Contents

Configuring MPLS L2VPN

MPLS L2VPN provides point-to-point and point-to-multipoint connections. This chapter describes only the MPLS L2VPN technologies that provide point-to-point connections. For information about the MPLS L2VPN technologies that provide point-to-multipoint connections, see "Configuring VPLS."

About MPLS L2VPN

MPLS L2VPN is an implementation of Pseudo Wire Emulation Edge-to-Edge (PWE3). It offers Layer 2 VPN services over an MPLS or IP backbone. MPLS L2VPN can transparently transmit Layer 2 data for different data link layer protocols such as Ethernet and ATM.

Basic concepts of MPLS L2VPN

CE

A customer edge (CE) is a customer device directly connected to the service provider network.

PE

A provider edge (PE) is a service provider device connected to one or more CEs. It provides VPN access by mapping and forwarding packets between user networks and public tunnels.

AC

An attachment circuit (AC) is a link between a CE and a PE, such as an FR DLCI, ATM VPI/VCI, Ethernet interface, VLAN, or PPP connection.

PW

A Pseudowire (PW) is a virtual bidirectional connection between two PEs. An MPLS PW comprises a pair of LSPs in opposite directions.

Public tunnel

A public tunnel is a connection that carries one or more PWs across the MPLS or IP backbone. It can be an LSP tunnel, an MPLS TE tunnel, or a GRE tunnel.

Cross-connect

A cross-connect connects two physical or virtual circuits such as ACs and PWs. It switches packets between the two physical or virtual circuits. Cross-connects include AC to AC cross-connect, AC to PW cross-connect, and PW to PW cross-connect.

Site ID

A site ID uniquely identifies a site in a VPN. Sites in different VPNs can have the same site ID.

RD

A route distinguisher (RD) is added before a site ID to distinguish the sites that have the same site ID but reside in different VPNs. An RD and a site ID uniquely identify a VPN site.

Label block

A label block is a set of labels. It includes the following parameters:

- **Label base**—The LB specifies the initial label value of the label block. A PE automatically selects an LB value that cannot be manually modified.

- **Label range**—The LR specifies the number of labels that the label block contains. The LB and LR determine the labels contained in the label block. For example, if the LB is 1000 and the LR is 5, the label block contains labels 1000 through 1004.
- **Label-block offset**—The LO specifies the offset of a label block. If the existing label block becomes insufficient as the VPN sites increase, you can add a new label block to enlarge the label range. A PE uses an LO to identify the position of the new label block. The LO value of a label block is the sum of the LRs of all previously assigned label blocks. For example, if the LR and LO of the first label block are 10 and 0, the LO of the second label block is 10. If the LR of the second label block is 20, the LO of the third label block is 30.

A label block with LB, LO, and LR as 1000, 10, and 5, respectively, is represented as 1000/10/5.

For example, a VPN has 10 sites, and a PE assigns the first label block LB1/0/10 to the VPN. When another 15 sites are added, the PE keeps the first label block and assigns the second label block LB2/10/15 to extend the network. LB1 and LB2 are the initial label values that are randomly selected by the PE.

Route target

PEs use the BGP route target attribute (also called VPN target attribute) to manage BGP L2VPN information advertisement. PEs support the following types of route target attributes:

- **Export target attribute**—When a PE sends L2VPN information to the peer PE in a BGP update message, it sets the route target attribute in the update message to an export target. L2VPN information includes the site ID, RD, and label block.
- **Import target attribute**—When a PE receives an update message from the peer PE, it checks the route target attribute in the update message. If the route target value matches an import target, the PE accepts the L2VPN information in the update message.

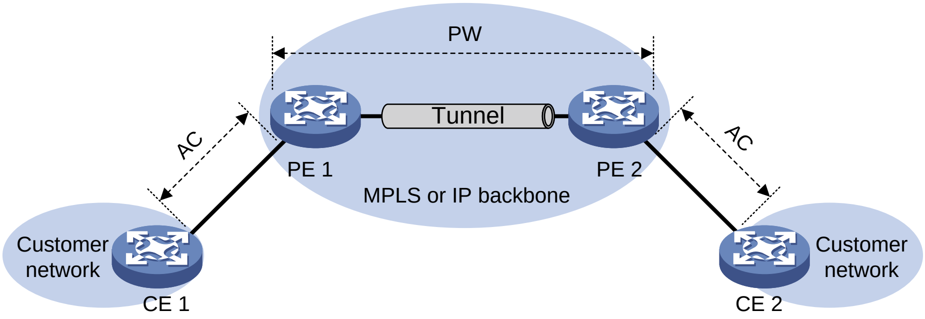
Route target attributes determine from which PEs a PE can receive L2VPN information.

MPLS L2VPN network models

MPLS L2VPN network models include the remote connection and local connection models.

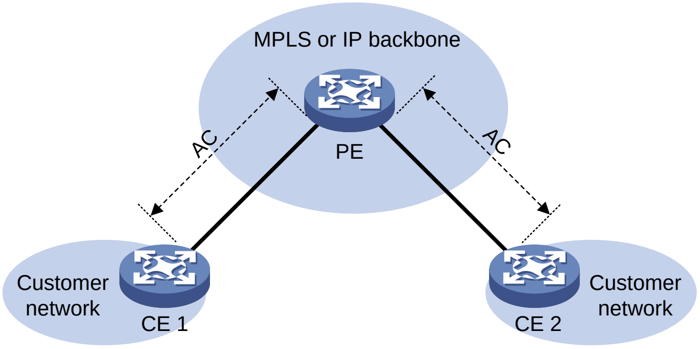
As shown in Figure 1, the remote connection model connects two CEs through a PW on an MPLS or IP backbone.

Figure 1 Remote connection model



As shown in Figure 2, the local connection model connects two CEs to the same PE so the CEs can communicate through the PE.

Figure 2 Local connection model



The local connection model is not supported in the current software version.

Remote connection establishment

To set up a remote MPLS L2VPN connection:

1. Set up a public tunnel to carry one or more PWs between PEs.
2. Set up a PW to connect customer networks.
3. Set up an AC between a PE and a CE.
4. Bind the AC to the PW.

After the PE receives packets from the AC, it adds the PW label into the packets and sends the packets to the peer PE through the public tunnel.

After the peer PE receives the packets from the public tunnel, it removes the PW label of the packets and forwards the packets to the AC bound to the PW.

Setting up a public tunnel

The public tunnel can be an LSP, MPLS TE, or GRE tunnel.

If multiple public tunnels exist between two PEs, you can configure a tunnel policy to control tunnel selection. For more information about tunnel policies, see "Configuring tunnel policies."

If a PW is established over an LSP or MPLS TE tunnel, packets on the PW have two labels. The outer label is the public LSP or MPLS TE tunnel label that MPLS uses to forward the packet to the peer PE. The inner label is the PW label that the peer PE uses to forward the packet to the destination CE.

Setting up a PW

PWs include static PWs, LDP PWs, BGP PWs, and Circuit Cross Connect (CCC) PWs.

- Static PW establishment

  To establish a static PW, configure the peer PE address, and the incoming and outgoing PW labels for the PW on the two PEs. Static PWs consume a small amount of resources but have complex configurations.

- LDP PW establishment

  To establish an LDP PW, configure LDP and specify the peer PE address on the two PEs. LDP defines a new FEC type named PW ID FEC for PEs to exchange PW-label bindings. The new FEC type uses a PW ID and a PW data encapsulation type to identify a PW. The PW ID is the ID of the PW between PEs. The PW data encapsulation type specifies the encapsulation type for data transmitted over the PW, such as ATM, FR, Ethernet, or VLAN. PEs advertise the PW label and PW ID FEC in label mapping messages to create a PW. Dynamic PWs have simple configurations but consume more resources than static PWs.

- BGP PW establishment

To establish BGP PWs, BGP advertises label block information in an extended BGP update to PEs in the same VPN. Each PE uses the received label block information to calculate outgoing labels and uses its own label block to calculate incoming labels. After two PEs complete label calculation, a BGP PW is established between them.

BGP PWs have the following features:

  - **Simplified configuration**—There is no need to manually specify peer PEs. A PE automatically find peer PEs after receiving label block information from the peer PEs.
  - **Reduced workload**—Label block advertisement enables assigning labels for multiple PWs at one time.

- CCC PW establishment

  To establish a CCC PW, manually specify the incoming and outgoing labels for the PW on the PEs, and create two static LSPs in opposite directions on P devices between PEs. There is no need to configure a public tunnel for the CCC PW. CCC employs only one level of label to transfer packets. The static LSPs on the P devices transfer data only for the CCC PW. They cannot be used by other connections or MPLS L3VPN.

Setting up an AC

Set up an AC by configuring a link layer connection between a PE and a CE.

An AC is an Ethernet service instance on a Layer 2 Ethernet interface or Layer 2 aggregate interface. It forwards packets that are received on the interface and meet the match criteria of the Ethernet service instance to the bound PW. If the match criterion is VLAN ID, the VLAN is unique on a per interface basis rather than on a global basis.

NOTE:

When VLANs are globally unique, packets with the same VLAN ID are forwarded over the PW bound with that VLAN ID regardless of the receiving interfaces. If VLANs are unique on a per interface basis, packets with the same VLAN ID from different interfaces can be forwarded over different PWs.

Binding the AC to the PW

Bind the Ethernet service instance to the PW, so the PE forwards packets between the AC and the PW.

PW data encapsulation types

MPLS L2VPN transports Layer 2 data of different data link layer protocols through PWs. A PE encapsulates a Layer 2 packet received from an AC according to the PW data encapsulation type.

Relationship between AC types and PW data encapsulation types

The PW data encapsulation type is determined by the link type of the AC, as shown in Table 1.

Table 1 Relationship between AC types and PW data encapsulation types

AC type	PW data encapsulation type
Ethernet	Ethernet
	VLAN

Ethernet over MPLS

Ethernet over MPLS uses MPLS L2VPN to connect Ethernets, and delivers Ethernet packets through a PW over the MPLS backbone.

The following PW data encapsulation types are available for Ethernet over MPLS:

- **Ethernet**—P-tag is not transferred on a PW.
    - For a packet from a CE:
        - If the packet contains a P-tag, the PE removes the P-tag, and adds a PW label and an outer tag into the packet before forwarding it.
        - If the packet contains no P-tag, the PE directly adds a PW label and an outer tag into the packet before forwarding it.
    - For a packet to a CE:
        - If the access mode is configured as VLAN by using the **ac interface** command, the PE adds a P-tag into the packet before sending it to the CE.
        - If the access mode is configured as Ethernet by using the **ac interface** command, the PE directly sends the packet to the CE.

    You cannot rewrite or remove existing tags.
- **VLAN**—Packets transmitted over a PW must carry a P-tag.
    - For a packet from a CE:
        - If the peer PE does not require the ingress to rewrite the P-tag, the PE keeps the P-tag unchanged for the packet, and then encapsulates the packet. If the packet contains no P-tag, the PE adds a null label (the label value is 0) into the packet, and then encapsulates the packet.
        - If the peer PE requires the ingress to rewrite the P-tag, the PE changes the P-tag to the expected VLAN tag (the tag value might be 0), and then adds a PW label and an outer tag into the packet. If the packet contains no P-tag, the PE adds a VLAN tag expected by the peer PE (the tag value might be 0), and then adds a PW label and an outer tag into the packet.
    - For a packet to a CE:
        - If the access mode is configured as VLAN by using the **ac interface** command, the PE rewrites or retains the P-tag before forwarding the packet.
        - If the access mode is configured as Ethernet by using the **ac interface** command, the PE removes the P-tag before forwarding the packet.

