.1           Multicast     Active    OPERATIONAL  Disabled  00:02:43
Statistics for ldp sessions:
    Multicast sessions: 1
    Targeted sessions: 0
```

State is displayed as OPERATIONAL, indicating that the PE1 and P set up the LDP session successfully.

#View the route label information on the device.

Take PE1 as an example:

```
PE1#show ip route 11.0.0.1 detail
Codes: C - Connected, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
    U - Per-user Static route
    O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external
```

```
O   11.0.0.1/32 [110/2] via 3.0.0.2, label 3, 00:5:23, gigabitethernet0
```

```
                    3.0.0.2 [0], gigabitethernet0

PE1#show ip route 12.0.0.1 detail
Codes: C - Connected, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external



O   12.0.0.1/32 [110/2] via 3.0.0.2, label 24016, 00:5:23, gigabitethernet0
                    3.0.0.2 [0], gigabitethernet0
```

You can see that thee loopback port route from PE1 to P, PE2 has the label information.

Note:

- For the checking methods of P, PE2, refer to PE1.

Step 4: Configure VPWS.

#On the AC interface gigabitethernet1 and gigabitethernet2 of PE1, configure VPWS.

```
PE1(config)#interface gigabitethernet1
PE1(config-if-gigabitethernet1)#mpls ip
PE1(config-if-gigabitethernet1)#xconnect 12.0.0.1 2 encapsulation mpls ethernet
PE1(config-if-gigabitethernet1)#exit
PE1(config)#interface gigabitethernet2
PE1(config-if-gigabitethernet2)#mpls ip
PE1(config-if-gigabitethernet2)#xconnect 12.0.0.1 1 encapsulation mpls ethernet
PE1(config-if-gigabitethernet2)#exit
```

#On the AC interface gigabitethernet1 and gigabitethernet2 of PE2, configure VPWS.

```
PE2(config)#interface gigabitethernet1
PE2(config-if-gigabitethernet1)#mpls ip
PE2(config-if-gigabitethernet1)#xconnect 10.0.0.1 1 encapsulation mpls ethernet
PE2(config-if-gigabitethernet1)#exit
PE2(config)#interface gigabitethernet2
PE2(config-if-gigabitethernet2)#mpls ip
PE2(config-if-gigabitethernet2)#xconnect 10.0.0.1 2 encapsulation mpls ethernet
PE2(config-if-gigabitethernet2)#exit
```

#On PE, view the VPWS setup status.

Take PE1 as an example:

```
PE1#show mpls ldp l2-circuit
VC-ID    Interface        State  Type      Local-Label  Remote-Label  Destination-Address
1        gigabitethernet2 UP     ethernet  24016        24019         12.0.0.1
2        gigabitethernet1 UP     ethernet  24017        24016         12.0.0.1
```

Statistics for L2-circuit:

```
L2-circuit up: 2
L2-circuit down: 0
```

State is displayed as UP, indicating that the VPWS is set up successfully on PE1.

Note:

- For the checking method of PE2, refer to PE1.
- Enable the MPLS forwarding basic capability on the desired AC interface, and do not configure the IP address.

Step 5: Check the result.

#On the PE, view the MPLS forwarding table.

Take PE1 as an example:

```
PE1#show mpls forwarding-table
Pro: L - LDP, O - OSPF, B - MP-BGP, R - RSVP, M - Mapped-Route, S - Static Label,ML - mLDP (ML FEC: Root address/OT/OV), RM - RSVP P2MP (RM FEC: P2MP ID/TID)

Pro Ident     FEC            Inlabel Outlabel Outgoing        Next hop
L   -VC-      2              /       24016    gigabitethernet0 12.0.0.1
L   -VC-      1              /       24019    gigabitethernet0 12.0.0.1
L   -VC-      1              24016   /        gigabitethernet2 12.0.0.1
L   -VC-      2              24017   /        gigabitethernet1 12.0.0.1
L   global    11.0.0.1/32    24018   3        gigabitethernet0 3.0.0.2
L   global    12.0.0.1/32    24019   24017    gigabitethernet0 3.0.0.2
```

You can see that there are the VPWS entries in the MPLS forwarding table of PE1.

Note:

- For the checking method of PE2, refer to PE1.

#On CE1, ping the gigabitethernet0 address of CE3, and the ping can be connected.

