Contents

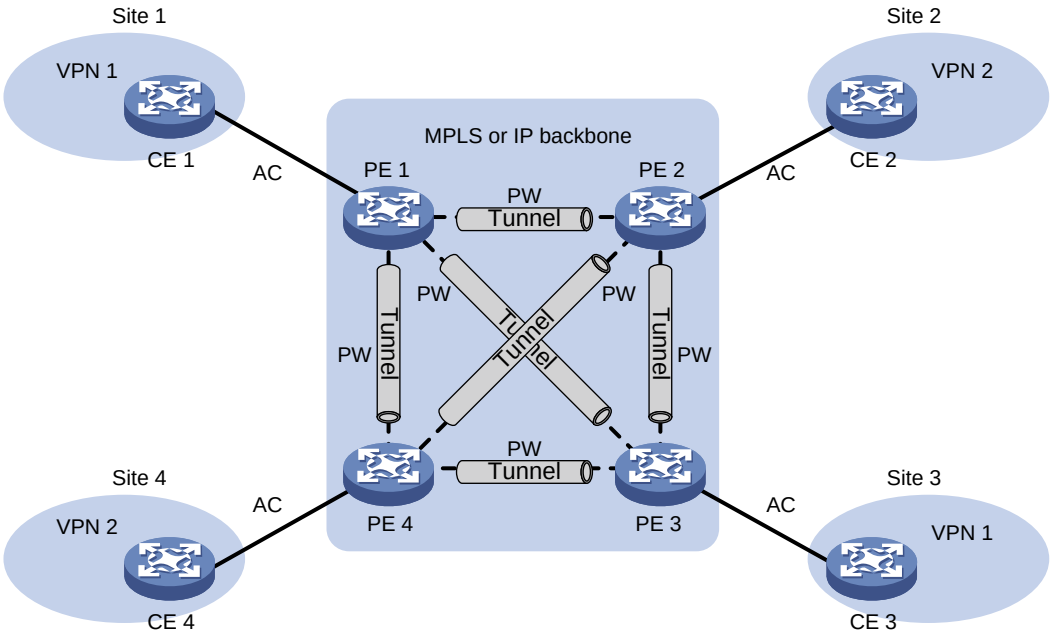
Configuring VPLS

Overview

Virtual Private LAN Service (VPLS) delivers a point-to-multipoint L2VPN service over an MPLS or IP backbone. The provider backbone emulates a switch to connect all geographically dispersed sites of each customer network. The backbone is transparent to the customer sites. The sites can communicate with each other as if they were on the same LAN.

Basic VPLS architecture

Figure 1 Basic VPLS architecture



As shown in Figure 1, the VPLS architecture mainly includes the following components:

- **CE**—A customer edge device is directly connected to the service provider network.
- **PE**—A provider edge device connects one or more CEs to the service provider network. A PE implements VPN access by mapping and forwarding packets between private networks and public network tunnels. A PE can be a UPE or NPE in a hierarchical VPLS.
- **AC**—An attachment circuit, physical or virtual, connects a CE and a PE, such as an Ethernet link or a VLAN.
- **PW**—A pseudowire is a bidirectional virtual connection between two PEs. An MPLS PW consists of two unidirectional MPLS LSPs in opposite directions.
- **Tunnel**—A tunnel can be an LSP tunnel, an MPLS TE tunnel, or a GRE tunnel. It carries one or more PWs over an IP/MPLS backbone. If a PW is carried on an LSP or MPLS TE tunnel, each packet on the PW contains two labels. The inner label is the PW label, which identifies the PW and ensures that the packet is forwarded to the correct VSI. The outer label is the public LSP or MPLS TE tunnel label, which ensures that the packet is correctly forwarded to the remote PE.
- **VPLS instance**—A customer network might contain multiple geographically dispersed sites (such as site 1 and site 3 in Figure 1.) The service provider uses VPLS to connect all the sites to

create a single Layer 2 VPN, which is referred to as a VPLS instance. Sites in different VPLS instances cannot communicate with each other at Layer 2.

- **VSI**—A virtual switch instance provides Layer 2 switching services for a VPLS instance on a PE. A VSI acts as a virtual switch that has all the functions of a conventional Ethernet switch, including source MAC address learning, MAC address aging, and flooding. VPLS uses VSIs to forward Layer 2 data packets in VPLS instances.

VPLS implementation

Creating a PW

PEs use PWs to forward packets among VPN sites. PWs include static PWs, LDP PWs, BGP PWs, and BGP auto-discovery LDP PWs.

- Static PW

  To create a static PW, specify the address of the remote PE, the incoming label, and the outgoing label.

- LDP PW

  To create an LDP PW, specify the address of the remote PE, and use LDP to advertise the PW-label binding to the remote PE. After the two PEs receive the PW-label binding from each other, they establish an LDP PW. The FEC type in the LDP message is PWid FEC Element that includes the PW ID field (FEC 128). The PW ID identifies the PW bound to the PW label.

- BGP PW

  To create a BGP PW, configure BGP to advertise label block information to the remote PE. After the two PEs receive label block information from each other, they use the label block information to calculate the incoming and outgoing labels and create the BGP PW. A PE also uses the received label block information to automatically find the remote PE.

- BGP auto-discovery LDP PW

  To create a BGP auto-discovery LDP PW, configure BGP to automatically find the remote PE, and use LDP to advertise the PW-label binding to the remote PE. After the two PEs receive the PW-label binding from each other, they establish a BGP auto-discovery LDP PW.

  The information advertised by BGP includes the ID (for example, LSR ID) and VPLS ID of the advertising PE. The receiving PE compares the received VPLS ID with its own VPLS ID. If the two VPLS IDs are identical, the two PEs use LDP to establish a PW. If not, the PEs do not establish a PW. The FEC type in the LDP message is Generalized PWid FEC Element (FEC 129), which contains the VPLS ID, Source Attachment Individual Identifier (SAII), and Target Attachment Individual Identifier (TAII). The SAII is the LSR ID of the advertising PE. The TAII identifies the remote PE and is advertised by the remote PE. VPLS ID+SAII+TAII uniquely identifies a PW in a VPLS instance.

MAC address learning, aging, and withdrawal

VPLS provides reachability through source MAC learning. A PE maintains a MAC address table for each VSI.

As shown in Figure 2, a PE learns source MAC addresses in the following ways:

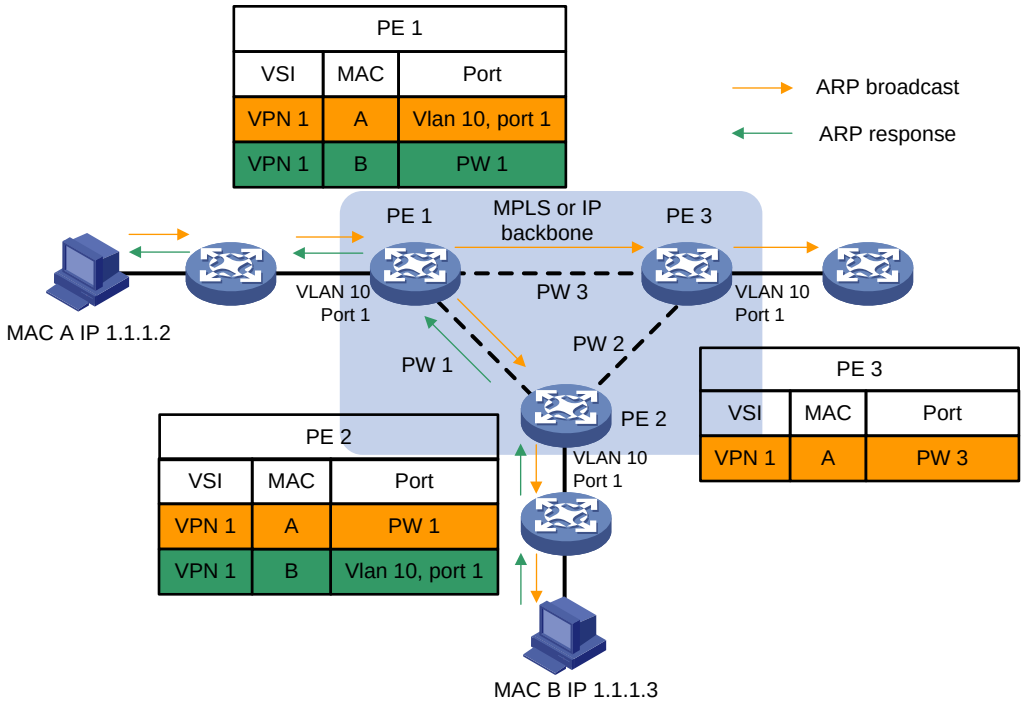
- Learning the source MAC addresses of directly connected sites.

  If the source MAC address of a packet from a CE does not exist in the MAC address table, the PE learns the source MAC address on the AC connected to the CE.

- Learning the source MAC addresses of remote sites connected through PWs.

  A VSI regards a PW as a logical Ethernet interface. If the source MAC address of a packet from a PW does not exist in the MAC address table, the PE learns the source MAC address on the PW of the VSI.

Figure 2 Source MAC address learning on a PE



The MAC address table uses an aging timer for each dynamic MAC address entry. If no packet is received from a MAC address before the aging timer expires, VPLS deletes the MAC address.

When an AC or a PW goes down, the PE deletes MAC addresses on the AC or PW. Then it sends an LDP address withdrawal message to notify all other PEs in the VPLS instance to delete those MAC addresses.

Unicast traffic forwarding and flooding

After a PE receives a unicast packet from an AC, the PE searches the MAC address table of the VSI bound to the AC for packet forwarding.

- If a match is found, the PE forwards the packet according to the matching entry. If the outgoing interface in the entry is a PW, the PE inserts the PW label to the packet, and adds the public tunnel header to the packet. It then forwards the packet to the remote PE over the PW. If the outgoing interface in the entry is a local interface, the PE directly forwards the packet to the local interface.
- If no match is found, the PE floods the packet to all other ACs and PWs in the VSI.

After a PE receives a unicast packet from a PW, the PE searches the MAC address table of the VSI bound to the PW for packet forwarding.

- If a match is found, the PE forwards the packet through the outgoing interface in the matching entry.
- If no match is found, the PE floods the packet to all ACs in the VSI.

Multicast and broadcast traffic forwarding and flooding

After a PE receives a multicast or broadcast packet from an AC, the PE floods the packet to all other ACs and the PWs in the VSI bound to the AC.

After a PE receives a multicast or broadcast packet from a PW, the PE floods the packet to all ACs in the VSI bound to the PW.

PW full mesh and split horizon

A Layer 2 network requires a loop prevention protocol such as STP to avoid loops. However, a loop prevention protocol on PEs brings management and maintenance difficulties. Therefore, VPLS uses the following methods to prevent loops:

- **Full mesh**—Every two PEs in a VPLS instance must establish a PW. The PWs form a full mesh among PEs in the VPLS instance.
- **Split horizon**—A PE does not forward packets received from a PW to any other PWs in the same VSI but only forwards those packets to ACs.

H-VPLS

VPLS requires a full mesh of PWs among all PEs in a VPLS instance. In a large-scale network, however, a full mesh of PWs causes very high PW signaling overhead and brings difficulties for network management and expansion. Hierarchical VPLS (H-VPLS) reduces the number of PWs by dividing a VPLS network into a backbone domain and edge domains.

Only static PWs and LDP PWs support H-VPLS.