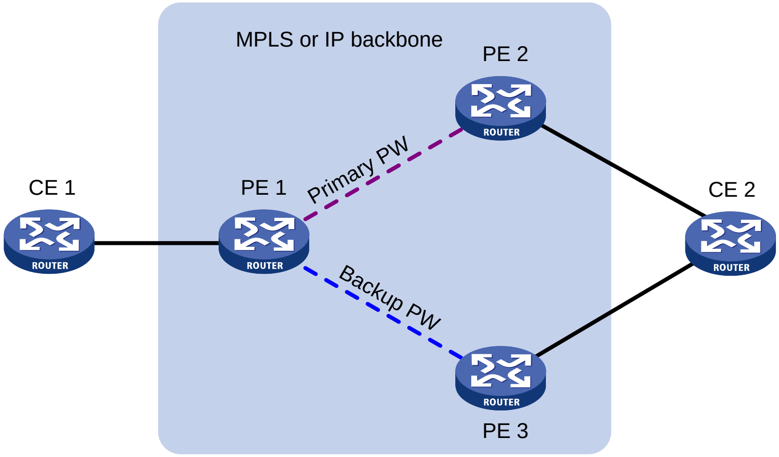
Ethernet over MPLS supports the following modes:

- **VLAN mode**—A Layer 3 Ethernet subinterface is bound to a PW. Packets received from the VLAN are forwarded through the bound PW. The peer PE can modify the VLAN tag as needed. The default PW data encapsulation type for VLAN mode is VLAN.
- **Flexible mode**—An Ethernet service instance on a Layer 2 Ethernet interface or Layer 2 aggregate interface is bound to a PW. Packets that are received from the interface and meet the match criteria of the Ethernet service instance are forwarded through the bound PW. You can configure flexible match criteria for the Ethernet service instance. For example, configure the Ethernet service instance to match all packets, tagged packets, or untagged packets. The default PW data encapsulation type for flexible mode is VLAN. Flexible mode can also implement the port and VLAN modes through match criteria configuration.

PW redundancy

PW redundancy provides redundant links between PEs so that the customer networks can communicate when the path over one PW fails. As shown in Figure 3, PE 1 establishes two PWs (one primary and one backup). The CEs communicate through the primary PW. When the primary PW fails, PE 1 brings up the backup PW and forwards packets from CE 1 to CE 2 through the backup PW. When CE 2 receives the packets, it updates its MAC address table, so that packets from CE 2 to CE 1 also travel through the backup PW. Only static PWs and LDP PWs support PW redundancy.

Figure 3 PW redundancy



The MPLS L2VPN determines whether the primary PW fails according to the LDP session status or the BFD result. The backup PW is used when one of the following conditions exists:

- The public tunnel of the primary PW is deleted, or BFD detects that the public tunnel has failed.
- The primary PW is deleted because the LDP session between PEs goes down, or BFD detects that the primary PW has failed.
- A manual PW switchover is performed.

A PW can be in either of the following states:

- **Active**—The PW is in active state and can forward packets.
- **Standby**—The PW is in standby state and cannot forward packets.

For LDP PWs, PEs use LDP to negotiate the states of the primary and backup PWs. In master/slave mode of PW redundancy, one PE of a PW operates as the master node and the other PE operates as the slave node. The master PE determines the PW state and then uses LDP to advertise the PW state to the slave PE. The slave PE uses the same PW state as the master PE based on the information received from the master PE. In this way, the master and slave PEs for the set of redundant PWs can use the same active PW to forward user packets.

MPLS L2VPN tasks at a glance

Configuring a remote connection

1. Enabling L2VPN
2. Configuring an AC

   Configuring an Ethernet service instance on an interface
3. Configuring a cross-connect
4. Configuring a PW

   Configure a static PW, LDP PW, BGP PW, and remote CCC connection as needed.
   - (Optional.) Configuring a PW class
   - Configuring a static PW
   - Configuring an LDP PW
   - Configuring a BGP PW
   - Configuring a remote CCC connection
5. Binding an AC to a cross-connect

6. (Optional.) Improving the MPLS L2VPN network reliability
   Configuring PW redundancy
7. (Optional.) Enabling SNMP notifications for L2VPN PW

Prerequisites for MPLS L2VPN

To establish an MPLS L2VPN, you must perform the following tasks:

1. Configure an IGP to achieve IP connectivity within the backbone.
2. Configure basic MPLS, LDP, GRE, or MPLS TE to set up public tunnels across the backbone.

Enabling L2VPN

Prerequisites

Before you enable L2VPN, perform the following tasks:

- Configure an LSR ID for the PE with the **`mpls lsr-id`** command.
- Enable MPLS with the **`mpls enable`** command on the core-facing interface of the PE.

For more information about the **`mpls lsr-id`** and **`mpls enable`** commands, see *MPLS Command Reference*.

Procedure

1. Enter system view.
   ```
   system-view
   ```
2. Enable L2VPN.
   ```
   l2vpn enable
   ```
   By default, L2VPN is disabled.

Configuring an Ethernet service instance on an interface

About configuring an Ethernet service instance on an interface

When the PE is connected to a CE through a Layer 2 Ethernet interface or Layer 2 aggregate interface, you can configure an Ethernet service instance on the interface to match packets for the AC.

Restrictions and guidelines

For information about configuring the match criterion of an Ethernet service instance by using the **`encapsulation`** command, see MPLS L2VPN commands in *MPLS Command Reference*.

Procedure

1. Enter system view.
   ```
   system-view
   ```
2. Enter interface view.
   - Enter Layer 2 Ethernet interface view.
     ```
     interface interface-type interface-number
     ```
   - Enter Layer 2 aggregate interface view.

interface bridge-aggregation *interface-number*

3. Create an Ethernet service instance and enter Ethernet service instance view.

   service-instance *instance-id*

4. Configure a packet match criterion for the Ethernet service instance.

   - Match packets with the specified outer VLAN IDs.

     encapsulation s-vid *vlan-id* [**only-tagged**]

     encapsulation s-vid *vlan-id-list*

   - Match packets with the specified outer VLAN IDs and the specified inner VLAN IDs.

     encapsulation s-vid *vlan-id-list* **c-vid** *vlan-id-list*

   - Match packets that have a VLAN tag or packets that do not have a VLAN tag.

     encapsulation { **tagged** | **untagged** }

   - Match packets that do not match any other Ethernet service instances on the interface.

     encapsulation default

     On an interface, you can configure the **default** criterion in only one Ethernet service instance. The Ethernet service instance matches all packets if it is the only instance on the interface.

   By default, no packet match criterion is configured.

Configuring a cross-connect

1. Enter system view.

   system-view

2. Create a cross-connect group and enter cross-connect group view.

   xconnect-group *group-name*

3. (Optional.) Configure a description for the cross-connect group.

   description *text*

   By default, no description is configured for a cross-connect group.

4. (Optional.) Enable the cross-connect group.

   undo shutdown

   By default, the cross-connect group is enabled.

5. Create a cross-connect and enter cross-connect view.

   connection *connection-name*

6. (Optional.) Set an MTU for the PW.

   mtu *size*

   The default MTU is 1500 bytes.

   The two PEs on an LDP PW must have the same MTU configured for the PW. Otherwise, the PW cannot come up.

Configuring a PW

Configuring a PW class

About configuring a PW class

You can configure PW attributes such as the PW data encapsulation type. PWs with the same attributes can use the same PW class.

Procedure

1. Enter system view.

   `system-view`

2. Create a PW class and enter PW class view.

   pw-class *class-name*

   By default, no PW classes exist.

3. Specify the PW data encapsulation type.

   pw-type { **ethernet** | **vlan** }

   By default, the PW data encapsulation type is VLAN.

Configuring a static PW

1. Enter system view.

   `system-view`

2. Enter cross-connect group view.

   xconnect-group *group-name*

3. Enter cross-connect view.

   connection *connection-name*

4. Configure a static PW, and enter cross-connect PW view.

   peer *ip-address* **pw-id** *pw-id* **in-label** *label-value* **out-label** *label-value* [**pw-class** *class-name* | **tunnel-policy** *tunnel-policy-name*] *

Configuring an LDP PW

About configuring an LDP PW

After an LDP PW is created, the PE automatically sends a targeted hello to create an LDP session to the peer PE. Then, the PE exchanges the PW ID FEC and PW label mapping with the peer.

Prerequisites

Before you configure an LDP PW, enable global and interface MPLS LDP on the PE. For information about MPLS LDP configuration, see "Configuring LDP."

Procedure

1. Enter system view.

   `system-view`

2. Enter cross-connect group view.

   xconnect-group *group-name*

3. Enter cross-connect view.

connection *connection-name*

4. Configure an LDP PW, and enter cross-connect PW view.

   peer *ip-address* **pw-id** *pw-id* [**pw-class** *class-name* | **tunnel-policy** *tunnel-policy-name*] *

Configuring a BGP PW

Configuring BGP to advertise MPLS L2VPN label block information

1. Enter system view.

   system-view

2. Enable BGP instance and enter BGP instance view.

   bgp *as-number* [**instance** *instance-name*]

   By default, BGP is disabled.

3. Configure the remote PE as a BGP peer.

   peer { *group-name* | *ip-address* [*mask-length*] } **as-number** *as-number*

   For more information about this command, see *Layer 3—IP Routing Command Reference*.

4. Create the BGP L2VPN address family and enter BGP L2VPN address family view.

   address-family l2vpn

5. Enable BGP to exchange BGP L2VPN information with the specified peer or peer group.

   peer { *group-name* | *ip-address* [*mask-length*] } **enable**

   By default, BGP cannot exchange BGP L2VPN information with any peer or peer group.

   For more information about this command, see *Layer 3—IP Routing Command Reference*.

6. Enable BGP to exchange label block information with the specified peer or peer group.

   peer { *group-name* | *ip-address* [*mask-length*] } **signaling** [**non-standard**]

   By default, BGP can exchange label block information with a BGP L2VPN peer or peer group by using RFC 4761 MP_REACH_NLRI.

7. Configure the BGP L2VPN address family.

   For more information, see "Configuring BGP L2VPN address family."

8. Reset BGP L2VPN sessions.

   For more information, see "Resetting BGP sessions."

Creating a BGP PW

1. Enter system view.

   system-view

2. Enter cross-connect group view.

   xconnect-group *group-name*

3. Configure the cross-connect group to automatically discover neighbors and create PWs through BGP and enter auto-discovery cross-connect group view.

   auto-discovery bgp

   By default, a cross-connect group does not automatically discover neighbors or create PWs through BGP.

4. Configure an RD for the cross-connect group.

   route-distinguisher *route-distinguisher*

   By default, no RD is configured for the cross-connect group.

5. Configure route targets for the cross-connect group.

vpn-target *vpn-target*&<1-8> [**both** | **export-extcommunity** | **import-extcommunity**]

By default, no route targets are configured for the cross-connect group.

6. (Optional.) Specify a PW class for the auto-discovery cross-connect group.

   pw-class *class-name*

   By default, no PW class is specified.

7. (Optional.) Set an MTU for the PW.

   mtu *size*

   The default MTU is 1500 bytes.

8. Create a local site and enter site view.

   site *site-id* [**range** *range-value*] [**default-offset** *default-offset*]

9. Create a cross-connect and enter auto-discovery cross-connect view.

   connection remote-site-id *remote-site-id*

   After you execute this command, a PW to the specified remote site is created and is bound to the cross-connect.