```
CE1#ping 1.0.0.3
```

```
Press key (ctrl + shift + 6) interrupt it.
Sending 5, 76-byte ICMP Echos to 1.0.0.3 , timeout is 2 seconds:
!!!!!
Success rate is 100% (5/5). Round-trip min/avg/max = 0/3/16 ms.
```

#On CE1, ping the gigabitethernet0 address of CE4, and the ping cannot be connected.

```
CE1#ping 1.0.0.4

Press key (ctrl + shift + 6) interrupt it.
Sending 5, 76-byte ICMP Echos to 1.0.0.4 , timeout is 2 seconds:
.....
Success rate is 0% (0/5).
```

#On CE2, ping the gigabitethernet0 address of CE4, and the ping can be connected.

```
CE2#ping 1.0.0.4

Press key (ctrl + shift + 6) interrupt it.
Sending 5, 76-byte ICMP Echos to 1.0.0.4 , timeout is 2 seconds:
!!!!!
Success rate is 100% (5/5). Round-trip min/avg/max = 0/3/16 ms.
```

#On CE2, ping the gigabitethernet0 address of CE3, and the ping cannot be connected.

```
CE2#ping 1.0.0.3

Press key (ctrl + shift + 6) interrupt it.
Sending 5, 76-byte ICMP Echos to 1.0.0.3 , timeout is 2 seconds:
.....
Success rate is 0% (0/5).
```

You can see that the CE devices in the same VPN can communicate with each other, and the CE devices in different VPNs cannot communicate with each other.

9.3.2. Configure Vlan to Access Martini VPWS

Network Requirements

- In the whole MPLS network, there are two VPNs, VPN1 and VPN2; CE1 and CE3 belong VPN1; CE2 and CE4 belong to VPN2.
- On the PE, enable the VPWS function, and adopt LDP as the VPWS signaling to set up PW.

- CE is connected via Vlan, realizing the communication between CEs in the same VPN. The CEs in different VPNs cannot communicate with each other.

Network Topology

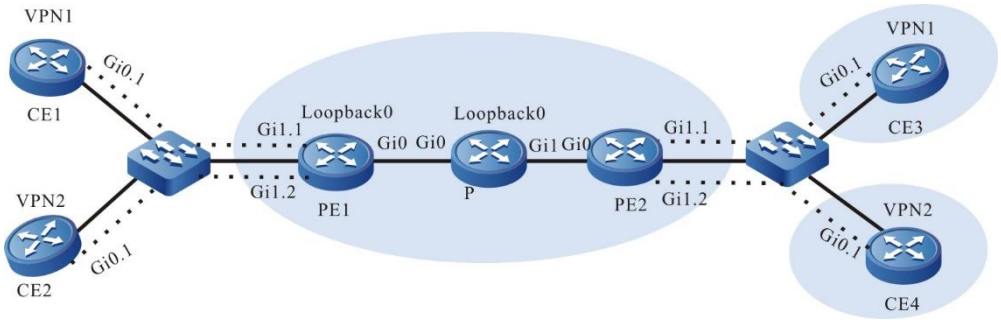

Figure 9-4 Configure Vlan to access Martini VPWS

Device	Interface	IP Address	Device	Interface	IP Address
CE1	Gi0.1	1.0.0.1/24	P	Gi0	3.0.0.2/24
CE2	Gi0.1	1.0.0.2/24		Gi1	4.0.0.1/24
CE3	Gi0.1	1.0.0.3/24		Loopback0	11.0.0.1/32
CE4	Gi0.1	1.0.0.4/24	PE2	Gi0	4.0.0.2/24
PE1	Gi0	3.0.0.1/24		Loopback0	12.0.0.1/32
	Loopback0	10.0.0.1/32			

Configuration Steps

Step 1: Configure the IP address of the interface. (omitted)

Step 2: Configure the global OSPF, and advertise the global route.

##On PE1, configure the global OSPF.