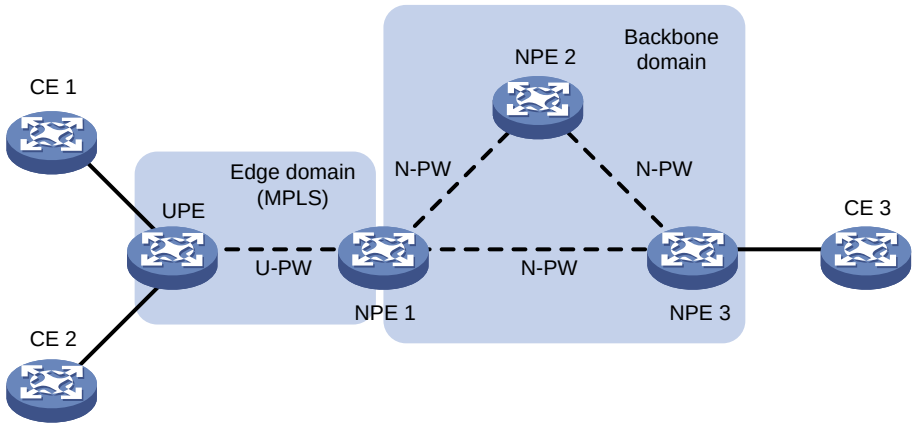
In H-VPLS:

- An edge domain provides access for a user network to the backbone domain.
- The Network Provider Edge (NPE) devices are fully meshed in the backbone domain. A PW between NPEs is referred to as an N-PW.
- A User facing-Provider Edge (UPE) device only establishes a PW with the neighboring NPE. A PW between a UPE and an NPE is referred to as a U-PW.

H-VPLS access modes

H-VPLS supports the following access modes: MPLS access and Ethernet access.

Figure 3 H-VPLS using MPLS access

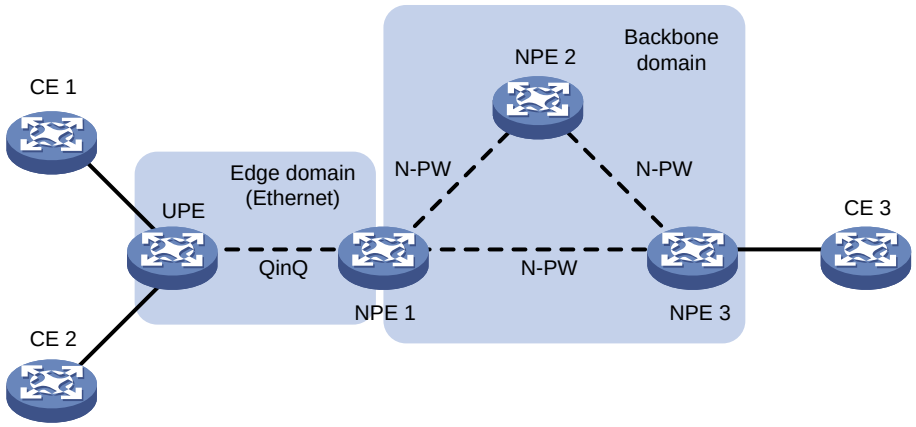


As shown in Figure 3, the edge domain is an MPLS network. The UPE creates a U-PW with NPE 1. The UPE does not create PWs to any remote PEs. After receiving a packet from a CE, the UPE adds the label assigned to the U-PW into the packet and forwards the packet to NPE 1 through a public tunnel. NPE 1 maps the packet to the VSI that corresponds to the PW label, and searches the MAC address table of the VSI to forward the packet.

NOTE:

A U-PW created on the NPE must have split horizon disabled because the NPE needs to forward packets between U-PW and N-PW.

Figure 4 H-VPLS using Ethernet access



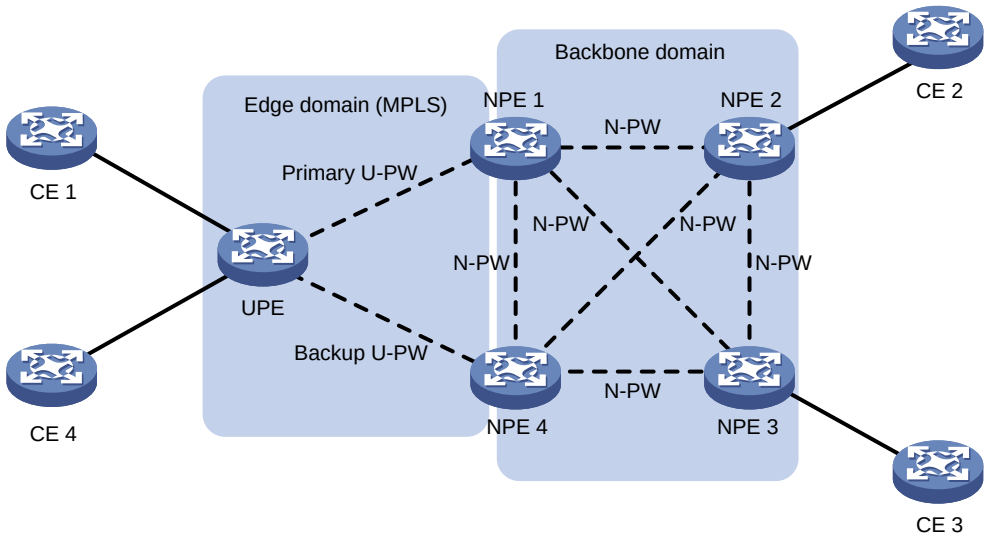
As shown in Figure 4, the edge domain is an Ethernet network. The UPE and NPE 1 establish a point-to-point Ethernet QinQ connection in between. After the UPE receives a packet from a CE, it adds an outer VLAN tag into the packet and forwards the packet to NPE 1. NPE 1 regards the outer VLAN tag as the service provider VLAN tag. It maps the packet to the VSI that corresponds to the VLAN tag and then searches the MAC address table of the VSI to forward the packet.

UPE dual homing and PW redundancy

To provide U-PW redundancy for a UPE, you can connect the UPE to two NPEs. Even if a U-PW fails, all customer sites connected to the UPE maintain the connectivity.

In the H-VPLS using MPLS access as shown in Figure 5, the UPE is connected to two NPEs through primary and backup U-PWs. The UPE uses the primary U-PW to forward traffic. When the primary U-PW fails, the UPE uses the backup U-PW to forward traffic.

Figure 5 UPE dual homing and redundancy in H-VPLS using MPLS access



The backup U-PW is used in the following scenarios:

- The primary U-PW goes down because the tunnel that carries the primary U-PW is deleted or a fault detection mechanism such as BFD detects a tunnel failure.
- The primary U-PW is deleted by the control plane. For example, the LDP session on the primary U-PW link is down, causing the primary U-PW to be deleted.
- BFD detects a failure of the primary U-PW.

- A primary and backup U-PW switchover is triggered by a command.

Configuration restrictions and guidelines

To configure VPLS, you must set the VXLAN hardware resource mode to Layer 2 gateway mode. In Layer 2 gateway mode, MPLS shares hardware resources with VXLAN. In any other mode than Layer 2 gateway mode, MPLS features are not available because no hardware resources can be used for MPLS. For more information about VXLAN hardware resource modes, see *VXLAN Configuration Guide*.

By default, a PE does not transmit LACP and LLDP packets through the VPLS network. To implement dynamic CE aggregation through the VPLS network, you must enable LACP packet transparent transmission on both the LACP packet incoming and outgoing interfaces on the PE. For information about LACP packet transparent transmission, see Ethernet link aggregation configuration in *Layer 2—LAN Switching Configuration Guide*.

If a PE is enabled with the spanning tree feature, the PE does not transmit BPDUs through the VPLS network. To enable the PE to transmit BPDUs through the VPLS network, use the **stp transparent enable** command to enable BPDU transparent transmission for the PE.

VPLS configuration task list

To configure a VPLS network, perform the following tasks:

- Configure an IGP to ensure IP connectivity within the backbone.
- Configure basic MPLS, LDP, GRE, or MPLS TE to establish public tunnels on the backbone network.
- Configure VPLS on PEs. For example, configure a VSI, establish a PW, and associate an AC and a VSI.

This chapter describes only VPLS configurations on a PE. For information about other configurations, see relevant configuration guides.

To configure VPLS on a PE, perform the following tasks:

Tasks at a glance	Remarks
(Required.) Enabling L2VPN	N/A
(Required.) Configuring an AC	N/A
(Required.) Configuring a VSI	N/A

Configuring a PW:
• (Optional.) Configuring a PW class
• (Required.) Choose either of the following tasks to configure a PW:
  ○ Configuring a static PW
  ○ Configuring an LDP PW
  ○ Configuring a BGP PW
  ○ Configuring a BGP auto-discovery LDP PW
	Choose a PW configuration method depending on the VPLS implementation.

(Required.) Binding an AC to a VSI	In an H-VPLS using MPLS access, do not perform this task on the access NPEs of the UPEs.
(Optional.) Configuring UPE dual homing: • Configuring static PW redundancy • Configuring LDP PW redundancy	N/A

Tasks at a glance	Remarks
(Required.) Configuring MAC address learning	N/A
(Optional.) Enabling SNMP notifications for L2VPN PW	N/A

Enabling L2VPN

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 backbone interface of the PE.

To enable L2VPN:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enable L2VPN.	**l2vpn enable**	By default, L2VPN is disabled.

Configuring an AC

An AC is an Ethernet service instance on a Layer 2 Ethernet 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 VSI. If the match criterion is VLAN ID, the VLAN is unique on a per-interface basis rather than on a per-device basis.

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

When you configure an Ethernet service instance, follow these restrictions and guidelines:

- Ethernet service instance and EVB are mutually exclusive on an interface. Do not configure both features on the same interface. Otherwise, the features cannot take effect. For more information about EVB, see *EVB Configuration Guide*.
- On a PE, if the interface connected to a PW and the interface connected to an AC reside on different IRF member devices, the default VLAN ID configured on the interface connected to the AC and the inner VLAN IDs configured in the **encapsulation** command must be different. The inner VLAN ID that is the same as the default VLAN ID will be removed from packets forwarded from the PW to the AC.

To configure an Ethernet service instance:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter Layer 2 Ethernet interface view or Layer 2 aggregate interface view.	• Enter Layer 2 Ethernet interface view: **interface** *interface-type interface-number* • Enter Layer 2 aggregate interface view: **interface bridge-aggregation** *interface-number*	N/A
3. Create an Ethernet service instance and enter Ethernet service instance view.	**service-instance** *instance-id*	By default, no Ethernet service instances exist.

Step	Command	Remarks
4. Configure a packet match criterion for the Ethernet service instance.	• **encapsulation s-vid** *vlan-id* [**only-tagged**] • **encapsulation s-vid** *vlan-id-list* • **encapsulation** { **default** | **tagged** | **untagged** }	By default, no packet match criterion is configured for the Ethernet service instance. If you configure the **encapsulation untagged** command on an Ethernet service instance, do not configure nesting on the Layer 2 Ethernet interface or Layer 2 aggregate interface to which the Ethernet service instance belongs. For more information about nesting, see QoS in *ACL and QoS Configuration Guide*.

5. (Optional.) Add an outer VLAN tag for incoming packets.	**rewrite inbound tag nest s-vid** *vlan-id*	By default, the device does not add an outer VLAN tag for incoming packets.
		Follow these restrictions and guidelines when you configure this command:
		• To configure both the **rewrite inbound tag nest** and **xconnect vsi** commands for the same Ethernet service instance, configure the **rewrite inbound tag nest** command first.
		• To bind an Ethernet service instance configured with the **rewrite inbound tag nest** command to a VSI, make sure the following conditions exist:
		  ○ The AC access mode of the Ethernet service instance is VLAN.
		  ○ The VSI is not bound to any Ethernet service instances that are not configured with the **rewrite inbound tag nest** command.
		• The **rewrite inbound tag nest** command does not take effect on packets with both inner and outer VLAN tags.
		• You must specify the same VLAN ID on both the local and remote PEs in the **rewrite inbound tag nest** command. The PE removes the outer VLAN ID specified by this command when it receives a packet.