10. (Optional.) Specify a tunnel policy for the auto-discovery cross-connect.

    tunnel-policy *tunnel-policy-name*

    By default, no tunnel policy is specified.

Configuring BGP L2VPN address family

1. Enter system view.

   system-view

2. Enter BGP instance view.

   bgp *as-number* [**instance** *instance-name*]

3. Enter BGP L2VPN address family view.

   address-family l2vpn

4. Permit the local AS number to appear in routes from the specified peer or peer group and specify the appearance times.

   peer { *group-name* | *ip-address* [*mask-length*] } **allow-as-loop** [*number*]

   By default, the local AS number is not allowed in routes from a peer or peer group.

   For more information about this command, see *Layer 3—IP Routing Command Reference*.

5. Enable route target-based filtering of incoming BGP L2VPN information.

   policy vpn-target

   By default, route target-based filtering of incoming BGP L2VPN information is enabled.

6. Configure BGP route reflection:

   a. Configure the router as a route reflector and specify a peer or peer group as its client.

      peer { *group-name* | *ip-address* [*mask-length*] } **reflect-client**

      By default, no route reflector or client is configured.

   b. Enable L2VPN information reflection between clients.

      reflect between-clients

      By default, L2VPN information reflection between clients is enabled.

   c. Configure the cluster ID of the route reflector.

      reflector cluster-id { *cluster-id* | *ip-address* }

      By default, a route reflector uses its own router ID as the cluster ID.

d. Configure a filtering policy for reflected L2VPN information.

   rr-filter *ext-comm-list-number*

   By default, the route reflector does not filter reflected L2VPN information.

   For more information about the commands, see *Layer 3—IP Routing Command Reference*.

7. Set the optimal route selection delay timer.

   route-select delay *delay-value*

   By default, the optimal route selection delay timer is 0 seconds, which means optimal route selection is not delayed. For more information about this command, see BGP commands in *Layer 3—IP Routing Command Reference*.

Resetting BGP sessions of L2VPN address family

To reset BGP sessions of the L2VPN address family, execute one of the following command in user view:

- Perform manual soft-reset for BGP sessions of the L2VPN address family.

  refresh bgp [**instance** *instance-name*] { *ip-address* [*mask-length*] | **all** | **external** | **group** *group-name* | **internal** } { **export** | **import** } **l2vpn**

- Reset BGP sessions of the L2VPN address family.

  reset bgp [**instance** *instance-name*] { *as-number* | *ip-address* [*mask-length*] | **all** | **external** | **group** *group-name* | **internal** } **l2vpn**

For more information about the commands, see *Layer 3—IP Routing Command Reference*.

Configuring a remote CCC connection

Restrictions and guidelines

The outgoing label specified on a device must be the same as the incoming label specified on the next-hop device.

CCC connection settings such as the encapsulation type must be consistent on the two PEs. Otherwise, the PEs might fail to forward packets over the CCC connection.

Procedure

1. Configure the PE devices of the CCC connection:

   a. Enter system view.

      system-view

   b. Enter cross-connect group view.

      xconnect-group *group-name*

   c. Enter cross-connect view.

      connection *connection-name*

   d. Create a remote CCC connection.

      ccc in-label *in-label-value* **out-label** *out-label-value* { **nexthop** *nexthop* | **out-interface** *interface-type interface-number* } [**pw-class** *class-name*]

      Use the **out-interface** keyword to specify the outgoing interface only on a point-to-point link. On other types of interfaces such as Layer 3 Ethernet interfaces and VLAN interfaces, you must use the **nexthop** keyword to specify the IP address of the next hop.

2. Configure P devices of the CCC connection:

   a. Enter system view.

      system-view

b. Configure a static LSP for each direction of the CCC connection.

static-lsp transit *lsp-name* **in-label** *in-label* { **nexthop** *next-hop-ip-address* | **outgoing-interface** *interface-type interface-number* } **out-label** *out-label*

For more information about this command, see *MPLS Command Reference*.

Binding an AC to a cross-connect

About binding an AC to a cross-connect

On a Layer 2 Ethernet or Layer 2 aggregate interface, you can create an Ethernet service instance and bind it to a cross-connect. The Ethernet service instance matches packets received on that interface. The matching packets are then forwarded to the bound PW or another AC. An Ethernet service instance can match all packets, tagged packets, or untagged packets.

When you bind an AC to a cross-connect, you can associate Track with the AC. Then, the AC is up only when one or more of the associated track entries are positive.

Associating Track with an AC helps detecting AC failure. For example, when an AC is a VE-L2VPN interface, the interface will not go down upon a link failure because the interface is a virtual interface. To resolve the problem, you can associate Track with the AC to detect failures on the link that connects the PE-agg to the L3VPN or IP backbone. When a failure occurs on the link, the VE-L2VPN interface is set to down. Consequently, the PW bound to the AC goes down. If the PW has a backup PW, traffic can be switched to the backup PW. For more information about VE-L2VPN interfaces and L2VPN access to L3VPN or IP backbone, see "Configuring L2VPN access to L3VPN or IP backbone."

Restrictions and guidelines for binding an AC to a cross-connect

If a Layer 2 Ethernet interface has been added to a link aggregation group, you cannot bind an Ethernet service instance on the interface to a cross-connect, and vice versa.

Binding an Ethernet service instance to a non-BGP cross-connect

1. Enter system view.

   system-view

2. Enter cross-connect group view.

   xconnect-group *group-name*

3. Enter cross-connect view.

   connection *connection-name*

4. Bind the Ethernet service instance on the interface to the cross-connect.

   ac interface *interface-type interface-number* **service-instance** *instance-id*] [**access-mode** { **ethernet** | **vlan** } [**track** *track-entry-number*&<1-3>]

   By default, no Ethernet service instance is bound to the cross-connect.

Binding an Ethernet service instance to a BGP cross-connect

1. Enter system view.

   system-view

2. Enter cross-connect group view.

   xconnect-group *group-name*

3. Enter auto-discovery cross-connect group view.

   auto-discovery bgp

4. Enter site view.

   site *site-id* [**range** *range-value*] [**default-offset** *default-offset-value*]

5. Enter auto-discovery cross-connect view.

   connection remote-site-id *remote-site-id*

6. Bind the Ethernet service instance on the interface to the BGP cross-connect.

   ac interface *interface-type interface-number* **service-instance** *instance-id*] [**access-mode** { **ethernet** | **vlan** } [**track** *track-entry-number*&<1-3>]

   By default, no Ethernet service instance is bound to the BGP cross-connect.

Configuring PW redundancy

Configuring static PW redundancy

1. Enter system view.

   system-view

2. Enter cross-connect group view.

   xconnect-group *group-name*

3. Enter cross-connect view.

   connection *connection-name*

4. (Optional.) Use the master/slave PW redundancy mode and configure the local PE as the master node.

   pw-redundancy master

   By default, the PW redundancy mode is master/slave and the local PE operates as the slave node.

   Do not configure this command on the local PE if the remote PE does not support the master/slave PW redundancy mode.

5. (Optional.) Specify the switchover mode and set the wait time for the switchover.

   revertive { **wtr** *wtr-time* | **never** }

   By default, the switchover mode is revertive and the switchover wait time is 0 seconds.

6. Enter cross-connect PW view.

   peer *ip-address* **pw-id** *pw-id* [**in-label** *label-value* **out-label** *label-value*] [**pw-class** *class-name* | **tunnel-policy** *tunnel-policy-name*] *

7. Configure a backup cross-connect PW and enter backup cross-connect PW view.

backup-peer *ip-address* **pw-id** *pw-id* **in-label** *label-value* **out-label** *label-value* [**pw-class** *class-name* | **tunnel-policy** *tunnel-policy-name*] *

Configuring LDP PW redundancy

1. Enter system view.

   system-view

2. Enter cross-connect group view.

   xconnect-group *group-name*

3. Enter cross-connect view.

   connection *connection-name*

4. (Optional.) Specify the switchover mode and set the wait time for the switchover.

   revertive { **wtr** *wtr-time* | **never** }

   By default, the switchover mode is revertive and the switchover wait time is 0 seconds.

5. Enter cross-connect PW view.

   peer *ip-address* **pw-id** *pw-id* [**ignore-standby-state** | **pw-class** *class-name* | **tunnel-policy** *tunnel-policy-name*] *

   For the local PE to ignore the PW active/standby states received from the remote PE, specify the **ignore-standby-state** keyword.

6. Configure a backup LDP PW and enter backup cross-connect PW view.

   backup-peer *ip-address* **pw-id** *pw-id* [**pw-class** *class-name* | **tunnel-policy** *tunnel-policy-name*] *

Performing a manual PW switchover

About performing a manual PW switchover

After you perform this task, if a PW has a backup PW or primary PW, this command switches traffic from the PW to the backup or primary PW. If the PW does not have a backup or primary PW, traffic switchover will not be performed.

Procedure

To manually switch the traffic of a PW to its backup PW, execute the following command in user view:

l2vpn switchover peer *ip-address* **pw-id** *pw-id*

Enabling SNMP notifications for L2VPN PW

About SNMP notifications for L2VPN PW

This feature enables L2VPN to generate SNMP notifications when PW deletions, PW switchovers, or PW status changes occur. For L2VPN event notifications to be sent correctly, you must also configure SNMP on the device. For more information about SNMP configuration, see the network management and monitoring configuration guide for the device.

Procedure

1. Enter system view.

   system-view

2. Enable SNMP notifications for L2VPN PW.

   snmp-agent trap enable l2vpn [**pw-delete** | **pw-switch** | **pw-up-down**] *

By default, SNMP notifications for L2VPN PW are disabled.

Display and maintenance commands for MPLS L2VPN

Execute **display** commands in any view and **reset** commands in user view.

Task	Command
Display BGP L2VPN peer group information.	**display bgp** [**instance** *instance-name*] **group l2vpn** [**group-name** *group-name*]
Display L2VPN label block information discovered by BGP.	**display bgp** [**instance** *instance-name*] **l2vpn signaling** [**peer** *ip-address* { **advertised** | **received** } [**statistics**] | **route-distinguisher** *route-distinguisher* [**site-id** *site-id* [**label-offset** *label-offset* [**advertise-info**]]] | **statistics**]
Display BGP L2VPN peer information.	**display bgp** [**instance** *instance-name*] **peer l2vpn** [*ip-address* *mask-length* | **group-name** *group-name* **log-info** | *ip-address* { **log-info** | **verbose** } | **verbose**]
Display BGP L2VPN update group information.	**display bgp** [**instance** *instance-name*] **update-group l2vpn** [*ip-address*]
Display L2VPN label block information.	**display l2vpn bgp** [**peer** *ip-address* | **local**] [**xconnect-group** *group-name*] [**verbose**]
Display cross-connect forwarding information.	**display l2vpn forwarding** { **ac** | **pw** } [**xconnect-group** *group-name*] [**slot** *slot-number*] [**verbose]**
Display LDP PW label information.	**display l2vpn ldp** [**peer** *ip-address* [**pw-id** *pw-id*] | **xconnect-group** *group-name*] [**verbose**]
Display L2VPN PW information.	**display l2vpn pw** [**xconnect-group** *group-name*] [**protocol** { **bgp** | **ldp** | **static** }] [**verbose**]
Display PW class information.	**display l2vpn pw-class** [*class-name*]
Display Ethernet service instance information.	**display l2vpn service-instance** [**interface** *interface-type interface-number* [**service-instance** *instance-id*]] [**verbose**]
Display cross-connect group information.	**display l2vpn xconnect-group** [**name** *group-name*] [**verbose**]
Reset BGP sessions for L2VPN.	**reset bgp** [**instance** *instance-name*] { *as-number* | *ip-address* [*mask-length*] | **all** | **external** | **group** *group-name* | **internal** } **l2vpn**

For more information about the **display bgp group l2vpn**, **display bgp peer l2vpn**, **display bgp update-group l2vpn**, and **reset bgp l2vpn** commands, see *Layer 3—IP Routing Command Reference*.