```
PE1#configure terminal
PE1(config)#router ospf 100
PE1(config-ospf)#network 10.0.0.1 0.0.0.0 area 0
PE1(config-ospf)#network 3.0.0.0 0.0.0.255 area 0
PE1(config-ospf)#exit
```

##On P, configure the global OSPF.

```
P#configure terminal
P(config)#router ospf 100
P(config-ospf)#network 11.0.0.1 0.0.0.0 area 0
P(config-ospf)#network 3.0.0.0 0.0.0.255 area 0
P(config-ospf)#network 4.0.0.0 0.0.0.255 area 0
P(config-ospf)#exit
```

##On PE2, configure the global OSPF.

```
PE2#configure terminal
PE2(config)#router ospf 100
PE2(config-ospf)#network 12.0.0.1 0.0.0.0 area 0
PE2(config-ospf)#network 4.0.0.0 0.0.0.255 area 0
PE2(config-ospf)#exit
```

#After configuration, view the core route table on PE and P.

Take PE1 as an example:

```
PE1#show ip route
Codes: C - connected, S - static, R - RIP,  O - OSPF, OE-OSPF External, M - Management
    D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-ISIS

C   3.0.0.0/24 is directly connected, 00:17:14, gigabitethernet0
O   4.0.0.0/24 [110/2] via 3.0.0.2, 00:01:44, gigabitethernet0

C   127.0.0.0/8 is directly connected, 2860:10:17, lo0
C   10.0.0.1/32 is directly connected, 00:30:04, loopback0
O   11.0.0.1/32 [110/2] via 3.0.0.2, 00:01:22, gigabitethernet0
O   12.0.0.1/32 [110/3] via 3.0.0.2, 00:00:49, gigabitethernet0
```

You can see that there is the information of the route to loopback0 segment of P, PE2 in the route table of PE1.

Note:

- For the checking methods of P, PE2, refer to PE1.

Step 3: Enable MPLS IP and MPLS LDP.

#On PE1, enable the global MPLS IP and MPLS LDP, and meanwhile, enable MPLS IP and MPLS LDP on the interface.

```
PE1(config)#mpls ip
```

```
PE1(config)#mpls ldp
PE1(config-ldp)#router-id 10.0.0.1
PE1(config-ldp)#address-family ipv4
PE1(config-ldp-af4)#transport-address 10.0.0.1
PE1(config-ldp-af4)#exit
PE1(config-ldp)#exit
PE1(config)#interface gigabitethernet0
PE1(config-if-gigabitethernet0)#mpls ip
PE1(config-if-gigabitethernet0)#mpls ldp
PE1(config-if-gigabitethernet0)#exit
```

#On P, enable the global MPLS IP and MPLS LDP, and meanwhile, enable MPLS IP and MPLS LDP on the interface.

```
P(config)#mpls ip
P(config)#mpls ldp
P(config-ldp)#router-id 11.0.0.1
P(config-ldp)#address-family ipv4
P(config-ldp-af4)#transport-address 11.0.0.1
P(config-ldp-af4)#exit
P(config-ldp)#exit
P(config)#interface gigabitethernet0
P(config-if-gigabitethernet0)#mpls ip
P(config-if-gigabitethernet0)#mpls ldp
P(config-if-gigabitethernet0)#exit
P(config)#interface gigabitethernet1
P(config-if-gigabitethernet1)#mpls ip
P(config-if-gigabitethernet1)#mpls ldp
P(config-if-gigabitethernet1)#exit
```

#On PE2, enable the global MPLS IP and MPLS LDP, and meanwhile, enable MPLS IP and MPLS LDP on the interface.