Configuring a VSI

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Create a VSI and enter VSI view.	**vsi** *vsi-name*	By default, no VSIs exist.
3. (Optional.) Configure a description for the VSI.	**description** *text*	By default, no description is configured for a VSI.
4. (Optional.) Set the default PW ID for the VSI.	**default-pw-id** *default-pw-id*	By default, no default PW ID is configured for the VSI.
5. Set an MTU for the VSI.	**mtu** *size*	By default, the MTU of a VSI is 1500 bytes.
6. (Optional.) Enable the VSI.	**undo shutdown**	By default, a VSI is enabled.

Configuring a PW

Configuring a PW class

In a PW class, you can configure PW attributes such as the PW data encapsulation type, and whether to enable control word. To simplify PW configuration, you can configure PWs with the same attributes by referencing the same PW class.

To configure a PW class:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Create a PW class and enter PW class view.	**pw-class** *class-name*	By default, no PW classes exist.
3. (Optional.) Enable control word.	**control-word enable**	By default, control word is disabled.
4. (Optional.) Specify the PW data encapsulation type.	**pw-type** { **ethernet** | **vlan** } [**force-for-vpls**]	By default, the PW data encapsulation type is VLAN.

Configuring a static PW

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter VSI view.	**vsi** *vsi-name*	N/A
3. Specify static signaling for PWs, and enter VSI static view.	**pwsignaling static**	By default, no PW signaling protocol is specified.
4. Configure a static PW, and enter VSI static PW view.	**peer** *ip-address* [**pw-id** *pw-id*] **in-label** *label-value* **out-label** *label-value* [**no-split-horizon** | **pw-class** *class-name* | **tunnel-policy** *tunnel-policy-name*]	By default, no static PWs exist. If both the default PW ID in the **default-pw-id** command and a PW ID in the **peer** command are configured, the PW ID in the **peer** command is

Step	Command	Remarks
	*	used. If only the default PW ID is configured, the default PW ID is used. If no default PW ID is configured, you must provide a PW ID in the **peer** command. You must specify the **no-split-horizon** keyword to disable split horizon when you configure an NPE to establish a U-PW with a UPE.

Configuring an LDP PW

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

To configure an LDP PW:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter VSI view.	**vsi** *vsi-name*	N/A
3. Specify LDP signaling for PWs, and enter VSI LDP signaling view.	**pwsignaling ldp**	By default, no PW signaling protocol is specified.
4. Configure an LDP PW, and enter VSI LDP PW view.	**peer** *ip-address* [**pw-id** *pw-id*] [**no-split-horizon** | **pw-class** *class-name* | **tunnel-policy** *tunnel-policy-name*] *	By default, no LDP PWs exist. If both the default PW ID in the **default-pw-id** command and a PW ID in the **peer** command are configured, the PW ID in the **peer** command is used. If only the default PW ID is configured, the default PW ID is used. If no default PW ID is configured, you must provide a PW ID in the **peer** command. You must specify the **no-split-horizon** keyword to disable split horizon when you configure an NPE to establish a U-PW with a UPE.

Configuring a BGP PW

To configure a BGP PW, perform the following configurations on PEs:

- Configure BGP to advertise VPLS label block information.
- Create a BGP PW.

Configuring BGP to advertise VPLS label block information

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enable BGP instance and enter BGP instance view.	**bgp** *as-number* [**instance** *instance-name*] [**multi-session-thread**]	By default, BGP is disabled.

Step	Command	Remarks
3. Configure the remote PE as a BGP peer.	**peer** { *group-name* | *ip-address* [*mask-length*] } **as-number** *as-number*	By default, no BGP peers exist.
4. Create the BGP L2VPN address family and enter BGP L2VPN address family view.	**address-family l2vpn**	By default, no BGP L2VPN address family exists.
5. Enable BGP to exchange L2VPN information with the specified peer or peer group.	**peer** { *group-name* | *ip-address* [*mask-length*] } **enable**	By default, BGP cannot exchange L2VPN information with any peer or peer group.
6. Enable BGP to exchange label block information with the specified peer or peer group.	**peer** { *group-name* | *ip-address* [*mask-length*] } **signaling**	By default, BGP can exchange label block information with a BGP L2VPN peer or peer group.
7. (Optional.) 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.
8. (Optional.) 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.
9. (Optional.) Configure the router as an RR and specify a peer or peer group as its client.	**peer** { *group-name* | *ip-address* [*mask-length*] } **reflect-client**	By default, no RR or client is configured.
10. (Optional.) Enable L2VPN information reflection between clients.	**reflect between-clients**	By default, L2VPN information reflection is enabled between clients.
11. (Optional.) Configure the cluster ID of the RR.	**reflector cluster-id** { *cluster-id* | *ip-address* }	By default, an RR uses its own router ID as the cluster ID.
12. (Optional.) Configure the filtering of reflected L2VPN information.	**rr-filter** *ext-comm-list-number*	By default, the RR does not filter reflected L2VPN information.
13. (Optional.) Return to user view.	**return**	N/A
14. (Optional.) Soft-reset L2VPN BGP sessions.	**refresh bgp** [**instance** *instance-name*] { *ip-address* [*mask-length*] | **all** | **external** | **group** *group-name* | **internal** } { **export** | **import** } **l2vpn**	N/A
15. (Optional.) Reset L2VPN BGP sessions.	**reset bgp** [**instance** *instance-name*] { *as-number* | *ip-address* [*mask-length*] | **all** | **external** | **group** *group-name* | **internal** } **l2vpn**	N/A

For more information about the **peer as-number**, **peer enable**, **peer allow-as-loop**, **peer reflect-client**, **reflect between-clients**, **reflector cluster-id**, **refresh bgp l2vpn**, and **reset bgp l2vpn** commands, see *Layer 3—IP Routing Command Reference*.

Creating a BGP PW

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter VSI view.	**vsi** *vsi-name*	N/A
3. Configure the VSI to automatically discover neighbors through BGP and enter auto-discovery VSI view.	**auto-discovery bgp**	By default, a VSI does not automatically discover neighbors through BGP.
4. Configure an RD for the auto-discovery VSI.	**route-distinguisher** *route-distinguisher*	By default, no RD is configured for the auto-discovery VSI.
5. Configure route targets for the auto-discovery VSI.	**vpn-target** *vpn-target*&<1-8> [**both** | **export-extcommunity** | **import-extcommunity**]	By default, no route targets are configured for the auto-discovery VSI.
6. (Optional.) Specify a PW class for the auto-discovery VSI.	**pw-class** *class-name*	By default, no PW class is specified.
7. (Optional.) Specify a tunnel policy for the auto-discovery VSI.	**tunnel-policy** *tunnel-policy-name*	By default, no tunnel policy is specified.
8. Use BGP to create a PW to an automatically discovered remote PE and enter auto-discovery VSI BGP signaling view.	**signaling-protocol bgp**	By default, no signaling protocol is specified.
9. Create a local site.	**site** *site-id* [**range** *range-value*] [**default-offset** *default-offset*]	By default, no local sites exist.

Configuring a BGP auto-discovery LDP PW

Before you perform this configuration, enable MPLS LDP on interfaces and globally. For more information, see "Configuring LDP."

To configure a BGP auto-discovery LDP PW, perform the following configurations on PEs:

- Configure BGP to advertise VPLS PE information.
- Use LDP to create a PW.

Configuring BGP to advertise VPLS PE information

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enable BGP instance and enter BGP instance view.	**bgp** *as-number* [**instance** *instance-name*] [**multi-session-thread**]	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*	By default, no BGP peers exist.
4. Create the BGP L2VPN address family and enter BGP L2VPN address family view.	**address-family l2vpn**	By default, no BGP L2VPN address family exists.
5. Enable BGP to exchange	**peer** { *group-name* | *ip-address*	By default, BGP cannot exchange

Step	Command	Remarks
VPLS PE information with the specified peer or peer group.	[*mask-length*] } **enable**	VPLS PE information with a peer or peer group.
6. Enable BGP to exchange VPLS PE information with the specified peer or peer group.	**peer** { *group-name* | *ip-address* [*mask-length*] } **auto-discovery** [**non-standard**]	By default, BGP can exchange VPLS PE information with a BGP L2VPN peer or peer group by using RFC 6074 MP_REACH_NLRI.
7. (Optional.) 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.
8. (Optional.) 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.
9. (Optional.) Configure the router as an RR and specify a peer or peer group as its client.	**peer** { *group-name* | *ip-address* [*mask-length*] } **reflect-client**	By default, no RR or client is configured.
10. (Optional.) Enable L2VPN information reflection between clients.	**reflect between-clients**	By default, L2VPN information reflection is enabled between clients.
11. (Optional.) Configure the cluster ID of the RR.	**reflector cluster-id** { *cluster-id* | *ip-address* }	By default, an RR uses its own router ID as the cluster ID.
12. (Optional.) Configure the filtering of reflected L2VPN information.	**rr-filter** *ext-comm-list-number*	By default, the RR does not filter reflected L2VPN information.
13. (Optional.) Return to user view.	**return**	N/A
14. (Optional.) Soft-reset L2VPN BGP sessions.	**refresh bgp** [**instance** *instance-name*] { *ip-address* [*mask-length*] | **all** | **external** | **group** *group-name* | **internal** } { **export** | **import** } **l2vpn**	N/A
15. (Optional.) Reset L2VPN BGP sessions.	**reset bgp** [**instance** *instance-name*] { *as-number* | *ip-address* [*mask-length*] | **all** | **external** | **group** *group-name* | **internal** } **l2vpn**	N/A

For more information about the **peer as-number**, **peer enable**, **peer allow-as-loop**, **peer reflect-client**, **reflect between-clients**, **reflector cluster-id**, **refresh bgp l2vpn**, and **reset bgp l2vpn** commands, see *Layer 3—IP Routing Command Reference*.

Creating a BGP auto-discovery LDP PW

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter VSI view.	**vsi** *vsi-name*	N/A
3. Configure the VSI to automatically discover	**auto-discovery bgp**	By default, a VSI does not automatically discover neighbors

Step	Command	Remarks
neighbors through BGP and enter auto-discovery VSI view.		through BGP.
4. Configure an RD for the auto-discovery VSI.	**route-distinguisher** *route-distinguisher*	By default, no RD is configured for the auto-discovery VSI.
5. Configure route targets for the auto-discovery VSI.	**vpn-target** *vpn-target*&<1-8> [**both** | **export-extcommunity** | **import-extcommunity**]	By default, no route targets are configured for the auto-discovery VSI.
6. (Optional.) Specify a PW class for the auto-discovery VSI.	**pw-class** *class-name*	By default, no PW class is specified.
7. (Optional.) Specify a tunnel policy for the auto-discovery VSI.	**tunnel-policy** *tunnel-policy-name*	By default, no tunnel policy is specified.
8. Use LDP to create a PW to an automatically discovered remote PE and enter auto-discovery VSI LDP signaling view.	**signaling-protocol ldp**	By default, no signaling protocol is specified.
9. Configure a VPLS ID for the VSI.	**vpls-id** *vpls-id*	By default, no VPLS ID is configured.

Binding an AC to a VSI

About binding an AC to a VSI

An AC is an Ethernet service instance on a Layer 2 Ethernet interface or Layer 2 aggregate interface. After you bind an Ethernet service instance to a VSI, the Ethernet service instance matches packets received on that interface. The matching packets are then forwarded based on the MAC address table of the VSI. An Ethernet service instance can match all packets, tagged packets, or untagged packets.

When you bind an AC to a VSI, 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

You can create an Ethernet service instance on a Layer 2 aggregate interface or one of its member ports, and bind the Ethernet service instance to a VSI. The Ethernet service instance on a member port cannot come up until you remove the port from the aggregation group.