MPLS L2VPN configuration examples

Example: Configuring a static PW

Network configuration

Create a static PW between PE 1 and PE 2 over the backbone to allow communication between CE 1 and CE 2 within VLAN 10.

Create Ethernet service instance 10 on Twenty-FiveGigE 1/0/1 to match packets with an outer VLAN ID of 10 on each PE.

Figure 4 Network diagram

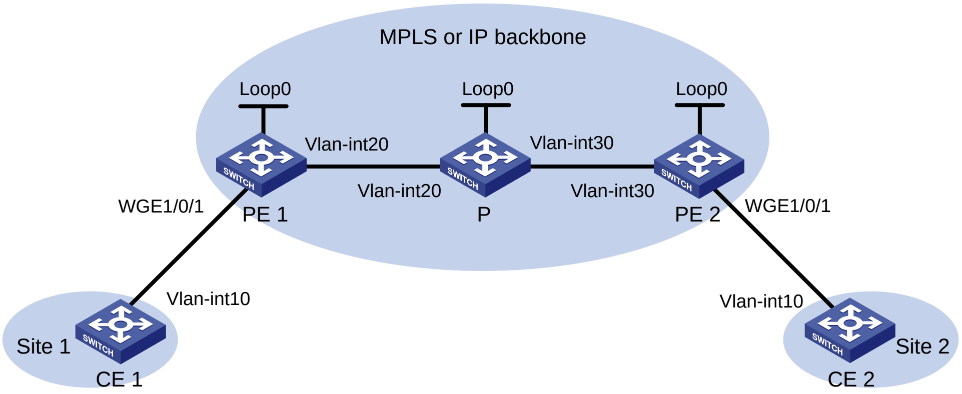


Table 2 Interface and IP address assignment

Device	Interface	IP address	Device	Interface	IP address
CE 1	Vlan-int10	100.1.1.1/24	P	Loop0	192.4.4.4/32
PE 1	Loop0	192.2.2.2/32		Vlan-int30	10.2.2.2/24
	Vlan-int20	10.1.1.1/24		Vlan-int20	10.1.1.2/24
CE 2	Vlan-int10	100.1.1.2/24	PE 2	Loop0	192.3.3.3/32
				Vlan-int30	10.2.2.1/24

Procedure

1. Configure VLANs and add ports to VLANs on each switch. (Details not shown.)
2. Configure CE 1.

```
<CE1> system-view
[CE1] interface vlan-interface 10
[CE1-Vlan-interface10] ip address 100.1.1.1 24
[CE1-Vlan-interface10] quit
```

3. Configure PE 1:

# Configure an LSR ID.

```
<PE1> system-view
[PE1] interface loopback 0
[PE1-LoopBack0] ip address 192.2.2.2 32
[PE1-LoopBack0] quit
[PE1] mpls lsr-id 192.2.2.2
```

# Enable L2VPN.

```
[PE1] l2vpn enable
```

# Enable global LDP.

```
[PE1] mpls ldp
[PE1-ldp] quit
```

# Configure VLAN-interface 20 (the interface connected to the P device), and enable LDP on the interface.

```
[PE1] interface vlan-interface 20
[PE1-Vlan-interface20] ip address 10.1.1.1 24
[PE1-Vlan-interface20] mpls enable
[PE1-Vlan-interface20] mpls ldp enable
[PE1-Vlan-interface20] quit
```

# Configure OSPF for LDP to create LSPs.

```
[PE1] ospf
[PE1-ospf-1] area 0
[PE1-ospf-1-area-0.0.0.0] network 10.1.1.1 0.0.0.255
[PE1-ospf-1-area-0.0.0.0] network 192.2.2.2 0.0.0.0
[PE1-ospf-1-area-0.0.0.0] quit
[PE1-ospf-1] quit
```

# Create VLAN 10 and assign Twenty-FiveGigE 1/0/1 to the VLAN.

```
[PE1] vlan 10
[PE1-vlan10] port twenty-fivegige 1/0/1
[PE1-vlan10] quit
```

# Create Ethernet service instance 10 on Twenty-FiveGigE 1/0/1 to match packets with an outer VLAN ID of 10.

```
[PE1] interface twenty-fivegige 1/0/1
[PE1-Twenty-FiveGigE1/0/1] service-instance 10
[PE1-Twenty-FiveGigE1/0/1-srv10] encapsulation s-vid 10
[PE1-Twenty-FiveGigE1/0/1-srv10] quit
[PE1-Twenty-FiveGigE1/0/1] quit
```

# Create a cross-connect group named **vpna**, create a cross-connect named **svc** in the group, and bind Ethernet service instance 10 on Twenty-FiveGigE 1/0/1 to the cross-connect.

```
[PE1] xconnect-group vpna
[PE1-xcg-vpna] connection svc
[PE1-xcg-vpna-svc] ac interface twenty-fivegige 1/0/1 service-instance 10
```

# Create a static PW for the cross-connect to bind the AC to the PW.

```
[PE1-xcg-vpna-svc] peer 192.3.3.3 pw-id 3 in-label 100 out-label 200
[PE1-xcg-vpna-svc-192.3.3.3-3] quit
[PE1-xcg-vpna-svc] quit
[PE1-xcg-vpna] quit
```

4. Configure the P device:

# Configure an LSR ID.

```
<P> system-view
[P] interface loopback 0
[P-LoopBack0] ip address 192.4.4.4 32
[P-LoopBack0] quit
[P] mpls lsr-id 192.4.4.4
```

# Enable global LDP.

```
[P] mpls ldp
[P-ldp] quit
```

# Configure VLAN-interface 20 (the interface connected to PE 1), and enable LDP on the interface.

```
[P] interface vlan-interface 20
[P-Vlan-interface20] ip address 10.1.1.2 24
[P-Vlan-interface20] mpls enable
[P-Vlan-interface20] mpls ldp enable
[P-Vlan-interface20] quit
```

# Configure VLAN-interface 30 (the interface connected to PE 2), and enable LDP on the interface.

```
[P] interface vlan-interface 30
[P-Vlan-interface30] ip address 10.2.2.2 24
[P-Vlan-interface30] mpls enable
[P-Vlan-interface30] mpls ldp enable
[P-Vlan-interface30] quit
```

# Configure OSPF for LDP to create LSPs.

```
[P] ospf
[P-ospf-1] area 0
[P-ospf-1-area-0.0.0.0] network 10.1.1.2 0.0.0.255
[P-ospf-1-area-0.0.0.0] network 10.2.2.2 0.0.0.255
[P-ospf-1-area-0.0.0.0] network 192.4.4.4 0.0.0.0
[P-ospf-1-area-0.0.0.0] quit
[P-ospf-1] quit
```

5. Configure PE 2:

# Configure an LSR ID.

```
<PE2> system-view
[PE2] interface loopback 0
[PE2-LoopBack0] ip address 192.3.3.3 32
[PE2-LoopBack0] quit
[PE2] mpls lsr-id 192.3.3.3
```

# Enable L2VPN.

```
[PE2] l2vpn enable
```

# Enable global LDP.

```
[PE2] mpls ldp
[PE2-ldp] quit
```

# Configure VLAN-interface 30 (the interface connected to the P device), and enable LDP on the interface.

```
[PE2] interface vlan-interface 30
[PE2-Vlan-interface30] ip address 10.2.2.1 24
[PE2-Vlan-interface30] mpls enable
[PE2-Vlan-interface30] mpls ldp enable
[PE2-Vlan-interface30] quit
```

# Configure OSPF for LDP to create LSPs.

```
[PE2] ospf
[PE2-ospf-1] area 0
[PE2-ospf-1-area-0.0.0.0] network 10.2.2.1 0.0.0.255
[PE2-ospf-1-area-0.0.0.0] network 192.3.3.3 0.0.0.0
```

```
[PE2-ospf-1-area-0.0.0.0] quit
[PE2-ospf-1] quit
```

# Create VLAN 10 and assign Twenty-FiveGigE 1/0/1 to the VLAN.

```
[PE2] vlan 10
[PE2-vlan10] port twenty-fivegige 1/0/1
[PE2-vlan10] quit
```

# Create Ethernet service instance 10 on Twenty-FiveGigE 1/0/1 to match packets with an outer VLAN ID of 10.

```
[PE2] interface twenty-fivegige 1/0/1
[PE2-Twenty-FiveGigE1/0/1] service-instance 10
[PE2-Twenty-FiveGigE1/0/1-srv10]encapsulation s-vid 10
[PE2-Twenty-FiveGigE1/0/1-srv10] quit
[PE2-Twenty-FiveGigE1/0/1] quit
```

# Create a cross-connect group named **vpna**, create a cross-connect named **svc** in the group, and bind Ethernet service instance 10 on Twenty-FiveGigE 1/0/1 to the cross-connect.

```
[PE2] xconnect-group vpna
[PE2-xcg-vpna] connection svc
[PE2-xcg-vpna-svc] ac interface twenty-fivegige 1/0/1 service-instance 10
```

# Create a static PW for the cross-connect to bind the AC to the PW.

```
[PE2-xcg-vpna-svc] peer 192.2.2.2 pw-id 3 in-label 200 out-label 100
[PE2-xcg-vpna-svc-192.2.2.2-3] quit
[PE2-xcg-vpna-svc] quit
[PE2-xcg-vpna] quit
```

6. Configure CE 2.

```
<CE2> system-view
[CE2] interface vlan-interface 10
[CE2-Vlan-interface10] ip address 100.1.1.2 24
[CE2-Vlan-interface10] quit
```

Verifying the configuration

# Verify that a static PW has been established on PE 1.

```
[PE1] display l2vpn pw
Flags: M - main, B - backup, BY - bypass, H - hub link, S - spoke link, N - no split horizon
Total number of PWs: 1
1 up, 0 blocked, 0 down, 0 defect, 0 idle, 0 duplicate

Xconnect-group Name: vpna
Peer            PW ID/Rmt Site    In/Out Label    Proto  Flag  Link ID    State
192.3.3.3       3                 100/200         Static M     0          Up
```

# Verify that a static PW has been established on PE 2.

```
[PE2] display l2vpn pw
Flags: M - main, B - backup, BY - bypass, H - hub link, S - spoke link, N - no split horizon
Total number of PWs: 1
1 up, 0 blocked, 0 down, 0 defect, 0 idle, 0 duplicate

Xconnect-group Name: vpna
Peer            PW ID/Rmt Site    In/Out Label    Proto  Flag  Link ID    State
192.2.2.2       3                 200/100         Static M     0          Up
```

# Verify that CE 1 and CE 2 can ping each other. (Details not shown.)

Example: Configuring an LDP PW

Network configuration

Create an LDP PW between PE 1 and PE 2, and use flexible mode to match packets from each AC to allow communication between CE 1 and CE 2 within VLAN 10 without consuming VLAN resources on PEs.