```
PE2(config)#mpls ip
PE2(config)#mpls ldp
PE2(config-ldp)#router-id 12.0.0.1
PE2(config-ldp)#address-family ipv4
PE2(config-ldp-af4)#transport-address 12.0.0.1
PE2(config-ldp-af4)#exit
PE2(config-ldp)#exit
PE2(config)#interface gigabitethernet0
```

```
PE2(config-if-gigabitethernet0)#mpls ip
PE2(config-if-gigabitethernet0)#mpls ldp
PE2(config-if-gigabitethernet0)#exit
```

Note:

- router-id and transport-address can be configured manually and also can be generated automatically. Usually, they are configured to be the same. If not manually configuring router-id and transport-address, the device automatically select: from the up interfaces, first select the maximum IP address in the Loopback interfaces; if the device is not configured with the Loopback interface address, select the maximum IP address in the common interfaces.

#After configuration, view the LDP session information on PE and P.

Take PE1 as an example:

```
PE1#show mpls ldp session
Peer IP Address    Peer Type     My Role   State        DS Cap    DeadTime
11.0.0.1           Multicast     Active    OPERATIONAL  Disabled  00:02:43
Statistics for ldp sessions:
    Multicast sessions: 1
    Targeted sessions: 0
```

State is displayed as OPERATIONAL, indicating that the PE1 and P set up the LDP session successfully.

#View the route label information on the device.

Take PE1 as an example:

```
PE1#show ip route 11.0.0.1 detail
Codes: C - Connected, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
    U - Per-user Static route
    O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external



O   11.0.0.1/32 [110/2] via 3.0.0.2, label 3, 00:5:23, gigabitethernet0
                        3.0.0.2 [0], gigabitethernet0


PE1#show ip route 12.0.0.1 detail
Codes: C - Connected, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
    U - Per-user Static route
    O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external
```

```
O   12.0.0.1/32 [110/2] via 3.0.0.2, label 24017, 00:5:23, gigabitethernet0
                        3.0.0.2 [0], gigabitethernet0
```

You can see that the loopback port route from PE1 to P, PE2 has the label information.

Note:

- For the checking methods of P, PE2, refer to PE1.

Step 4: Configure VPWS.

#Configure VPWS on the AC interface gigabitethernet1.1 and gigabitethernet1.2 of PE1.

```
PE1(config)#interface gigabitethernet1.1
PE1(config-if-gigabitethernet1.1)encapsulation dot1q 100
PE1(config-if-gigabitethernet1.1)#mpls ip
PE1(config-if-gigabitethernet1.1)#xconnect 12.0.0.1 1 encapsulation mpls vlan
PE1(config-if-gigabitethernet1.1)#exit
PE1(config)#interface gigabitethernet1.2
PE1(config-if-gigabitethernet1.2)encapsulation dot1q 200
PE1(config-if-gigabitethernet1.2)#mpls ip
PE1(config-if-gigabitethernet1.2)#xconnect 12.0.0.1 2 encapsulation mpls vlan
PE1(config-if-gigabitethernet1.2)#exit
```

#Configure VPWS on the AC interface gigabitethernet1.1 and gigabitethernet1.2 of PE2.

```
PE2(config)#interface gigabitethernet1.1
PE2(config-if-gigabitethernet1.1)encapsulation dot1q 100
PE2(config-if-gigabitethernet1.1)#mpls ip
PE2(config-if-gigabitethernet1.1)#xconnect 10.0.0.1 1 encapsulation mpls vlan
PE2(config-if-gigabitethernet1.1)#exit
PE2(config)#interface gigabitethernet1.2
PE2(config-if-gigabitethernet1.2)encapsulation dot1q 200
PE2(config-if-gigabitethernet1.2)#mpls ip
PE2(config-if-gigabitethernet1.2)#xconnect 10.0.0.1 2 encapsulation mpls vlan
PE2(config-if-gigabitethernet1.2)#exit
```

#On PE, view the VPWS setup status.

Take PE1 as an example:

```
PE1#show mpls ldp l2-circuit
VC-ID   Interface          State  Type  Local-Label  Remote-Label  Destination-
Address
1       gigabitethernet1.1 UP     vlan  24016        24019         12.0.0.1
```

```
2       gigabitethernet1.2  UP      vlan   24017        24016        12.0.0.1
Statistics for L2-circuit:
    L2-circuit up: 2
    L2-circuit down: 0
```

State is displayed as UP, indicating that the VPWS is set up successfully on PE1.

Note:

- For the checking method of PE2, refer to PE1.
- Enable the MPLS forwarding basic capability on the desired AC interface, and do not configure the IP address.

Step 5: Check the result.

#On the PE, view the MPLS forwarding table.

Take PE1 as an example:

```
PE1#show mpls forwarding-table
Pro: L - LDP, O - OSPF, B - MP-BGP, R - RSVP, M - Mapped-Route, S - Static Label,ML - mLDP (ML FEC: Root address/OT/OV), RM - RSVP P2MP (RM FEC: P2MP ID/TID)

Pro Ident       FEC             Inlabel Outlabel Outgoing       Next hop
L   -VC-        2               /       24016    gigabitethernet0    12.0.0.1
L   -VC-        1               /       24019    gigabitethernet0    12.0.0.1
L   -VC-        1               24016   /        gigabitethernet2    12.0.0.1
L   -VC-        2               24017   /        gigabitethernet1    12.0.0.1
L   global      11.0.0.1/32     24018   3        gigabitethernet0    3.0.0.2
L   global      12.0.0.1/32     24019   24017    gigabitethernet0    3.0.0.2
```

You can see that there are the VPWS entries in the MPLS forwarding table of PE1.

Note:

- For the checking method of PE2, refer to PE1.

#On CE1, ping the gigabitethernet0.1 address of CE3, and the ping can be connected.

```
CE1#ping 1.0.0.3

Press key (ctrl + shift + 6) interrupt it.
Sending 5, 76-byte ICMP Echos to 1.0.0.3 , timeout is 2 seconds:
!!!!!
Success rate is 100% (5/5). Round-trip min/avg/max = 0/3/16 ms.
```

#On CE1, ping the gigabitethernet0.1 address of CE4, and the ping cannot be connected.

```
CE1#ping 1.0.0.4

Press key (ctrl + shift + 6) interrupt it.
Sending 5, 76-byte ICMP Echos to 1.0.0.4 , timeout is 2 seconds:
.....
Success rate is 0% (0/5).
```

#On CE2, ping the gigabitethernet0.1 address of CE3, and the ping can be connected.

```
CE2#ping 1.0.0.4

Press key (ctrl + shift + 6) interrupt it.
Sending 5, 76-byte ICMP Echos to 1.0.0.4 , timeout is 2 seconds:
!!!!!
Success rate is 100% (5/5). Round-trip min/avg/max = 0/3/16 ms.
```

#On CE2, ping the gigabitethernet0.1 address of CE3, and the ping cannot be connected.

```
CE2#ping 1.0.0.3

Press key (ctrl + shift + 6) interrupt it.
Sending 5, 76-byte ICMP Echos to 1.0.0.3 , timeout is 2 seconds:
.....
Success rate is 0% (0/5).
```

You can see that the CE devices in the same VPN can communicate with each other, and the CE devices in different VPNs cannot communicate with each other.

10. ОБЩАЯ ИНФОРМАЦИЯ

10.1. Замечания и предложения

Мы всегда стремимся улучшить нашу документацию и помочь вам работать лучше, поэтому мы хотим услышать вас. Мы всегда рады обратной связи, в особенности:

- ошибки в содержании, непонятные или противоречащие места в тексте;
- идеи по улучшению документации, чтобы находить информацию быстрее;
- неработающие ссылки и замечания к навигации по документу.

Если вы хотите написать нам по поводу данного документа, то используйте, пожалуйста, форму обратной связи на qtech.ru.

10.2. Гарантия и сервис

Процедура и необходимые действия по вопросам гарантии описаны на сайте QTECH в разделе «Поддержка» −> «Гарантийное обслуживание».

Ознакомиться с информацией по вопросам тестирования оборудования можно на сайте QTECH в разделе «Поддержка» −> «Взять оборудование на тест».

Вы можете написать напрямую в службу сервиса по электронной почте sc@qtech.ru.

10.3. Техническая поддержка

Если вам необходимо содействие в вопросах, касающихся нашего оборудования, то можете воспользоваться нашей автоматизированной системой запросов технического сервис-центра helpdesk.qtech.ru.

Телефон Технической поддержки +7 (495) 797-33-11 доб. 0