Procedure

To bind an Ethernet service instance to a VSI:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A

Step	Command	Remarks
2. Enter Layer 2 Ethernet interface view or Layer 2 aggregate interface view.	• Enter Layer 2 Ethernet interface view: **interface** *interface-type interface-number* • Enter Layer 2 aggregate interface view: **interface bridge-aggregation** *interface-number*	N/A
3. Create an Ethernet service instance and enter Ethernet service instance view.	**service-instance** *instance-id*	By default, no Ethernet service instances exist.
4. Bind the Ethernet service instance to a VSI.	**xconnect vsi** *vsi-name* [**access-mode** { **ethernet** | **vlan** }] * [**track** *track-entry-number*&<1-3>]	By default, an Ethernet service instance is not bound to any VSI.

Configuring UPE dual homing

This task includes the following configurations:

- Create a backup PW for the primary PW.
- Specify whether to switch traffic from the backup PW to the primary PW when the primary PW recovers, and set the wait time for the switchover.
- Perform a manual PW switchover.

Configuring static PW redundancy

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter VSI view.	**vsi** *vsi-name*	N/A
3. Specify static signaling for PWs, and enter VSI static view.	**pwsignaling static**	By default, no PW signaling protocol is specified for the VSI.
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. Configure a static PW and enter VSI static PW view.	**peer** *ip-address* [**pw-id** *pw-id*] [**in-label** *label-value* **out-label** *label-value*] [**no-split-horizon** | **pw-class** *class-name* | **tunnel-policy** *tunnel-policy-name*] *	By default, no static PWs exist.
6. Configure a backup static PW and enter VSI static backup 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*] *	By default, no backup static PW exists. If both the default PW ID in the **default-pw-id** command and a PW ID in the **backup-peer** command are configured, the PW ID in the **backup-peer** command is used. If only the default PW ID is configured, the default PW ID is used. If no default PW ID is configured, you must provide a

Step	Command	Remarks
		PW ID in the **backup-peer** command.
7. Return to user view.	**return**	N/A
8. Manually switch traffic of the PW to its backup PW.	**l2vpn switchover peer** *ip-address* **pw-id** *pw-id*	N/A

Configuring LDP PW redundancy

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter VSI view.	**vsi** *vsi-name*	N/A
3. Specify LDP signaling for PWs, and enter VSI LDP signaling view.	**pwsignaling ldp**	By default, no PW signaling protocol is specified for the VSI.
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. Configure an LDP PW and enter VSI LDP PW view.	**peer** *ip-address* [**pw-id** *pw-id*] [**no-split-horizon** | **pw-class** *class-name* | **tunnel-policy** *tunnel-policy-name*] *	By default, no LDP PWs exist.
6. Configure a backup LDP PW and enter VSI LDP backup PW view.	**backup-peer** *ip-address* [**pw-id** *pw-id*] [**pw-class** *class-name* | **tunnel-policy** *tunnel-policy-name*] *	By default, no backup LDP PW exists. If both the default PW ID in the **default-pw-id** command and a PW ID in the **backup-peer** command are configured, the PW ID in the **backup-peer** command is used. If only the default PW ID is configured, the default PW ID is used. If no default PW ID is configured, you must provide a PW ID in the **backup-peer** command.
7. Return to user view.	**return**	N/A
8. Manually switch traffic of the PW to its backup PW.	**l2vpn switchover peer** *ip-address* **pw-id** *pw-id*	N/A

Configuring MAC address learning

To configure MAC address learning:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter VSI view.	**vsi** *vsi-name*	N/A
3. Enable MAC address learning for the VSI.	**mac-learning enable**	By default, MAC address learning is enabled for a VSI.

Enabling 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.

To enable SNMP notifications for L2VPN PW:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
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.

Displaying and maintaining VPLS

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

Task	Command
Display LDP PW label information.	**display l2vpn ldp** [**peer** *ip-address* [**pw-id** *pw-id* | **vpls-id** *vpls-id*] | **vsi** *vsi-name*] [**verbose**]
Display L2VPN forwarding information.	**display l2vpn forwarding** { **ac | pw** } [**vsi** *vsi-name*] [**slot** *slot-number*] [**verbose**]
Display MAC address table information for one or all VSIs.	**display l2vpn mac-address** [**vsi** *vsi-name*] [**dynamic**] [**count** | **verbose**]
Display L2VPN PW information.	**display l2vpn pw** [**vsi** *vsi-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 VSI information.	**display l2vpn vsi** [**name** *vsi-name*] [**verbose**]
Display information about automatically discovered VPLS PEs.	**display l2vpn auto-discovery** [**peer** *ip-address*] [**vsi** *vsi-name*]
Display VPLS label block information.	**display l2vpn bgp** [**instance** *instance-name*] [**peer** *ip-address* | **local**] [**vsi** *vsi-name*] [**verbose**]
Display BGP L2VPN peer group information.	**display bgp** [**instance** *instance-name*] **group l2vpn** [**group-name** *group-name*]
Display VPLS PE information discovered by BGP.	**display bgp** [**instance** *instance-name*] **l2vpn auto-discovery** [**peer** *ip-address* { **advertised** | **received** } | **route-distinguisher** *route-distinguisher* [**pe-address** *ip-address* [**advertise-info**]]]
Display VPLS label block information discovered by BGP.	**display bgp** [**instance** *instance-name*] **l2vpn signaling** [**peer** *ip-address* { **advertised** | **received** } | **route-distinguisher** *route-distinguisher* [**site-id** *site-id* [**label-offset** *label-offset* [**advertise-info**]]]]
Display BGP L2VPN peer information.	**display bgp** [**instance** *instance-name*] **peer l2vpn** [*ip-address mask-length* | **group-name** *group-name*

Task	Command
	log-info | *ip-address* { **log-info** | **verbose** } | **verbose**]
Display BGP L2VPN update group information.	**display bgp** [**instance** *instance-name*] **update-group l2vpn** [*ip-address*]
Clear MAC address entries for one or all VSIs.	**reset l2vpn mac-address** [**vsi** *vsi-name*]
Reset L2VPN BGP sessions.	**reset bgp** { *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*.

VPLS configuration examples

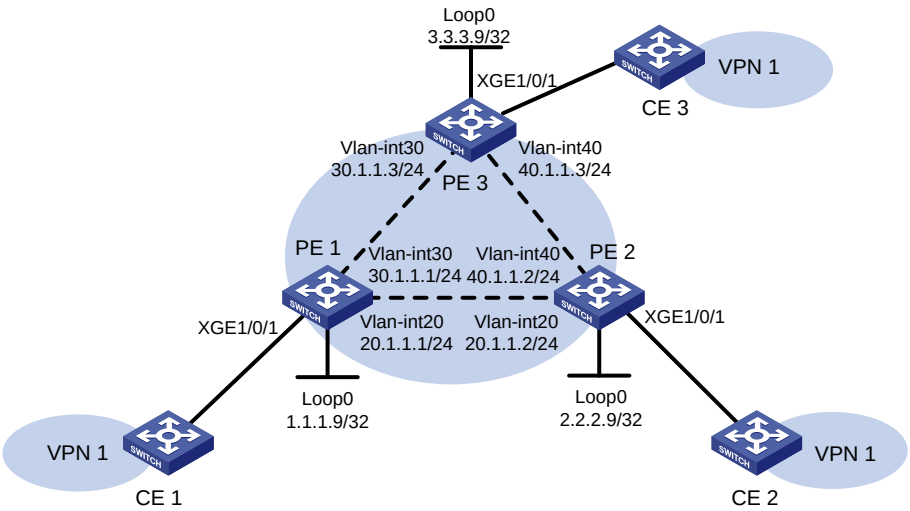
Static PW configuration example

Network requirements

Configure a VSI on each PE, and establish static PWs between the PEs to interconnect the CEs.

Configure an Ethernet service instance on Ten-GigabitEthernet 1/0/1 to match packets with an outer VLAN ID of 100 on each PE. Bind the Ethernet service instance to the VSI to forward the matching packets through the VSI.

Figure 6 Network diagram



Configuration procedure

Before configuration, disable the spanning tree feature globally or map each VLAN to an MSTI. For more information, see *Layer 2—LAN Switching Configuration Guide*.

This task includes the following configurations:

- Configure basic MPLS on each PE: configure LSR ID, enable LDP, run IGP (OSPF in this example) to establish LSPs.
- Establish static PWs: enable L2VPN, create static PWs, and specify labels.

1. Configure PE 1:

Configure an LSR ID.

```
<PE1> system-view
[PE1] interface loopback 0
[PE1-LoopBack0] ip address 1.1.1.9 32
[PE1-LoopBack0] quit
[PE1] mpls lsr-id 1.1.1.9
```

Enable L2VPN.

```
[PE1] l2vpn enable
```

Enable global LDP.

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

Configure VLAN-interface 20 (the interface connected to PE 2), and enable LDP on the interface.

```
[PE1] interface vlan-interface 20
[PE1-Vlan-interface20] ip address 20.1.1.1 24
[PE1-Vlan-interface20] mpls enable
[PE1-Vlan-interface20] mpls ldp enable
[PE1-Vlan-interface20] quit
```

Configure VLAN-interface 30 (the interface connected to PE 3), and enable LDP on the interface.

```
[PE1] interface vlan-interface 30
[PE1-Vlan-interface30] ip address 30.1.1.1 24
[PE1-Vlan-interface30] mpls enable
[PE1-Vlan-interface30] mpls ldp enable
[PE1-Vlan-interface30] quit
```

Configure OSPF for LDP to create LSPs.

```
[PE1] ospf
[PE1-ospf-1] area 0
[PE1-ospf-1-area-0.0.0.0] network 20.1.1.0 0.0.0.255
[PE1-ospf-1-area-0.0.0.0] network 30.1.1.0 0.0.0.255
[PE1-ospf-1-area-0.0.0.0] network 1.1.1.9 0.0.0.0
[PE1-ospf-1-area-0.0.0.0] quit
[PE1-ospf-1] quit
```

Create a VSI, specify the peer PEs, and establish static PWs to the peer PEs.

```
[PE1] vsi svc
[PE1-vsi-svc] pwsignaling static
[PE1-vsi-svc-static] peer 2.2.2.9 pw-id 3 in-label 100 out-label 100
[PE1-vsi-svc-static-2.2.2.9-3] quit
[PE1-vsi-svc-static] peer 3.3.3.9 pw-id 3 in-label 200 out-label 200
[PE1-vsi-svc-static-3.3.3.9-3] quit
[PE1-vsi-svc-static] quit
[PE1-vsi-svc] quit
```

Create Ethernet service instance 10 on Ten-GigabitEthernet 1/0/1 to match packets with an outer VLAN ID of 100, and bind the Ethernet service instance to the VSI **svc**.

```
[PE1] interface ten-gigabitethernet 1/0/1
[PE1-Ten-GigabitEthernet1/0/1] service-instance 10
[PE1-Ten-GigabitEthernet1/0/1-srv10] encapsulation s-vid 100
[PE1-Ten-GigabitEthernet1/0/1-srv10] xconnect vsi svc
```

2. Configure PE 2:

Configure an LSR ID.

```
<PE2> system-view
[PE2] interface loopback 0
[PE2-LoopBack0] ip address 2.2.2.9 32
[PE2-LoopBack0] quit
[PE2] mpls lsr-id 2.2.2.9
```

Enable L2VPN.

```
[PE2] l2vpn enable
```

Enable global LDP.