Figure 5 Network diagram

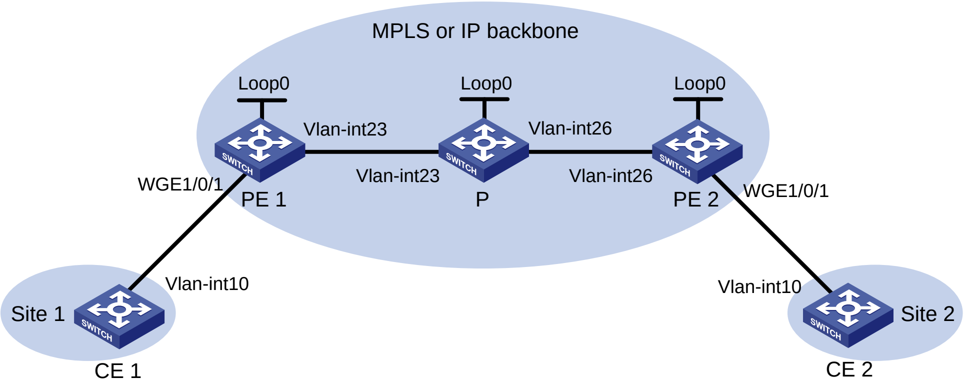


Table 3 Interface and IP address assignment

Device	Interface	IP address	Device	Interface	IP address
CE 1	Vlan-int10	100.1.1.1/24	P	Loop0	192.4.4.4/32
PE 1	Loop0	192.2.2.2/32		Vlan-int23	23.1.1.2/24
	Vlan-int23	23.1.1.1/24		Vlan-int26	26.2.2.2/24
CE 2	Vlan-int10	100.1.1.2/24	PE 2	Loop0	192.3.3.3/32
				Vlan-int26	26.2.2.1/24

Procedure

1. Configure VLANs and add ports to VLANs on each switch. (Details not shown.)
2. Configure CE 1.

```
<CE1> system-view
[CE1] interface vlan-interface 10
[CE1-Vlan-interface10] ip address 100.1.1.1 24
[CE1-Vlan-interface10] quit
```

3. Configure PE 1:

# Configure an LSR ID.

```
<PE1> system-view
[PE1] interface loopback 0
[PE1-LoopBack0] ip address 192.2.2.2 32
[PE1-LoopBack0] quit
[PE1] mpls lsr-id 192.2.2.2
```

# Enable L2VPN.

```
[PE1] l2vpn enable
```

# Enable global LDP.

```
[PE1] mpls ldp
[PE1-ldp] quit
```

# Configure VLAN-interface 23 (the interface connected to the P device), and enable LDP on the interface.

```
[PE1] interface vlan-interface 23
[PE1-Vlan-interface23] ip address 23.1.1.1 24
[PE1-Vlan-interface23] mpls enable
[PE1-Vlan-interface23] mpls ldp enable
[PE1-Vlan-interface23] quit
```

# Configure OSPF for LDP to create LSPs.

```
[PE1] ospf
[PE1-ospf-1] area 0
[PE1-ospf-1-area-0.0.0.0] network 23.1.1.1 0.0.0.255
[PE1-ospf-1-area-0.0.0.0] network 192.2.2.2 0.0.0.0
[PE1-ospf-1-area-0.0.0.0] quit
[PE1-ospf-1] quit
```

# Create Ethernet service instance 1000 on Twenty-FiveGigE 1/0/1 (the interface connected to CE 1).

```
[PE1] interface twenty-fivegige 1/0/1
[PE1-Twenty-FiveGigE1/0/1] service-instance 1000
[PE1-Twenty-FiveGigE1/0/1-srv1000] encapsulation s-vid 10
[PE1-Twenty-FiveGigE1/0/1-srv1000] quit
[PE1-Twenty-FiveGigE1/0/1] quit
```

# Create a cross-connect group named **vpn1**, create a cross-connect named **ldp** in the group, and bind Ethernet service instance 1000 on Twenty-FiveGigE 1/0/1 to the cross-connect.

```
[PE1] xconnect-group vpn1
[PE1-xcg-vpn1] connection ldp
[PE1-xcg-vpn1-ldp] ac interface twenty-fivegige 1/0/1 service-instance 1000
```

# Create an LDP PW for the cross-connect to bind the AC to the PW.

```
[PE1-xcg-vpn1-ldp] peer 192.3.3.3 pw-id 1000
[PE1-xcg-vpn1-ldp-192.3.3.3-1000] quit
[PE1-xcg-vpn1-ldp] quit
[PE1-xcg-vpn1] quit
```

4. Configure the P device:

# Configure an LSR ID.

```
<P> system-view
[P] interface loopback 0
[P-LoopBack0] ip address 192.4.4.4 32
[P-LoopBack0] quit
[P] mpls lsr-id 192.4.4.4
```

# Enable global LDP.

```
[P] mpls ldp
[P-ldp] quit
```

# Configure VLAN-interface 23 (the interface connected to PE 1), and enable LDP on the interface.

```
[P] interface vlan-interface 23
[P-Vlan-interface23] ip address 23.1.1.2 24
```

```
[P-Vlan-interface23] mpls enable
[P-Vlan-interface23] mpls ldp enable
[P-Vlan-interface23] quit
```

# Configure VLAN-interface 26 (the interface connected to PE 2), and enable LDP on the interface.

```
[P] interface vlan-interface 26
[P-Vlan-interface26] ip address 26.2.2.2 24
[P-Vlan-interface26] mpls enable
[P-Vlan-interface26] mpls ldp enable
[P-Vlan-interface26] quit
```

# Configure OSPF for LDP to create LSPs.

```
[P] ospf
[P-ospf-1] area 0
[P-ospf-1-area-0.0.0.0] network 23.1.1.2 0.0.0.255
[P-ospf-1-area-0.0.0.0] network 26.2.2.2 0.0.0.255
[P-ospf-1-area-0.0.0.0] network 192.4.4.4 0.0.0.0
[P-ospf-1-area-0.0.0.0] quit
[P-ospf-1] quit
```

5. Configure PE 2:

# Configure an LSR ID.

```
<PE2> system-view
[PE2] interface loopback 0
[PE2-LoopBack0] ip address 192.3.3.3 32
[PE2-LoopBack0] quit
[PE2] mpls lsr-id 192.3.3.3
```

# Enable L2VPN.

```
[PE2] l2vpn enable
```

# Enable global LDP.

```
[PE2] mpls ldp
[PE2-ldp] quit
```

# Configure VLAN-interface 26 (the interface connected to the P device), and enable LDP on the interface.

```
[PE2] interface vlan-interface 26
[PE2-Vlan-interface26] ip address 26.2.2.1 24
[PE2-Vlan-interface26] mpls enable
[PE2-Vlan-interface26] mpls ldp enable
[PE2-Vlan-interface26] quit
```

# Configure OSPF for LDP to create LSPs.

```
[PE2] ospf
[PE2-ospf-1] area 0
[PE2-ospf-1-area-0.0.0.0] network 192.3.3.3 0.0.0.0
[PE2-ospf-1-area-0.0.0.0] network 26.2.2.0 0.0.0.255
[PE2-ospf-1-area-0.0.0.0] quit
[PE2-ospf-1] quit
```

# Create Ethernet service instance 1000 on Twenty-FiveGigE 1/0/1 (the interface connected to CE 2).

```
[PE2] interface twenty-fivegige 1/0/1
[PE2-Twenty-FiveGigE1/0/1] service-instance 1000
```

```
[PE2-Twenty-FiveGigE1/0/1-srv1000] encapsulation s-vid 10
[PE2-Twenty-FiveGigE1/0/1-srv1000] quit
[PE2-Twenty-FiveGigE1/0/1] quit
```

# Create a cross-connect group named **vpn1**, create a cross-connect named **ldp** in the group, and bind Ethernet service instance 1000 on Twenty-FiveGigE 1/0/1 to the cross-connect.

```
[PE2] xconnect-group vpn1
[PE2-xcg-vpn1] connection ldp
[PE2-xcg-vpn1-ldp] ac interface twenty-fivegige 1/0/1 service-instance 1000
```

# Create an LDP PW for the cross-connect to bind the AC to the PW.

```
[PE2-xcg-vpn1-ldp] peer 192.2.2.2 pw-id 1000
[PE2-xcg-vpn1-ldp-192.2.2.2-1000] quit
[PE2-xcg-vpn1-ldp] quit
[PE2-xcg-vpn1] quit
```

6. Configure CE 2.

```
<CE2> system-view
[CE2] interface vlan-interface 10
[CE2-Vlan-interface10] ip address 100.1.1.2 24
[CE2-Vlan-interface10] quit
```

Verifying the configuration

# Verify that an LDP PW has been established on PE 1.

```
[PE1] display l2vpn pw
Flags: M - main, B - backup, BY - bypass, H - hub link, S - spoke link, N - no split horizon
Total number of PWs: 1
1 up, 0 blocked, 0 down, 0 defect, 0 idle, 0 duplicate

Xconnect-group Name: vpn1
Peer            PW ID/Rmt Site    In/Out Label    Proto  Flag  Link ID    State
192.3.3.3       1000              1151/1279       LDP    M     1          Up
```

# Verify that an LDP PW has been established on PE 2.

```
[PE2] display l2vpn pw
Flags: M - main, B - backup, BY - bypass, H - hub link, S - spoke link, N - no split horizon
Total number of PWs: 1
1 up, 0 blocked, 0 down, 0 defect, 0 idle, 0 duplicate

Xconnect-group Name: vpn1
Peer            PW ID/Rmt Site    In/Out Label    Proto  Flag  Link ID    State
192.2.2.2       1000              1279/1151       LDP    M     1          Up
```

# Verify that CE 1 and CE 2 can ping each other. (Details not shown.)

Example: Configuring a BGP PW

Network configuration

Create a BGP PW between PE 1 and PE 2 to allow communication between CE 1 and CE 2 within VLAN 10.

Create Ethernet service instance 10 on Twenty-FiveGigE 1/0/1 to match packets with an outer VLAN ID of 10 on each PE.

Figure 6 Network diagram

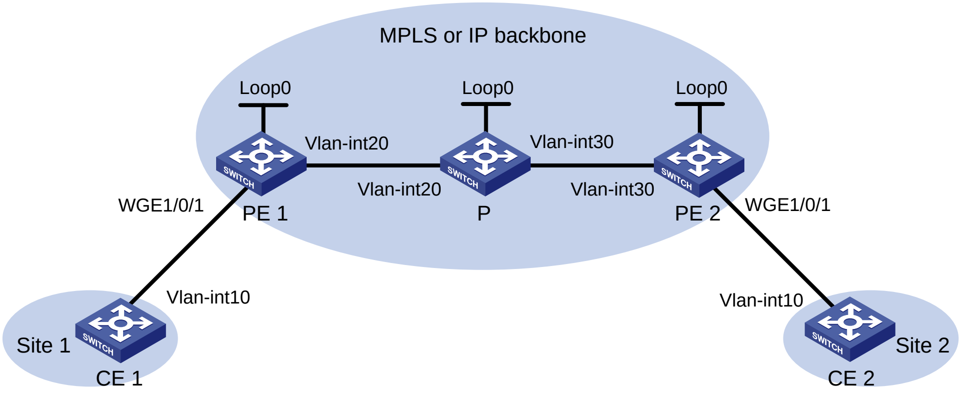


Table 4 Interface and IP address assignment

Device	Interface	IP address	Device	Interface	IP address
CE 1	Vlan-int10	100.1.1.1/24	P	Loop0	192.4.4.4/32
PE 1	Loop0	192.2.2.2/32		Vlan-int20	10.1.1.2/24
	Vlan-int20	10.1.1.1/24		Vlan-int30	10.2.2.2/24
CE 2	Vlan-int10	100.1.1.2/24	PE 2	Loop0	192.3.3.3/32
				Vlan-int30	10.2.2.1/24

Procedure

1. Configure VLANs and add ports to VLANs on each switch. (Details not shown.)
2. Configure CE 1.

```
<CE1> system-view
[CE1] interface vlan-interface 10
[CE1-Vlan-interface10] ip address 100.1.1.1 24
[CE1-Vlan-interface10] quit
```

3. Configure PE 1:

# Configure an LSR ID.

```
<PE1> system-view
[PE1] interface loopback 0
[PE1-LoopBack0] ip address 192.2.2.2 32
[PE1-LoopBack0] quit
[PE1] mpls lsr-id 192.2.2.2
```

# Enable L2VPN.

```
[PE1] l2vpn enable
```

# Enable LDP globally.

```
[PE1] mpls ldp
[PE1-ldp] quit
```

# Configure VLAN-interface 20 (the interface connected to the P device), and enable LDP on the interface.

```
[PE1] interface vlan-interface 20
[PE1-Vlan-interface20] ip address 10.1.1.1 24
[PE1-Vlan-interface20] mpls enable
```

```
[PE1-Vlan-interface20] mpls ldp enable
[PE1-Vlan-interface20] quit
```

# Enable OSPF for LSP establishment.

```
[PE1] ospf
[PE1-ospf-1] area 0
[PE1-ospf-1-area-0.0.0.0] network 10.1.1.1 0.0.0.255
[PE1-ospf-1-area-0.0.0.0] network 192.2.2.2 0.0.0.0
[PE1-ospf-1-area-0.0.0.0] quit
[PE1-ospf-1] quit
```

# Create an IBGP connection to PE 2, and enable BGP to advertise L2VPN information to PE 2.

```
[PE1] bgp 100
[PE1-bgp-default] peer 192.3.3.3 as-number 100
[PE1-bgp-default] peer 192.3.3.3 connect-interface loopback 0
[PE1-bgp-default] address-family l2vpn
[PE1-bgp-default-l2vpn] peer 192.3.3.3 enable
[PE1-bgp-default-l2vpn] quit
[PE1-bgp-default] quit
```

# Create VLAN 10 and assign Twenty-FiveGigE 1/0/1 to the VLAN.

```
[PE1] vlan 10
[PE1-vlan10] port twenty-fivegige 1/0/1
[PE1-vlan10] quit
```

# Create Ethernet service instance 10 on Twenty-FiveGigE 1/0/1 to match packets with an outer VLAN ID of 10.

```
[PE1] interface twenty-fivegige 1/0/1
[PE1-Twenty-FiveGigE1/0/1] service-instance 10
[PE1-Twenty-FiveGigE1/0/1-srv10]encapsulation s-vid 10
[PE1-Twenty-FiveGigE1/0/1-srv10] quit
[PE1-Twenty-FiveGigE1/0/1] quit
```

# Create a cross-connect group named **vpnb**, create a local site named **site 1**, and create a BGP PW from **site 1** to remote site **site 2**.

```
[PE1] xconnect-group vpnb
[PE1-xcg-vpnb] auto-discovery bgp
[PE1-xcg-vpnb-auto] route-distinguisher 2:2
[PE1-xcg-vpnb-auto] vpn-target 2:2 export-extcommunity
[PE1-xcg-vpnb-auto] vpn-target 2:2 import-extcommunity
[PE1-xcg-vpnb-auto] site 1 range 10 default-offset 0
[PE1-xcg-vpnb-auto-1] connection remote-site-id 2
```

# Bind Ethernet service instance 10 on Twenty-FiveGigE 1/0/1 to the PW.

```
[PE1-xcg-vpnb-auto-1-2] ac interface twenty-fivegige 1/0/1 service-instance 10
[PE1-xcg-vpnb-auto-1-2] return
```

4. Configure the P device:

# Configure an LSR ID.

```
<P> system-view
[P] interface loopback 0
[P-LoopBack0] ip address 192.4.4.4 32
[P-LoopBack0] quit
[P] mpls lsr-id 192.4.4.4
```

# Enable LDP globally.

```
[P] mpls ldp
[P-ldp] quit
```

# Configure VLAN-interface 20 (the interface connected to PE 1), and enable LDP on the interface.

```
[P] interface vlan-interface 20
[P-Vlan-interface20] ip address 10.1.1.2 24
[P-Vlan-interface20] mpls enable
[P-Vlan-interface20] mpls ldp enable
[P-Vlan-interface20] quit
```

# Configure VLAN-interface 30 (the interface connected to PE 2), and enable LDP on the interface.

```
[P] interface vlan-interface 30
[P-Vlan-interface30] ip address 10.2.2.2 24
[P-Vlan-interface30] mpls enable
[P-Vlan-interface30] mpls ldp enable
[P-Vlan-interface30] quit
```

# Enable OSPF for LSP establishment.

```
[P] ospf
[P-ospf-1] area 0
[P-ospf-1-area-0.0.0.0] network 10.1.1.2 0.0.0.255
[P-ospf-1-area-0.0.0.0] network 10.2.2.2 0.0.0.255
[P-ospf-1-area-0.0.0.0] network 192.4.4.4 0.0.0.0
[P-ospf-1-area-0.0.0.0] quit
[P-ospf-1] quit
```

5. Configure PE 2:

# Configure an LSR ID.

```
<PE2> system-view
[PE2] interface loopback 0
[PE2-LoopBack0] ip address 192.3.3.3 32
[PE2-LoopBack0] quit
[PE2] mpls lsr-id 192.3.3.3
```

# Enable L2VPN.

```
[PE2] l2vpn enable
```

# Enable LDP globally.

```
[PE2] mpls ldp
[PE2-ldp] quit
```

# Configure VLAN-interface 30 (the interface connected to the P device), and enable LDP on the interface.

```
[PE2] interface vlan-interface 30
[PE2-Vlan-interface30] ip address 10.2.2.1 24
[PE2-Vlan-interface30] mpls enable
[PE2-Vlan-interface30] mpls ldp enable
[PE2-Vlan-interface30] quit
```

# Enable OSPF for LSP establishment.

```
[PE2] ospf
[PE2-ospf-1] area 0
[PE2-ospf-1-area-0.0.0.0] network 192.3.3.3 0.0.0.0
[PE2-ospf-1-area-0.0.0.0] network 10.2.2.0 0.0.0.255
```

```
[PE2-ospf-1-area-0.0.0.0] quit
[PE2-ospf-1] quit
```

# Create an IBGP connection to PE 1, and enable BGP to advertise L2VPN information to PE 1.

```
[PE2] bgp 100
[PE2-bgp-default] peer 192.2.2.2 as-number 100
[PE2-bgp-default] peer 192.2.2.2 connect-interface loopback 0
[PE2-bgp-default] address-family l2vpn
[PE2-bgp-default-l2vpn] peer 192.2.2.2 enable
[PE2-bgp-default-l2vpn] quit
[PE2-bgp-default] quit
```

# Create VLAN 10 and assign Twenty-FiveGigE 1/0/1 to the VLAN.

```
[PE2] vlan 10
[PE2-vlan10] port twenty-fivegige 1/0/1
[PE2-vlan10] quit
```

# Create Ethernet service instance 10 on Twenty-FiveGigE 1/0/1 to match packets with an outer VLAN ID of 10.

```
[PE2] interface twenty-fivegige 1/0/1
[PE2-Twenty-FiveGigE1/0/1] service-instance 10
[PE2-Twenty-FiveGigE1/0/1-srv10]encapsulation s-vid 10
[PE2-Twenty-FiveGigE1/0/1-srv10] quit
[PE2-Twenty-FiveGigE1/0/1] quit
```

# Create a cross-connect group named **vpnb**, create a local site named **site 2**, and create a BGP PW from **site 2** to remote site **site 1**.

```
[PE2] xconnect-group vpnb
[PE2-xcg-vpnb] auto-discovery bgp
[PE2-xcg-vpnb-auto] route-distinguisher 2:2
[PE2-xcg-vpnb-auto] vpn-target 2:2 export-extcommunity
[PE2-xcg-vpnb-auto] vpn-target 2:2 import-extcommunity
[PE2-xcg-vpnb-auto] site 2 range 10 default-offset 0
[PE2-xcg-vpnb-auto-2] connection remote-site-id 1
```

# Bind Ethernet service instance 10 on Twenty-FiveGigE 1/0/1 to the PW.

```
[PE2-xcg-vpnb-auto-2-1] ac interface twenty-fivegige 1/0/1 service-instance 10
[PE2-xcg-vpnb-auto-2-1] return
```

6. Configure CE 2.

```
<CE2> system-view
[CE2] interface vlan-interface 10
[CE2-Vlan-interface10] ip address 100.1.1.2 24
[CE2-Vlan-interface10] quit
```

Verifying the configuration

# Verify that a BGP PW has been established on PE 1.

```
<PE1> display l2vpn pw
Flags: M - main, B - backup, BY - bypass, H - hub link, S - spoke link, N - no split horizon
Total number of PWs: 1
1 up, 0 blocked, 0 down, 0 defect, 0 idle, 0 duplicate

Xconnect-group Name: vpnb
Peer            PW ID/Rmt Site    In/Out Label    Proto   Flag  Link ID  State
192.3.3.3       2                 1036/1025       BGP     M     1        Up
```

# Verify that a BGP PW has been established on PE 2.

```
<PE2> display l2vpn pw
Flags: M - main, B - backup, BY - bypass, H - hub link, S - spoke link, N - no split horizon
Total number of PWs: 1
1 up, 0 blocked, 0 down, 0 defect, 0 idle, 0 duplicate

Xconnect-group Name: vpnb
Peer            PW ID/Rmt Site    In/Out Label    Proto   Flag  Link ID  State
192.2.2.2       1                 1025/1036       BGP     M     1        Up
```

# Verify that CE 1 and CE 2 can ping each other. (Details not shown.)

Example: Configuring a remote CCC connection

Network configuration

Create a remote CCC connection between PE 1 and PE 2 to allow communication between CE 1 and CE 2 within VLAN 10.

Create Ethernet service instance 10 on Twenty-FiveGigE 1/0/1 to match packets with an outer VLAN ID of 10 on each PE.