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

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

```
[PE2] interface vlan-interface 20
[PE2-Vlan-interface20] ip address 20.1.1.2 24
[PE2-Vlan-interface20] mpls enable
[PE2-Vlan-interface20] mpls ldp enable
[PE2-Vlan-interface20] quit
```

Configure VLAN-interface 40 (the interface connected to PE 3), and enable LDP on the interface.

```
[PE2] interface vlan-interface 40
[PE2-Vlan-interface40] ip address 40.1.1.2 24
[PE2-Vlan-interface40] mpls enable
[PE2-Vlan-interface40] mpls ldp enable
[PE2-Vlan-interface40] quit
```

Configure OSPF for LDP to create LSPs.

```
[PE2] ospf
[PE2-ospf-1] area 0
[PE2-ospf-1-area-0.0.0.0] network 20.1.1.0 0.0.0.255
[PE2-ospf-1-area-0.0.0.0] network 40.1.1.0 0.0.0.255
[PE2-ospf-1-area-0.0.0.0] network 2.2.2.9 0.0.0.0
[PE2-ospf-1-area-0.0.0.0] quit
[PE2-ospf-1] quit
```

Create a VSI, specify the peer PEs, and establish static PWs to the peer PEs.

```
[PE2] vsi svc
[PE2-vsi-svc] pwsignaling static
[PE2-vsi-svc-static] peer 1.1.1.9 pw-id 3 in-label 100 out-label 100
[PE2-vsi-svc-static-1.1.1.9-3] quit
[PE2-vsi-svc-static] peer 3.3.3.9 pw-id 3 in-label 300 out-label 300
[PE2-vsi-svc-static-3.3.3.9-3] quit
[PE2-vsi-svc-static] quit
[PE2-vsi-svc] quit
```

Create Ethernet service instance 10 on Ten-GigabitEthernet 1/0/1 to match packets with an outer VLAN ID of 100, and bind the Ethernet service instance to the VSI **svc**.

```
[PE2] interface ten-gigabitethernet 1/0/1
[PE2-Ten-GigabitEthernet1/0/1] service-instance 10
[PE2-Ten-GigabitEthernet1/0/1-srv10] encapsulation s-vid 100
```

```
[PE2-Ten-GigabitEthernet1/0/1-srv10] xconnect vsi svc
```

3. Configure PE 3:

Configure an LSR ID.

```
<PE3> system-view
[PE3] interface loopback 0
[PE3-LoopBack0] ip address 3.3.3.9 32
[PE3-LoopBack0] quit
[PE3] mpls lsr-id 3.3.3.9
```

Enable L2VPN.

```
[PE3] l2vpn enable
```

Enable global LDP.

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

Configure VLAN-interface 30 (the interface connected to PE 1), and enable LDP on the interface.

```
[PE3] interface vlan-interface 30
[PE3-Vlan-interface30] ip address 30.1.1.3 24
[PE3-Vlan-interface30] mpls enable
[PE3-Vlan-interface30] mpls ldp enable
[PE3-Vlan-interface30] quit
```

Configure VLAN-interface 40 (the interface connected to PE 2), and enable LDP on the interface.

```
[PE3] interface vlan-interface 40
[PE3-Vlan-interface40] ip address 40.1.1.3 24
[PE3-Vlan-interface40] mpls enable
[PE3-Vlan-interface40] mpls ldp enable
[PE3-Vlan-interface40] quit
```

Configure OSPF for LDP to create LSPs.

```
[PE3] ospf
[PE3-ospf-1] area 0
[PE3-ospf-1-area-0.0.0.0] network 30.1.1.0 0.0.0.255
[PE3-ospf-1-area-0.0.0.0] network 40.1.1.0 0.0.0.255
[PE3-ospf-1-area-0.0.0.0] network 3.3.3.9 0.0.0.0
[PE3-ospf-1-area-0.0.0.0] quit
[PE3-ospf-1] quit
```

Create a VSI, specify the peer PEs, and establish static PWs to the peer PEs.

```
[PE3] vsi svc
[PE3-vsi-svc] pwsignaling static
[PE3-vsi-svc-static] peer 1.1.1.9 pw-id 3 in-label 200 out-label 200
[PE3-vsi-svc-static-1.1.1.9-3] quit
[PE3-vsi-svc-static] peer 2.2.2.9 pw-id 3 in-label 300 out-label 300
[PE3-vsi-svc-static-2.2.2.9-3] quit
[PE3-vsi-svc-static] quit
[PE3-vsi-svc] quit
```

Create Ethernet service instance 10 on Ten-GigabitEthernet 1/0/1 to match packets with an outer VLAN ID of 100, and bind the Ethernet service instance to the VSI **svc**.

```
[PE3] interface ten-gigabitethernet 1/0/1
[PE3-Ten-GigabitEthernet1/0/1] service-instance 10
```

```
[PE3-Ten-GigabitEthernet1/0/1-srv10] encapsulation s-vid 100
[PE3-Ten-GigabitEthernet1/0/1-srv10] xconnect vsi svc
```

Verifying the configuration

Verify that two static PWs in up state have been established on PE 1.

```
[PE1] display l2vpn pw verbose
VSI Name: svc
  Peer: 2.2.2.9          PW ID: 3
    Signaling Protocol  : Static
    Link ID             : 8          PW State : Up
    In Label            : 100        Out Label: 100
    MTU                 : 1500
    PW Attributes       : Main
    VCCV CC             : -
    VCCV BFD            : -
    Tunnel Group ID     : 0x160000001
    Tunnel NHLFE IDs    : 1027
  Peer: 3.3.3.9          PW ID: 3
    Signaling Protocol  : Static
    Link ID             : 9          PW State : Up
    In Label            : 200        Out Label: 200
    MTU                 : 1500
    PW Attributes       : Main
    VCCV CC             : -
    VCCV BFD            : -
    Tunnel Group ID     : 0x260000002
    Tunnel NHLFE IDs    : 1028
```

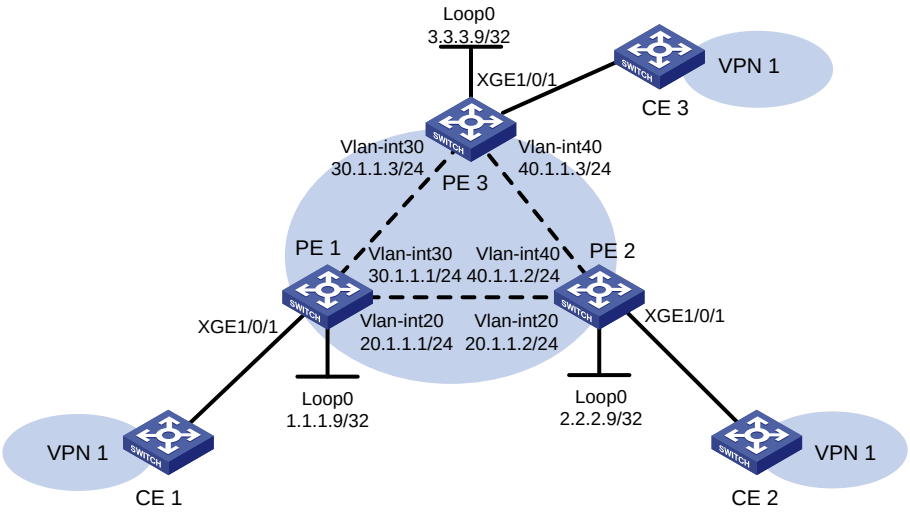
LDP PW configuration example

Network requirements

Configure a VSI on each PE, and establish LDP PWs between the PEs to interconnect the CEs.

Configure an Ethernet service instance on Ten-GigabitEthernet 1/0/1 to match packets with an outer VLAN ID of 100 on each PE. Bind the Ethernet service instance to the VSI to forward the matching packets through the VSI.

Figure 7 Network diagram



Configuration procedure

Before configuration, disable the spanning tree feature globally or map each VLAN to an MSTI. For more information, see *Layer 2—LAN Switching Configuration Guide*.

1. Configure an IGP and public tunnels on each PE. (Details not shown.)
2. Configure PE 1:

   # Configure basic MPLS.

   ```
   <PE1> system-view
   [PE1] interface loopback 0
   [PE1-LoopBack0] ip address 1.1.1.9 32
   [PE1-LoopBack0] quit
   [PE1] mpls lsr-id 1.1.1.9
   [PE1] mpls ldp
   [PE1-ldp] quit
   ```

   # Enable L2VPN.

   ```
   [PE1] l2vpn enable
   ```

   # Configure VSI **aaa** that uses LDP as the PW signaling protocol, and establish PWs to PE 2 and PE 3.

   ```
   [PE1] vsi aaa
   [PE1-vsi-aaa] pwsignaling ldp
   [PE1-vsi-aaa-ldp] peer 2.2.2.9 pw-id 500
   [PE1-vsi-aaa-ldp-2.2.2.9-500] quit
   [PE1-vsi-aaa-ldp] peer 3.3.3.9 pw-id 500
   [PE1-vsi-aaa-ldp-3.3.3.9-500] quit
   [PE1-vsi-aaa-ldp] quit
   [PE1-vsi-aaa] quit
   ```

   # Create Ethernet service instance 10 on Ten-GigabitEthernet 1/0/1 to match packets with an outer VLAN ID of 100, and bind the Ethernet service instance to the VSI **aaa**.

   ```
   [PE1] interface ten-gigabitethernet 1/0/1
   [PE1-Ten-GigabitEthernet1/0/1] service-instance 10
   [PE1-Ten-GigabitEthernet1/0/1-srv10] encapsulation s-vid 100
   [PE1-Ten-GigabitEthernet1/0/1-srv10] xconnect vsi aaa
   ```

3. Configure PE 2:

Configure basic MPLS.

```
<PE2> system-view
[PE2] interface loopback 0
[PE2-LoopBack0] ip address 2.2.2.9 32
[PE2-LoopBack0] quit
[PE2] mpls lsr-id 2.2.2.9
[PE2] mpls ldp
[PE2-ldp] quit
```

Enable L2VPN.

```
[PE2] l2vpn enable
```

Configure VSI **aaa** that uses LDP as the PW signaling protocol, and establish PWs to PE 1 and PE 3.

```
[PE2] vsi aaa
[PE2-vsi-aaa] pwsignaling ldp
[PE2-vsi-aaa-ldp] peer 1.1.1.9 pw-id 500
[PE2-vsi-aaa-ldp-1.1.1.9-500] quit
[PE2-vsi-aaa-ldp] peer 3.3.3.9 pw-id 500
[PE2-vsi-aaa-ldp-3.3.3.9-500] quit
[PE2-vsi-aaa-ldp] quit
[PE2-vsi-aaa] quit
```

Create Ethernet service instance 10 on Ten-GigabitEthernet 1/0/1 to match packets with an outer VLAN ID of 100, and bind the Ethernet service instance to the VSI **aaa**.

```
[PE2] interface ten-gigabitethernet 1/0/1
[PE2-Ten-GigabitEthernet1/0/1] service-instance 10
[PE2-Ten-GigabitEthernet1/0/1-srv10] encapsulation s-vid 100
[PE2-Ten-GigabitEthernet1/0/1-srv10] xconnect vsi aaa
```

4. Configure PE 3:

Configure basic MPLS.

```
<PE3> system-view
[PE3] interface loopback 0
[PE3-LoopBack0] ip address 3.3.3.9 32
[PE3-LoopBack0] quit
[PE3] mpls lsr-id 3.3.3.9
[PE3] mpls ldp
[PE3-ldp] quit
```

Enable L2VPN.

```
[PE3] l2vpn enable
```

Configure VSI **aaa** that uses LDP as the PW signaling protocol, and establish PWs to PE 1 and PE 2.

```
[PE3] vsi aaa
[PE3-vsi-aaa] pwsignaling ldp
[PE3-vsi-aaa-ldp] peer 1.1.1.9 pw-id 500
[PE3-vsi-aaa-ldp-1.1.1.9-500] quit
[PE3-vsi-aaa-ldp] peer 2.2.2.9 pw-id 500
[PE3-vsi-aaa-ldp-2.2.2.9-500] quit
[PE3-vsi-aaa-ldp] quit
[PE3-vsi-aaa] quit
```