Figure 7 Network diagram

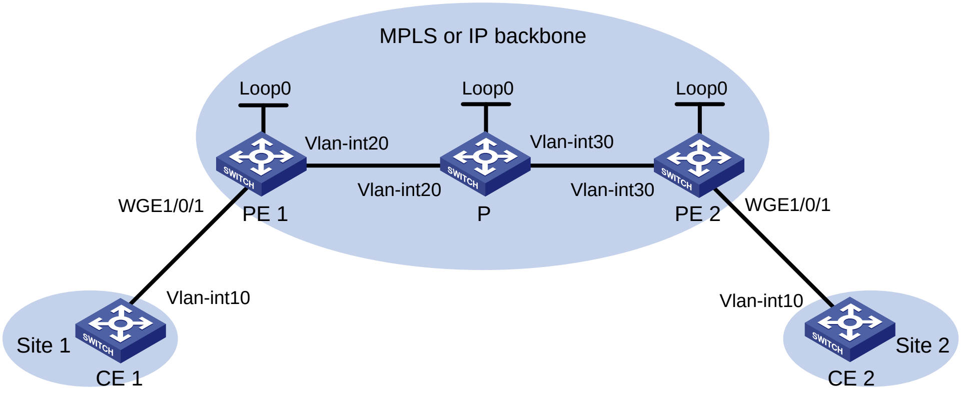


Table 5 Interface and IP address assignment

Device	Interface	IP address	Device	Interface	IP address
CE 1	Vlan-int10	100.1.1.1/24	P	Loop0	192.4.4.4/32
PE 1	Loop0	192.2.2.2/32		Vlan-int20	10.1.1.2/24
	Vlan-int20	10.1.1.1/24		Vlan-int30	10.2.2.2/24
CE 2	Vlan-int10	100.1.1.2/24	PE 2	Loop0	192.3.3.3/32
				Vlan-int30	10.2.2.1/24

Procedure

1. Configure VLANs and add ports to VLANs on each switch. (Details not shown.)
2. Configure CE 1.

```
<CE1> system-view
[CE1] interface vlan-interface 10
[CE1-Vlan-interface10] ip address 100.1.1.1 24
```

```
[CE1-Vlan-interface10] quit
```

3. Configure PE 1:

   # Configure an LSR ID.

   ```
   <PE1> system-view
   [PE1] interface loopback 0
   [PE1-LoopBack0] ip address 192.2.2.2 32
   [PE1-LoopBack0] quit
   [PE1] mpls lsr-id 192.2.2.2
   ```

   # Enable L2VPN.

   ```
   [PE1] l2vpn enable
   ```

   # Configure VLAN-interface 20 (the interface connected to the P device), and enable MPLS on the interface.

   ```
   [PE1] interface vlan-interface 20
   [PE1-Vlan-interface20] ip address 10.1.1.1 24
   [PE1-Vlan-interface20] mpls enable
   [PE1-Vlan-interface20] quit
   ```

   # Create VLAN 10 and assign Twenty-FiveGigE 1/0/1 to the VLAN.

   ```
   [PE1] vlan 10
   [PE1-vlan10] port twenty-fivegige 1/0/1
   [PE1-vlan10] quit
   ```

   # Create Ethernet service instance 10 on Twenty-FiveGigE 1/0/1 to match packets with an outer VLAN ID of 10.

   ```
   [PE1] interface twenty-fivegige 1/0/1
   [PE1-Twenty-FiveGigE1/0/1] service-instance 10
   [PE1-Twenty-FiveGigE1/0/1-srv10]encapsulation s-vid 10
   [PE1-Twenty-FiveGigE1/0/1-srv10] quit
   [PE1-Twenty-FiveGigE1/0/1] quit
   ```

   # Create a cross-connect group named **ccc**, and create a remote CCC connection that has incoming label 101, outgoing label 201, and next hop 10.1.1.2.

   ```
   [PE1] xconnect-group ccc
   [PE1-xcg-ccc] connection ccc
   [PE1-xcg-ccc-ccc] ccc in-label 101 out-label 201 nexthop 10.1.1.2
   ```

   # Bind Ethernet service instance 10 on Twenty-FiveGigE 1/0/1 to the CCC connection.

   ```
   [PE1-xcg-ccc-ccc] ac interface twenty-fivegige 1/0/1 service-instance 10
   [PE1-xcg-ccc-ccc] quit
   [PE1-xcg-ccc] quit
   ```

4. Configure the P device:

   # Configure an LSR ID.

   ```
   <P> system-view
   [P] interface loopback 0
   [P-LoopBack0] ip address 192.4.4.4 32
   [P-LoopBack0] quit
   [P] mpls lsr-id 192.4.4.4
   ```

   # Configure VLAN-interface 20 (the interface connected to PE 1), and enable MPLS on the interface.

   ```
   [P] interface vlan-interface 20
   [P-Vlan-interface20] ip address 10.1.1.2 24
   [P-Vlan-interface20] mpls enable
   ```

```
[P-Vlan-interface20] quit
```

# Configure VLAN-interface 30 (the interface connected to PE 2), and enable MPLS on the interface.

```
[P] interface vlan-interface 30
[P-Vlan-interface30] ip address 10.2.2.2 24
[P-Vlan-interface30] mpls enable
[P-Vlan-interface30] quit
```

# Configure a static LSP to forward packets from PE 1 to PE 2.

```
[P] static-lsp transit pe1-pe2 in-label 201 nexthop 10.2.2.1 out-label 202
```

# Configure a static LSP to forward packets from PE 2 to PE 1.

```
[P] static-lsp transit pe2-pe1 in-label 102 nexthop 10.1.1.1 out-label 101
```

5. Configure PE 2:

# Configure an LSR ID.

```
<PE2> system-view
[PE2] interface loopback 0
[PE2-LoopBack0] ip address 192.3.3.3 32
[PE2-LoopBack0] quit
[PE2] mpls lsr-id 192.3.3.3
```

# Enable L2VPN.

```
[PE2] l2vpn enable
```

# Configure VLAN-interface 30 (the interface connected to the P device), and enable MPLS on the interface.

```
[PE2] interface vlan-interface 30
[PE2-Vlan-interface30] ip address 10.2.2.1 24
[PE2-Vlan-interface30] mpls enable
[PE2-Vlan-interface30] quit
```

# Create VLAN 10 and assign Twenty-FiveGigE 1/0/1 to the VLAN.

```
[PE2] vlan 10
[PE2-vlan10] port twenty-fivegige 1/0/1
[PE2-vlan10] quit
```

# Create Ethernet service instance 10 on Twenty-FiveGigE 1/0/1 to match packets with an outer VLAN ID of 10.

```
[PE2] interface twenty-fivegige 1/0/1
[PE2-Twenty-FiveGigE1/0/1] service-instance 10
[PE2-Twenty-FiveGigE1/0/1-srv10]encapsulation s-vid 10
[PE2-Twenty-FiveGigE1/0/1-srv10] quit
[PE2-Twenty-FiveGigE1/0/1] quit
```

# Create a cross-connect group named **ccc**, and create a remote CCC connection that has incoming label 202, outgoing label 102, and next hop 10.2.2.2.

```
[PE2] xconnect-group ccc
[PE2-xcg-ccc] connection ccc
[PE2-xcg-ccc-ccc] ccc in-label 202 out-label 102 nexthop 10.2.2.2
```

# Bind Ethernet service instance 10 on Twenty-FiveGigE 1/0/1 to the CCC connection.

```
[PE2-xcg-ccc-ccc] ac interface twenty-fivegige 1/0/1 service-instance 10
[PE2-xcg-ccc-ccc] quit
[PE2-xcg-ccc] quit
```

6. Configure CE 2.

```
<CE2> system-view
```

```
    [CE2] interface vlan-interface 10
    [CE2-Vlan-interface10] ip address 100.1.1.2 24
    [CE2-Vlan-interface10] quit
```

Verifying the configuration

# Verify that a remote CCC connection (identified by PW ID/Rmt Site "-" and Proto Static) has been established on PE 1.

```
[PE1] display l2vpn pw
Flags: M - main, B - backup, BY - bypass, H - hub link, S - spoke link, N - no split horizon
Total number of PWs: 1
1 up, 0 blocked, 0 down, 0 defect, 0 idle, 0 duplicate

Xconnect-group Name: ccc
Peer            PW ID/Rmt Site    In/Out Label    Proto   Flag  Link ID  State
10.1.1.2        -                 101/201         Static  M     0        Up
```

# Verify that a remote CCC connection has been established on PE 2.

```
[PE2] display l2vpn pw
Flags: M - main, B - backup, BY - bypass, H - hub link, S - spoke link, N - no split horizon
Total number of PWs: 1
1 up, 0 blocked, 0 down, 0 defect, 0 idle, 0 duplicate

Xconnect-group Name: ccc
Peer            PW ID/Rmt Site    In/Out Label    Proto   Flag  Link ID  State
10.2.2.2        -                 202/102         Static  M     0        Up
```

# Verify that CE 1 and CE 2 can ping each other. (Details not shown.)

Example: Configuring LDP PW redundancy

Network configuration

Create two LDP PWs to implement PW redundancy between CE 1 and CE 2. The primary PW goes through PE 1—PE 2. The backup PW goes through PE 1—PE 3. When the primary PW fails, CE 1 and CE 2 communicate through the backup PW.

Figure 8 Network diagram

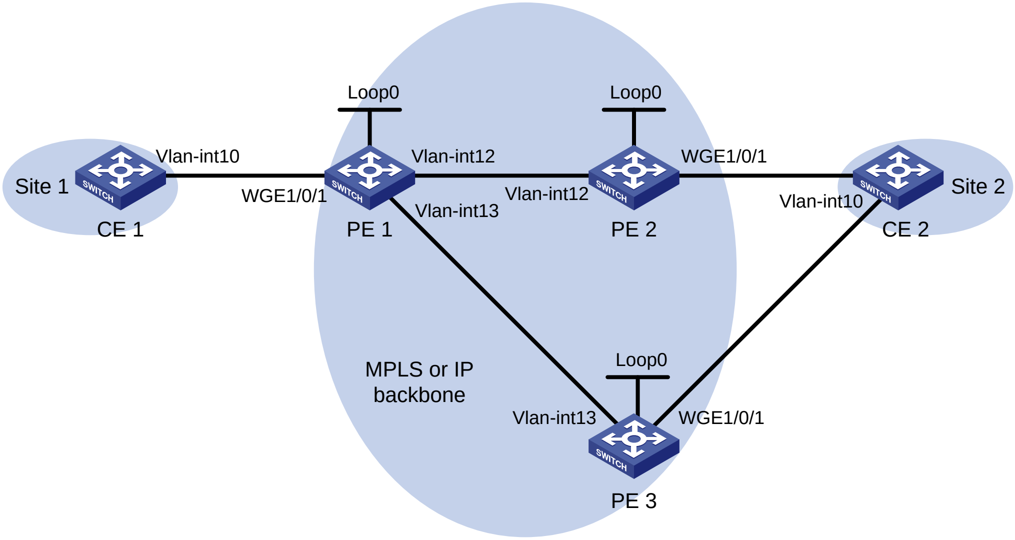


Table 6 Interface and IP address assignment

Device	Interface	IP address	Device	Interface	IP address
CE 1	Vlan-int10	100.1.1.1/24	PE 2	Loop0	2.2.2.2/32
PE 1	Loop0	1.1.1.1/32		Vlan-int12	12.1.1.2/24
	Vlan-int12	12.1.1.1/24	PE 3	Loop0	3.3.3.3/32
	Vlan-int13	13.1.1.1/24		Vlan-int13	13.1.1.3/24
CE 2	Vlan-int10	100.1.1.2/24			

Procedure

1. Configure VLANs and add ports to VLANs on each switch. (Details not shown.)
2. Disable the spanning tree feature globally or map each VLAN to an MSTI. (Details not shown.) For more information, see *Layer 2—LAN Switching Configuration Guide*.
3. Configure CE 1.

```
<CE1> system-view
[CE1] interface vlan-interface 10
[CE1-Vlan-interface10] ip address 100.1.1.1 24
[CE1-Vlan-interface10] quit
```

4. Configure PE 1:

# Configure an LSR ID.

```
<PE1> system-view
[PE1] interface loopback 0
[PE1-LoopBack0] ip address 1.1.1.1 32
[PE1-LoopBack0] quit
[PE1] mpls lsr-id 1.1.1.1
```