Create Ethernet service instance 10 on Ten-GigabitEthernet 1/0/1 to match packets with an outer VLAN ID of 100, and bind the Ethernet service instance to the VSI **aaa**.

```
[PE3] interface ten-gigabitethernet 1/0/1
[PE3-Ten-GigabitEthernet1/0/1] service-instance 10
[PE3-Ten-GigabitEthernet1/0/1-srv10] encapsulation s-vid 100
[PE3-Ten-GigabitEthernet1/0/1-srv10] xconnect vsi aaa
```

Verifying the configuration

Verify that two LDP PWs in up state have been established on PE 1.

```
[PE1] display l2vpn pw verbose
VSI Name: aaa
  Peer: 2.2.2.9          PW ID: 500
    Signaling Protocol  : LDP
    Link ID             : 8          PW State : Up
    In Label            : 1279       Out Label: 1279
    MTU                 : 1500
    PW Attributes       : Main
    VCCV CC             : -
    VCCV BFD            : -
    Tunnel Group ID     : 0x260000000
    Tunnel NHLFE IDs    : 1028
  Peer: 3.3.3.9          PW ID: 500
    Signaling Protocol  : LDP
    Link ID             : 9          PW State : Up
    In Label            : 1278       Out Label: 1277
    MTU                 : 1500
    PW Attributes       : Main
    VCCV CC             : -
    VCCV BFD            : -
    Tunnel Group ID     : 0x360000001
    Tunnel NHLFE IDs    : 1029
```

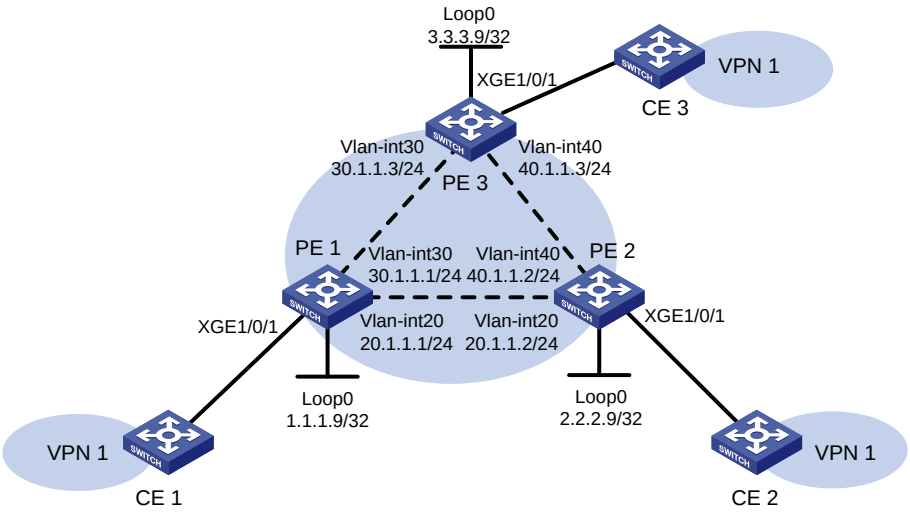
BGP PW configuration example

Network requirements

Configure a VSI on each PE, and establish BGP PWs between the PEs to interconnect CEs.

Configure an Ethernet service instance on Ten-GigabitEthernet 1/0/1 to match packets with an outer VLAN ID of 100 on each PE. Bind the Ethernet service instance to the VSI to forward the matching packets through the VSI.

Figure 8 Network diagram



Configuration procedure

Before configuration, disable the spanning tree feature globally or map each VLAN to an MSTI. For more information, see *Layer 2—LAN Switching Configuration Guide*.

1. Configure an IGP and public tunnels on each PE. (Details not shown.)
2. Configure PE 1:

   # Configure basic MPLS.

```
<PE1> system-view
[PE1] interface loopback 0
[PE1-LoopBack0] ip address 1.1.1.9 32
[PE1-LoopBack0] quit
[PE1] mpls lsr-id 1.1.1.9
[PE1] mpls ldp
[PE1-ldp] quit
```

   # Establish IBGP connections to PE 2 and PE 3, and use BGP to advertise VPLS label block information.

```
[PE1] bgp 100
[PE1-bgp-default] peer 2.2.2.9 as-number 100
[PE1-bgp-default] peer 2.2.2.9 connect-interface loopback 0
[PE1-bgp-default] peer 3.3.3.9 as-number 100
[PE1-bgp-default] peer 3.3.3.9 connect-interface loopback 0
[PE1-bgp-default] address-family l2vpn
[PE1-bgp-default-l2vpn] peer 2.2.2.9 enable
[PE1-bgp-default-l2vpn] peer 3.3.3.9 enable
[PE1-bgp-default-l2vpn] quit
[PE1-bgp-default] quit
```

   # Enable L2VPN.

```
[PE1] l2vpn enable
```

   # Configure VSI **aaa** to use BGP to establish BGP PWs to PE 2 and PE 3.

```
[PE1] vsi aaa
[PE1-vsi-aaa] auto-discovery bgp
[PE1-vsi-aaa-auto] route-distinguisher 1:1
```

```
[PE1-vsi-aaa-auto] vpn-target 1:1
[PE1-vsi-aaa-auto] signaling-protocol bgp
[PE1-vsi-aaa-auto-bgp] site 1 range 10 default-offset 0
[PE1-vsi-aaa-auto-bgp] quit
[PE1-vsi-aaa-auto] quit
[PE1-vsi-aaa] quit
```

Create Ethernet service instance 10 on Ten-GigabitEthernet 1/0/1 to match packets with an outer VLAN ID of 100, and bind the Ethernet service instance to the VSI **aaa**.

```
[PE1] interface ten-gigabitethernet 1/0/1
[PE1-Ten-GigabitEthernet1/0/1] service-instance 10
[PE1-Ten-GigabitEthernet1/0/1-srv10] encapsulation s-vid 100
[PE1-Ten-GigabitEthernet1/0/1-srv10] xconnect vsi aaa
```

3. Configure PE 2:

Configure basic MPLS.

```
<PE2> system-view
[PE2] interface loopback 0
[PE2-LoopBack0] ip address 2.2.2.9 32
[PE2-LoopBack0] quit
[PE2] mpls lsr-id 2.2.2.9
[PE2] mpls ldp
[PE2-ldp] quit
```

Establish IBGP connections to PE 2 and PE 3, and use BGP to advertise VPLS label block information.

```
[PE2] bgp 100
[PE2-bgp-default] peer 1.1.1.9 as-number 100
[PE2-bgp-default] peer 1.1.1.9 connect-interface loopback 0
[PE2-bgp-default] peer 3.3.3.9 as-number 100
[PE2-bgp-default] peer 3.3.3.9 connect-interface loopback 0
[PE2-bgp-default] address-family l2vpn
[PE2-bgp-default-l2vpn] peer 1.1.1.9 enable
[PE2-bgp-default-l2vpn] peer 3.3.3.9 enable
[PE2-bgp-default-l2vpn] quit
[PE2-bgp-default] quit
```

Enable L2VPN.

```
[PE2] l2vpn enable
```

Configure VSI **aaa** to use BGP to establish BGP PWs to PE 1 and PE 3.

```
[PE2] vsi aaa
[PE2-vsi-aaa] auto-discovery bgp
[PE2-vsi-aaa-auto] route-distinguisher 1:1
[PE2-vsi-aaa-auto] vpn-target 1:1
[PE2-vsi-aaa-auto] signaling-protocol bgp
[PE2-vsi-aaa-auto-bgp] site 2 range 10 default-offset 0
[PE2-vsi-aaa-auto-bgp] quit
[PE2-vsi-aaa-auto] quit
[PE2-vsi-aaa] quit
```

Create Ethernet service instance 10 on Ten-GigabitEthernet 1/0/1 to match packets with an outer VLAN ID of 100, and bind the Ethernet service instance to the VSI **aaa**.

```
[PE2] interface ten-gigabitethernet 1/0/1
```

```
[PE2-Ten-GigabitEthernet1/0/1] service-instance 10
[PE2-Ten-GigabitEthernet1/0/1-srv10] encapsulation s-vid 100
[PE2-Ten-GigabitEthernet1/0/1-srv10] xconnect vsi aaa
```

4. Configure PE 3:

Configure basic MPLS.

```
<PE3> system-view
[PE3] interface loopback 0
[PE3-LoopBack0] ip address 3.3.3.9 32
[PE3-LoopBack0] quit
[PE3] mpls lsr-id 3.3.3.9
[PE3] mpls ldp
[PE3-ldp] quit
```

Establish IBGP connections to PE 1 and PE 2, and use BGP to advertise VPLS label block information.

```
[PE3] bgp 100
[PE3-bgp-default] peer 1.1.1.9 as-number 100
[PE3-bgp-default] peer 1.1.1.9 connect-interface loopback 0
[PE3-bgp-default] peer 2.2.2.9 as-number 100
[PE3-bgp-default] peer 2.2.2.9 connect-interface loopback 0
[PE3-bgp-default] address-family l2vpn
[PE3-bgp-default-l2vpn] peer 1.1.1.9 enable
[PE3-bgp-default-l2vpn] peer 2.2.2.9 enable
[PE3-bgp-default-l2vpn] quit
[PE3-bgp-default] quit
```

Enable L2VPN.

```
[PE3] l2vpn enable
```

Configure VSI **aaa** to use BGP to establish BGP PWs to PE 1 and PE 2.

```
[PE3] vsi aaa
[PE3-vsi-aaa] auto-discovery bgp
[PE3-vsi-aaa-auto] route-distinguisher 1:1
[PE3-vsi-aaa-auto] vpn-target 1:1
[PE3-vsi-aaa-auto] signaling-protocol bgp
[PE3-vsi-aaa-auto-bgp] site 3 range 10 default-offset 0
[PE3-vsi-aaa-auto-bgp] quit
[PE3-vsi-aaa-auto] quit
[PE3-vsi-aaa] quit
```

Create Ethernet service instance 10 on Ten-GigabitEthernet 1/0/1 to match packets with an outer VLAN ID of 100, and bind the Ethernet service instance to the VSI **aaa**.

```
[PE3] interface ten-gigabitethernet 1/0/1
[PE3-Ten-GigabitEthernet1/0/1] service-instance 10
[PE3-Ten-GigabitEthernet1/0/1-srv10] encapsulation s-vid 100
[PE3-Ten-GigabitEthernet1/0/1-srv10] xconnect vsi aaa
```

Verifying the configuration

Verify that two BGP PWs have been established on PE 1.

```
[PE1] display l2vpn pw verbose
VSI Name: aaa
  Peer: 2.2.2.9          Remote Site: 2
    Signaling Protocol  : BGP
```

```
    Link ID             : 9          PW State : Up
    In Label            : 1295       Out Label: 1025
    MTU                 : 1500
    PW Attributes       : Main
    VCCV CC             : -
    VCCV BFD            : -
    Tunnel Group ID     : 0x800000160000001
    Tunnel NHLFE IDs    : 1027
  Peer: 3.3.3.9          Remote Site: 3
    Signaling Protocol  : BGP
    Link ID             : 10         PW State : Up
    In Label            : 1296       Out Label: 1025
    MTU                 : 1500
    PW Attributes       : Main
    VCCV CC             : -
    VCCV BFD            : -
    Tunnel Group ID     : 0x800000060000000
    Tunnel NHLFE IDs    : 1026
```

Display VPLS label block information received from PE 2 and PE 3 on PE 1.

```
[PE1] display l2vpn bgp verbose
VSI Name: aaa
 Remote Site ID     : 2
 Offset             : 0
 RD                 : 1:1
 PW State           : Up
 Encapsulation      : BGP-VPLS
 MTU                : 1500
 Nexthop            : 2.2.2.9
 Local VC Label     : 1295
 Remote VC Label    : 1025
 Link ID            : 9
 Local Label Block  : 1293/10/0
 Remote Label Block : 1024/10/0
 Export Route Target: 1:1

 Remote Site ID     : 3
 Offset             : 0
 RD                 : 1:1
 PW State           : Up
 Encapsulation      : BGP-VPLS
 MTU                : 1500
 Nexthop            : 3.3.3.9
 Local VC Label     : 1296
 Remote VC Label    : 1025
 Link ID            : 10
 Local Label Block  : 1293/10/0
 Remote Label Block : 1024/10/0
 Export Route Target: 1:1
```

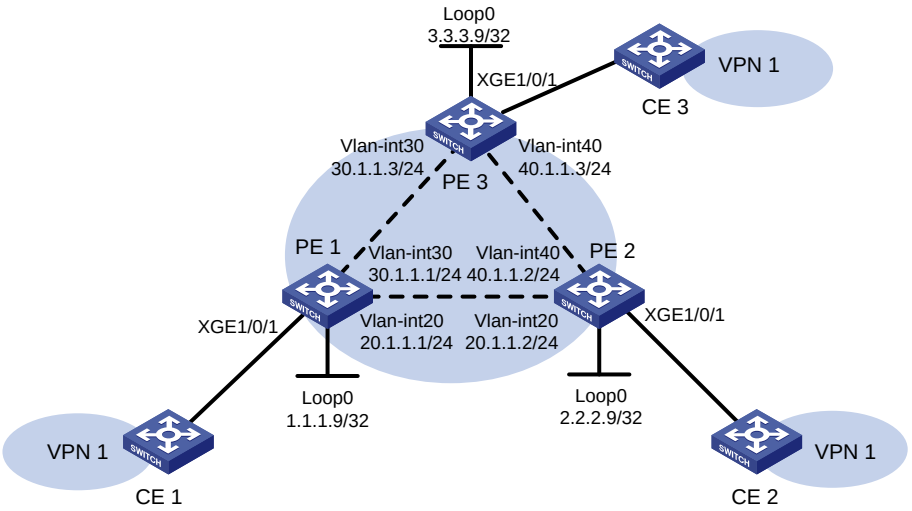
BGP auto-discovery LDP PW configuration example

Network requirements

Configure a VSI on each PE. Use BGP to discover remote PEs and use LDP to create PWs among PEs so CEs in different sites of VPN 1 can communicate with each other.

Configure an Ethernet service instance on Ten-GigabitEthernet 1/0/1 to match packets with an outer VLAN ID of 100 on each PE. Bind the Ethernet service instance to the VSI to forward the matching packets through the VSI.

Figure 9 Network diagram



Configuration procedure

Before configuration, disable the spanning tree feature globally or map each VLAN to an MSTI. For more information, see *Layer 2—LAN Switching Configuration Guide*.

1. Configure an IGP and public tunnels on each PE. (Details not shown.)
2. Configure PE 1:

   # Configure basic MPLS.

```
<PE1> system-view
[PE1] interface loopback 0
[PE1-LoopBack0] ip address 1.1.1.9 32
[PE1-LoopBack0] quit
[PE1] mpls lsr-id 1.1.1.9
[PE1] mpls ldp
[PE1-ldp] quit
```

   # Establish IBGP connections to PE 1 and PE 2, and use BGP to advertise VPLS PE information.

```
[PE1] bgp 100
[PE1-bgp-default] peer 2.2.2.9 as-number 100
[PE1-bgp-default] peer 2.2.2.9 connect-interface loopback 0
[PE1-bgp-default] peer 3.3.3.9 as-number 100
[PE1-bgp-default] peer 3.3.3.9 connect-interface loopback 0
[PE1-bgp-default] address-family l2vpn
[PE1-bgp-default-l2vpn] peer 2.2.2.9 enable
[PE1-bgp-default-l2vpn] peer 3.3.3.9 enable
```

```
[PE1-bgp-default-l2vpn] quit
[PE1-bgp-default] quit
```

Enable L2VPN.

```
[PE1] l2vpn enable
```

Configure VSI **aaa** to use BGP to discover remote PEs and use LDP to establish LDP PWs to PE 2 and PE 3.

```
[PE1] vsi aaa
[PE1-vsi-aaa] auto-discovery bgp
[PE1-vsi-aaa-auto] route-distinguisher 1:1
[PE1-vsi-aaa-auto] vpn-target 1:1
[PE1-vsi-aaa-auto] signaling-protocol ldp
[PE1-vsi-aaa-auto-ldp] vpls-id 100:100
[PE1-vsi-aaa-auto-ldp] quit
[PE1-vsi-aaa-auto] quit
[PE1-vsi-aaa] quit
```

Create Ethernet service instance 10 on Ten-GigabitEthernet 1/0/1 to match packets with an outer VLAN ID of 100, and bind the Ethernet service instance to the VSI **aaa**.

```
[PE1] interface ten-gigabitethernet 1/0/1
[PE1-Ten-GigabitEthernet1/0/1] service-instance 10
[PE1-Ten-GigabitEthernet1/0/1-srv10] encapsulation s-vid 100
[PE1-Ten-GigabitEthernet1/0/1-srv10] xconnect vsi aaa
```

3. Configure PE 2:

Configure basic MPLS.

```
<PE2> system-view
[PE2] interface loopback 0
[PE2-LoopBack0] ip address 2.2.2.9 32
[PE2-LoopBack0] quit
[PE2] mpls lsr-id 2.2.2.9
[PE2] mpls ldp
[PE2-ldp] quit
```

Establish IBGP connections to PE 1 and PE 3, and use BGP to advertise VPLS PE information.

```
[PE2] bgp 100
[PE2-bgp-default] peer 1.1.1.9 as-number 100
[PE2-bgp-default] peer 1.1.1.9 connect-interface loopback 0
[PE2-bgp-default] peer 3.3.3.9 as-number 100
[PE2-bgp-default] peer 3.3.3.9 connect-interface loopback 0
[PE2-bgp-default] address-family l2vpn
[PE2-bgp-default-l2vpn] peer 1.1.1.9 enable
[PE2-bgp-default-l2vpn] peer 3.3.3.9 enable
[PE2-bgp-default-l2vpn] quit
[PE2-bgp-default] quit
```

Enable L2VPN.

```
[PE2] l2vpn enable
```

Configure VSI **aaa** to use BGP to discover remote PEs and use LDP to establish LDP PWs to PE 1 and PE 3.

```
[PE2] vsi aaa
[PE2-vsi-aaa] auto-discovery bgp
```

```
[PE2-vsi-aaa-auto] route-distinguisher 1:1
[PE2-vsi-aaa-auto] vpn-target 1:1
[PE2-vsi-aaa-auto] signaling-protocol ldp
[PE2-vsi-aaa-auto-ldp] vpls-id 100:100
[PE2-vsi-aaa-auto-ldp] quit
[PE2-vsi-aaa-auto] quit
[PE2-vsi-aaa] quit
```

Create Ethernet service instance 10 on Ten-GigabitEthernet 1/0/1 to match packets with an outer VLAN ID of 100, and bind the Ethernet service instance to the VSI **aaa**.

```
[PE2] interface ten-gigabitethernet 1/0/1
[PE2-Ten-GigabitEthernet1/0/1] service-instance 10
[PE2-Ten-GigabitEthernet1/0/1-srv10] encapsulation s-vid 100
[PE2-Ten-GigabitEthernet1/0/1-srv10] xconnect vsi aaa
```

4. Configure PE 3:

Configure basic MPLS.

```
<PE3> system-view
[PE3] interface loopback 0
[PE3-LoopBack0] ip address 3.3.3.9 32
[PE3-LoopBack0] quit
[PE3] mpls lsr-id 3.3.3.9
[PE3] mpls ldp
[PE3-ldp] quit
```

Establish IBGP connections to PE 1 and PE 2, and use BGP to advertise VPLS PE information.

```
[PE3] bgp 100
[PE3-bgp-default] peer 1.1.1.9 as-number 100
[PE3-bgp-default] peer 1.1.1.9 connect-interface loopback 0
[PE3-bgp-default] peer 2.2.2.9 as-number 100
[PE3-bgp-default] peer 2.2.2.9 connect-interface loopback 0
[PE3-bgp-default] address-family l2vpn
[PE3-bgp-default-l2vpn] peer 1.1.1.9 enable
[PE3-bgp-default-l2vpn] peer 2.2.2.9 enable
[PE3-bgp-default-l2vpn] quit
[PE3-bgp-default] quit
```

Enable L2VPN.

```
[PE3] l2vpn enable
```

Configure VSI **aaa** to use BGP to discover remote PEs and use LDP to establish LDP PWs to PE 1 and PE 2.

```
[PE3] vsi aaa
[PE3-vsi-aaa] auto-discovery bgp
[PE3-vsi-aaa-auto] route-distinguisher 1:1
[PE3-vsi-aaa-auto] vpn-target 1:1
[PE3-vsi-aaa-auto] signaling-protocol ldp
[PE3-vsi-aaa-auto-ldp] vpls-id 100:100
[PE3-vsi-aaa-auto-ldp] quit
[PE3-vsi-aaa-auto] quit
[PE3-vsi-aaa] quit
```

Create Ethernet service instance 10 on Ten-GigabitEthernet 1/0/1 to match packets with an outer VLAN ID of 100, and bind the Ethernet service instance to the VSI **aaa**.

```
[PE3] interface ten-gigabitethernet 1/0/1
[PE3-Ten-GigabitEthernet1/0/1] service-instance 10
[PE3-Ten-GigabitEthernet1/0/1-srv10] encapsulation s-vid 100
[PE3-Ten-GigabitEthernet1/0/1-srv10] xconnect vsi aaa
```

Verifying the configuration

Verify that two PWs have been established on PE 1.

```
[PE1] display l2vpn pw verbose
VSI Name: aaa
  Peer: 2.2.2.9          VPLS ID: 100:100
    Signaling Protocol  : LDP
    Link ID             : 8          PW State : Up
    In Label            : 1555       Out Label: 1555
    MTU                 : 1500
    PW Attributes       : Main
    VCCV CC             : -
    VCCV BFD            : -
    Tunnel Group ID     : 0x800000060000000
    Tunnel NHLFE IDs    : 1029
  Peer: 3.3.3.9          VPLS ID: 100:100
    Signaling Protocol  : LDP
    Link ID             : 9          PW State : Up
    In Label            : 1554       Out Label: 1416
    MTU                 : 1500
    PW Attributes       : Main
    VCCV CC             : -
    VCCV BFD            : -
    Tunnel Group ID     : 0x800000160000001
    Tunnel NHLFE IDs    : 1030
```

Display LDP PW label information on PE 1.

```
[PE1] display l2vpn ldp verbose
Peer: 2.2.2.9          VPLS ID: 100:100
  VSI Name: aaa
  PW State: Up
  PW Status Communication: Notification method
  PW ID FEC (Local/Remote):
    Local AII   : (1.1.1.9, 2.2.2.9)
    Remote AII  : (2.2.2.9, 1.1.1.9)
    PW Type     : VLAN/VLAN
    Group ID    : 0/0
    Label       : 1555/1555
    Control Word: Disabled/Disabled
    VCCV CV Type: -/-
    VCCV CC Type: -/-
    MTU         : 1500/1500
    PW Status   : PW forwarding/PW forwarding
```