# Enable global MPLS LDP.

```
[PE1] mpls ldp
[PE1-ldp] quit
```

# Configure VLAN interface 12 (the interface connected to PE 2) and VLAN interface 13 (the interface connected to PE 3), and enable LDP for the interfaces.

```
[PE1] interface vlan-interface 12
[PE1-Vlan-interface12] ip address 12.1.1.1 24
[PE1-Vlan-interface12] mpls enable
[PE1-Vlan-interface12] mpls ldp enable
[PE1-Vlan-interface12] quit
[PE1] interface vlan-interface 13
[PE1-Vlan-interface13] ip address 13.1.1.1 24
[PE1-Vlan-interface13] mpls enable
[PE1-Vlan-interface13] mpls ldp enable
[PE1-Vlan-interface13] quit
```

# Configure OSPF for LDP to create LSPs.

```
[PE1] ospf
[PE1-ospf-1] area 0
[PE1-ospf-1-area-0.0.0.0] network 1.1.1.1 0.0.0.0
[PE1-ospf-1-area-0.0.0.0] network 12.1.1.0 0.0.0.255
[PE1-ospf-1-area-0.0.0.0] network 13.1.1.0 0.0.0.255
[PE1-ospf-1-area-0.0.0.0] quit
[PE1-ospf-1] quit
```

# Enable L2VPN.

```
[PE1] l2vpn enable
```

# Create Ethernet service instance 10 on Twenty-FiveGigE 1/0/1 to match packets with an outer VLAN ID of 10.

```
[PE1] interface twenty-fivegige 1/0/1
[PE1-Twenty-FiveGigE1/0/1] port link-type trunk
[PE1-Twenty-FiveGigE1/0/1] port trunk permit vlan 10
[PE1-Twenty-FiveGigE1/0/1] service-instance 10
[PE1-Twenty-FiveGigE1/0/1-srv10] encapsulation s-vid 10
[PE1-Twenty-FiveGigE1/0/1-srv10] quit
[PE1-Twenty-FiveGigE1/0/1] quit
```

# Create a cross-connect group named **vpna**, create a cross-connect named **ldp** in the group, and bind Ethernet service instance 10 on Twenty-FiveGigE 1/0/1 to the cross-connect.

```
[PE1] xconnect-group vpna
[PE1-xcg-vpna] connection ldp
[PE1-xcg-vpna-ldp] ac interface twenty-fivegige 1/0/1 service-instance 10
```

# Create primary and backup LDP PWs for the cross-connect to bind the AC to the PWs and to implement PW redundancy.

```
[PE1-xcg-vpna-ldp] peer 2.2.2.2 pw-id 20
[PE1-xcg-vpna-ldp-2.2.2.2-20] backup-peer 3.3.3.3 pw-id 30
[PE1-xcg-vpna-ldp-3.3.3.3-30-backup] quit
[PE1-xcg-vpna-ldp-2.2.2.2-20] quit
[PE1-xcg-vpna-ldp] quit
[PE1-xcg-vpna] quit
[PE1] quit
```

5. Configure PE 2:

# Configure LSR ID.

```
<PE2> system-view
```

```
[PE2] interface loopback 0
[PE2-LoopBack0] ip address 2.2.2.2 32
[PE2-LoopBack0] quit
[PE2] mpls lsr-id 2.2.2.2
```

# Enable global MPLS LDP.

```
[PE2] mpls ldp
[PE2-ldp] quit
```

# Configure VLAN interface 12 (the interface connected to PE 1), and enable LDP on it.

```
[PE2] interface vlan-interface 12
[PE2-Vlan-interface12] ip address 12.1.1.2 24
[PE2-Vlan-interface12] mpls enable
[PE2-Vlan-interface12] mpls ldp enable
[PE2-Vlan-interface12] quit
```

# Configure OSPF for LDP to create LSPs.

```
[PE2] ospf
[PE2-ospf-1] area 0
[PE2-ospf-1-area-0.0.0.0] network 12.1.1.0 0.0.0.255
[PE2-ospf-1-area-0.0.0.0] network 2.2.2.2 0.0.0.0
[PE2-ospf-1-area-0.0.0.0] quit
[PE2-ospf-1] quit
```

# Enable L2VPN.

```
[PE2] l2vpn enable
```

# Create Ethernet service instance 10 on Twenty-FiveGigE 1/0/1 to match packets with an outer VLAN ID of 10.

```
[PE2] interface twenty-fivegige 1/0/1
[PE2-Twenty-FiveGigE1/0/1] port link-type trunk
[PE2-Twenty-FiveGigE1/0/1] port trunk permit vlan 10
[PE2-Twenty-FiveGigE1/0/1] service-instance 10
[PE2-Twenty-FiveGigE1/0/1-srv10] encapsulation s-vid 10
[PE2-Twenty-FiveGigE1/0/1-srv10] quit
[PE2-Twenty-FiveGigE1/0/1] quit
```

# Create a cross-connect group named **vpna**, create a cross-connect named **ldp** in the group, and bind Ethernet service instance 10 on Twenty-FiveGigE 1/0/1 to the cross-connect.

```
[PE2] xconnect-group vpna
[PE2-xcg-vpna] connection ldp
[PE2-xcg-vpna-ldp] ac interface twenty-fivegige 1/0/1 service-instance 10
```

# Create an LDP PW for the cross-connect to bind the AC to the PW.

```
[PE2-xcg-vpna-ldp] peer 1.1.1.1 pw-id 20
[PE2-xcg-vpna-ldp-1.1.1.1-20] quit
[PE2-xcg-vpna-ldp] quit
[PE2-xcg-vpna] quit
```

6. Configure PE 3:

# Configure an LSR ID.

```
<PE3> system-view
[PE3] interface loopback 0
[PE3-LoopBack0] ip address 3.3.3.3 32
[PE3-LoopBack0] quit
[PE3] mpls lsr-id 3.3.3.3
```

# Enable global MPLS LDP.

```
[PE3] mpls ldp
[PE3-ldp] quit
```

# Configure VLAN interface 13 (the interface connected to PE 1), and enable LDP on it.

```
[PE3] interface vlan-interface 13
[PE3-Vlan-interface13] ip address 13.1.1.3 24
[PE3-Vlan-interface13] mpls enable
[PE3-Vlan-interface13] mpls ldp enable
[PE3-Vlan-interface13] quit
```

# Configure OSPF on PE 3 for LDP to create LSPs.

```
[PE3] ospf
[PE3-ospf-1] area 0
[PE3-ospf-1-area-0.0.0.0] network 13.1.1.0 0.0.0.255
[PE3-ospf-1-area-0.0.0.0] network 3.3.3.3 0.0.0.0
[PE3-ospf-1-area-0.0.0.0] quit
[PE3-ospf-1] quit
```

# Enable L2VPN.

```
[PE3] l2vpn enable
```

# Create Ethernet service instance 10 on Twenty-FiveGigE 1/0/1 to match packets with an outer VLAN ID of 10.

```
[PE3] interface twenty-fivegige 1/0/1
[PE3-Twenty-FiveGigE1/0/1] port link-type trunk
[PE3-Twenty-FiveGigE1/0/1] port trunk permit vlan 10
[PE3-Twenty-FiveGigE1/0/1] service-instance 10
[PE3-Twenty-FiveGigE1/0/1-srv10] encapsulation s-vid 10
[PE3-Twenty-FiveGigE1/0/1-srv10] quit
[PE3-Twenty-FiveGigE1/0/1] quit
```

# Create a cross-connect group named **vpna**, create a cross-connect named **ldp** in the group, and bind Ethernet service instance 10 on Twenty-FiveGigE 1/0/1 to the cross-connect.

```
[PE3] xconnect-group vpna
[PE3-xcg-vpna] connection ldp
[PE3-xcg-vpna-ldp] ac interface twenty-fivegige 1/0/1 service-instance 10
```

# Create an LDP PW for the cross-connect to bind the AC to the PW.

```
[PE3-xcg-vpna-ldp] peer 1.1.1.1 pw-id 30
[PE3-xcg-vpna-ldp-1.1.1.1-30] quit
[PE3-xcg-vpna-ldp] quit
[PE3-xcg-vpna] quit
```

7. Configure CE 2.

```
<CE2> system-view
[CE2] interface vlan-interface 10
[CE2-Vlan-interface10] ip address 100.1.1.2 24
[CE2-Vlan-interface10] quit
```

Verifying the configuration

# Verify that two LDP PWs have been established on PE 1.

```
<PE1> display l2vpn pw
Flags: M - main, B - backup, BY - bypass, H - hub link, S - spoke link, N - no split horizon
Total number of PWs: 2
1 up, 1 blocked, 0 down, 0 defect, 0 idle, 0 duplicate
```

```
Xconnect-group Name: vpna
Peer            PW ID/Rmt Site    In/Out Label    Proto  Flag  Link ID    State
2.2.2.2         20                1151/1279       LDP    M     1          Up
3.3.3.3         30                1150/1279       LDP    B     1          Blocked
```

# Display detailed information about the primary and backup PWs on PE 1.

```
<PE1> display l2vpn pw verbose
Xconnect-group Name: vpna
 Connection Name: ldp
  Peer: 2.2.2.2          PW ID: 20
    Signaling Protocol  : LDP
    Link ID             : 1          PW State : Up
    In Label            : 1151       Out Label: 1279
    Wait to Restore Time: 0 sec
    MTU                 : 1500
    PW Attributes       : Main
    VCCV CC             : -
    VCCV BFD            : -
    Tunnel Group ID     : 0x260000002
    Tunnel NHLFE IDs    : 1025
  Peer: 3.3.3.3          PW ID: 30
    Signaling Protocol  : LDP
    Link ID             : 1          PW State : Blocked
    In Label            : 1150       Out Label: 1279
    MTU                 : 1500
    PW Attributes       : Backup
    VCCV CC             : -
    VCCV BFD            : -
    Tunnel Group ID     : 0x360000003
    Tunnel NHLFE IDs    : 1027
```

# Verify that an LDP PW has been established on PE 2.

```
[PE2] display l2vpn pw
Flags: M - main, B - backup, BY - bypass, H - hub link, S - spoke link, N - no split horizon
Total number of PWs: 1
1 up, 0 blocked, 0 down, 0 defect, 0 idle, 0 duplicate

Xconnect-group Name: vpna
Peer            PW ID/Rmt Site    In/Out Label    Proto  Flag  Link ID    State
1.1.1.1         20                1279/1151       LDP    M     1          Up
```

# Verify that an LDP PW has been established on PE 3.

```
[PE3] display l2vpn pw
Flags: M - main, B - backup, BY - bypass, H - hub link, S - spoke link, N - no split horizon
Total number of PWs: 1
1 up, 0 blocked, 0 down, 0 defect, 0 idle, 0 duplicate

Xconnect-group Name: vpna
Peer            PW ID/Rmt Site    In/Out Label    Proto  Flag  Link ID    State
1.1.1.1         30                1279/1150       LDP    M     1          Up
```

# Verify that CE 1 and CE 2 can ping each other. (Details not shown.)

# Manually switch to the backup PW on PE 1.

```
<PE1> l2vpn switchover peer 2.2.2.2 pw-id 20
```

# Verify that the PW switchover is successful on PE 1.

```
<PE1> display l2vpn pw
Flags: M - main, B - backup, BY - bypass, H - hub link, S - spoke link, N - no split horizon
Total number of PWs: 2
1 up, 1 blocked, 0 down, 0 defect, 0 idle, 0 duplicate

Xconnect-group Name: vpna
Peer            PW ID/Rmt Site    In/Out Label    Proto  Flag  Link ID    State
2.2.2.2         20                1151/1279       LDP    M     1          Blocked
3.3.3.3         30                1150/1279       LDP    B     1          Up
```

# Verify that CE 1 and CE 2 can ping each other. (Details not shown.)