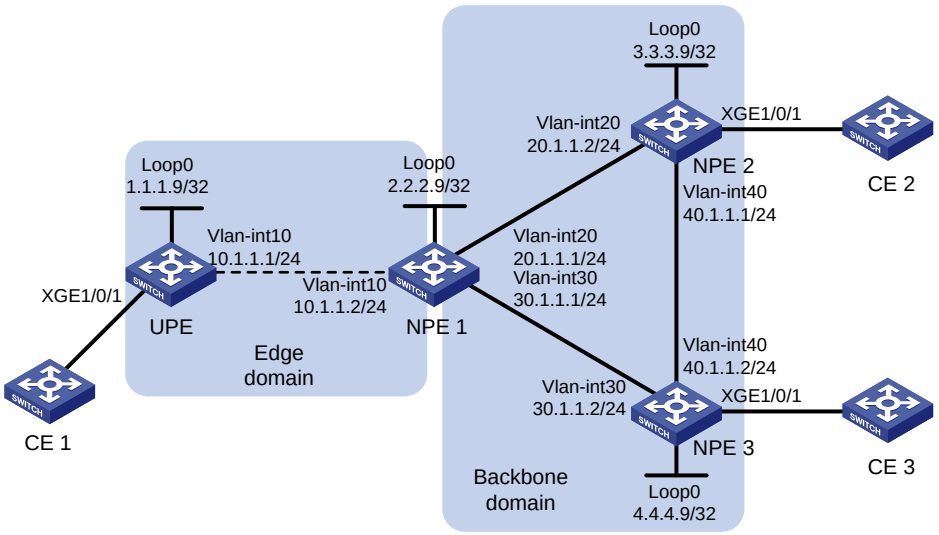
```
Peer: 3.3.3.9          VPLS ID: 100:100
  VSI Name: aaa
  PW State: Up
  PW Status Communication: Notification method
  PW ID FEC (Local/Remote):
    Local AII   : (1.1.1.9, 3.3.3.9)
    Remote AII  : (3.3.3.9, 1.1.1.9)
    PW Type     : VLAN/VLAN
    Group ID    : 0/0
    Label       : 1554/1416
    Control Word: Disabled/Disabled
    VCCV CV Type: -/-
    VCCV CC Type: -/-
    MTU         : 1500/1500
    PW Status   : PW forwarding/PW forwarding
```

H-VPLS using MPLS access configuration example

Network requirements

Configure an H-VPLS network using MPLS access to avoid full-mesh PW configuration. The H-VPLS uses LDP as the PW signaling protocol.

Figure 10 Network diagram



Configuration procedure

Before configuration, disable the spanning tree feature globally or map each VLAN to an MSTI. For more information, see *Layer 2—LAN Switching Configuration Guide*.

1. Configure an IGP and public tunnels on each PE. (Details not shown.)
2. Configure UPE:

   # Configure basic MPLS.

   ```
   <UPE> system-view
   [UPE] interface loopback 0
   [UPE-LoopBack0] ip address 1.1.1.9 32
   [UPE-LoopBack0] quit
   ```

```
[UPE] mpls lsr-id 1.1.1.9
[UPE] mpls ldp
[UPE-ldp] quit
```

Enable L2VPN.

```
[UPE] l2vpn enable
```

Configure VSI **aaa** to use LDP to establish a U-PW to NPE 1.

```
[UPE] vsi aaa
[UPE-vsi-aaa] pwsignaling ldp
[UPE-vsi-aaa-ldp] peer 2.2.2.9 pw-id 500
[UPE-vsi-aaa-ldp-2.2.2.9-500] quit
[UPE-vsi-aaa-ldp] quit
[UPE-vsi-aaa] quit
```

Create Ethernet service instance 10 on Ten-GigabitEthernet 1/0/1 to match packets with an outer VLAN ID of 100, and bind the Ethernet service instance to the VSI **aaa**.

```
[UPE] interface ten-gigabitethernet 1/0/1
[UPE-Ten-GigabitEthernet1/0/1] service-instance 10
[UPE-Ten-GigabitEthernet1/0/1-srv10] encapsulation s-vid 100
[UPE-Ten-GigabitEthernet1/0/1-srv10] xconnect vsi aaa
```

3. Configure NPE 1:

Configure basic MPLS.

```
<NPE1> system-view
[NPE1] interface loopback 0
[NPE1-LoopBack0] ip address 2.2.2.9 32
[NPE1-LoopBack0] quit
[NPE1] mpls lsr-id 2.2.2.9
[NPE1] mpls ldp
[NPE1–ldp] quit
```

Enable L2VPN.

```
[NPE1] l2vpn enable
```

Configure VSI **aaa** that uses LDP as the PW signaling protocol, establish a U-PW to the UPE, and establish N-PWs to NPE 2 and NPE 3.

```
[NPE1] vsi aaa
[NPE1-vsi-aaa] pwsignaling ldp
[NPE1-vsi-aaa-ldp] peer 1.1.1.9 pw-id 500 no-split-horizon
[NPE1-vsi-aaa-ldp-1.1.1.9-500] quit
[NPE1-vsi-aaa-ldp] peer 3.3.3.9 pw-id 500
[NPE1-vsi-aaa-ldp-3.3.3.9-500] quit
[NPE1-vsi-aaa-ldp] peer 4.4.4.9 pw-id 500
[NPE1-vsi-aaa-ldp-4.4.4.9-500] quit
[NPE1-vsi-aaa-ldp] quit
[NPE1-vsi-aaa] quit
```

4. Configure NPE 2:

Configure basic MPLS.

```
<NPE2> system-view
[NPE2] interface loopback 0
[NPE2-LoopBack0] ip address 3.3.3.9 32
[NPE2-LoopBack0] quit
[NPE2] mpls lsr-id 3.3.3.9
```

```
[NPE2] mpls ldp
[NPE2–ldp] quit
```

Enable L2VPN.

```
[NPE2] l2vpn enable
```

Configure VSI **aaa** that uses LDP as the PW signaling protocol, and establish N-PWs to NPE 1 and NPE 3.

```
[NPE2] vsi aaa
[NPE2-vsi-aaa] pwsignal ldp
[NPE2-vsi-aaa-ldp] peer 2.2.2.9 pw-id 500
[NPE2-vsi-aaa-ldp-2.2.2.9-500] quit
[NPE2-vsi-aaa-ldp] peer 4.4.4.9 pw-id 500
[NPE2-vsi-aaa-ldp-4.4.4.9-500] quit
[NPE2-vsi-aaa-ldp] quit
[NPE2-vsi-aaa] quit
```

Create Ethernet service instance 10 on Ten-GigabitEthernet 1/0/1 to match packets with an outer VLAN ID of 100, and bind the Ethernet service instance to the VSI **aaa**.

```
[NPE2] interface ten-gigabitethernet 1/0/1
[NPE2-Ten-GigabitEthernet1/0/1] service-instance 10
[NPE2-Ten-GigabitEthernet1/0/1-srv10] encapsulation s-vid 100
[NPE2-Ten-GigabitEthernet1/0/1-srv10] xconnect vsi aaa
[NPE2-Ten-GigabitEthernet1/0/1-srv10] quit
[NPE2-Ten-GigabitEthernet1/0/1] quit
```

5. Configure NPE 3:

Configure basic MPLS.

```
<NPE3> system-view
[NPE3] interface loopback 0
[NPE3-LoopBack0] ip address 4.4.4.9 32
[NPE3-LoopBack0] quit
[NPE3] mpls lsr-id 4.4.4.9
[NPE3] mpls ldp
[NPE3–ldp] quit
```

Enable L2VPN.

```
[NPE3] l2vpn enable
```

Configure VSI **aaa** that uses LDP as the PW signaling protocol, and establish N-PWs to NPE 1 and NPE 2.

```
[NPE3] vsi aaa
[NPE3-vsi-aaa] pwsignal ldp
[NPE3-vsi-aaa-ldp] peer 2.2.2.9 pw-id 500
[NPE3-vsi-aaa-ldp-2.2.2.9-500] quit
[NPE3-vsi-aaa-ldp] peer 3.3.3.9 pw-id 500
[NPE3-vsi-aaa-ldp-3.3.3.9-500] quit
[NPE3-vsi-aaa-ldp] quit
[NPE3-vsi-aaa] quit
```

Create Ethernet service instance 10 on Ten-GigabitEthernet 1/0/1 to match packets with an outer VLAN ID of 100, and bind the Ethernet service instance to the VSI **aaa**.

```
[NPE3] interface ten-gigabitethernet 1/0/1
[NPE3-Ten-GigabitEthernet1/0/1] service-instance 10
[NPE3-Ten-GigabitEthernet1/0/1-srv10] encapsulation s-vid 100
```

```
[NPE3-Ten-GigabitEthernet1/0/1-srv10] xconnect vsi aaa
[NPE3-Ten-GigabitEthernet1/0/1-srv10] quit
[NPE3-Ten-GigabitEthernet1/0/1] quit
```

Verifying the configuration

Verify that PWs in up state have been established on each PE.

```
[UPE] display l2vpn pw verbose
VSI Name: aaa
  Peer: 2.2.2.9          PW ID: 500
    Signaling Protocol  : LDP
    Link ID             : 8          PW State : Up
    In Label            : 1277       Out Label: 1277
    MTU                 : 1500
    PW Attributes       : Main
    VCCV CC             : -
    VCCV BFD            : -
    Tunnel Group ID     : 0x460000000
    Tunnel NHLFE IDs    : 1030
[NPE1] display l2vpn pw verbose
VSI Name: aaa
  Peer: 1.1.1.9          PW ID: 500
    Signaling Protocol  : LDP
    Link ID             : 8          PW State : Up
    In Label            : 1277       Out Label: 1277
    MTU                 : 1500
    PW Attributes       : Main, No-split-horizon
    VCCV CC             : -
    VCCV BFD            : -
    Tunnel Group ID     : 0x460000000
    Tunnel NHLFE IDs    : 1030
  Peer: 3.3.3.9          PW ID: 500
    Signaling Protocol  : LDP
    Link ID             : 9          PW State : Up
    In Label            : 1276       Out Label: 1275
    MTU                 : 1500
    PW Attributes       : Main
    VCCV CC             : -
    VCCV BFD            : -
    Tunnel Group ID     : 0x560000001
    Tunnel NHLFE IDs    : 1031
  Peer: 4.4.4.9          PW ID: 500
    Signaling Protocol  : LDP
    Link ID             : 10          PW State : Up
    In Label            : 1278       Out Label: 1279
    MTU                 : 1500
    PW Attributes       : Main
    VCCV CC             : -
    VCCV BFD            : -
    Tunnel Group ID     : 0x570000001
```

```
    Tunnel NHLFE IDs    : 1032
[NPE2] display l2vpn pw verbose
VSI Name: aaa
  Peer: 2.2.2.9          PW ID: 500
    Signaling Protocol  : LDP
    Link ID             : 8          PW State : Up
    In Label            : 1275       Out Label: 1276
    MTU                 : 1500
    PW Attributes       : Main
    VCCV CC             : -
    VCCV BFD            : -
    Tunnel Group ID     : 0x660000000
    Tunnel NHLFE IDs    : 1031
  Peer: 4.4.4.9          PW ID: 500
    Signaling Protocol  : LDP
    Link ID             : 9          PW State : Up
    In Label            : 1277       Out Label: 1277
    MTU                 : 1500
    PW Attributes       : Main
    VCCV CC             : -
    VCCV BFD            : -
    Tunnel Group ID     : 0x670000000
    Tunnel NHLFE IDs    : 1032
[NPE3] display l2vpn pw verbose
VSI Name: aaa
  Peer: 2.2.2.9          PW ID: 500
    Signaling Protocol  : LDP
    Link ID             : 8          PW State : Up
    In Label            : 1279       Out Label: 1278
    MTU                 : 1500
    PW Attributes       : Main
    VCCV CC             : -
    VCCV BFD            : -
    Tunnel Group ID     : 0x660000000
    Tunnel NHLFE IDs    : 1031
  Peer: 3.3.3.9          PW ID: 500
    Signaling Protocol  : LDP
    Link ID             : 9          PW State : Up
    In Label            : 1277       Out Label: 1277
    MTU                 : 1500
    PW Attributes       : Main
    VCCV CC             : -
    VCCV BFD            : -
    Tunnel Group ID     : 0x670000000
    Tunnel NHLFE IDs    : 1032
```

Ethernet service instance and VSI binding configuration example

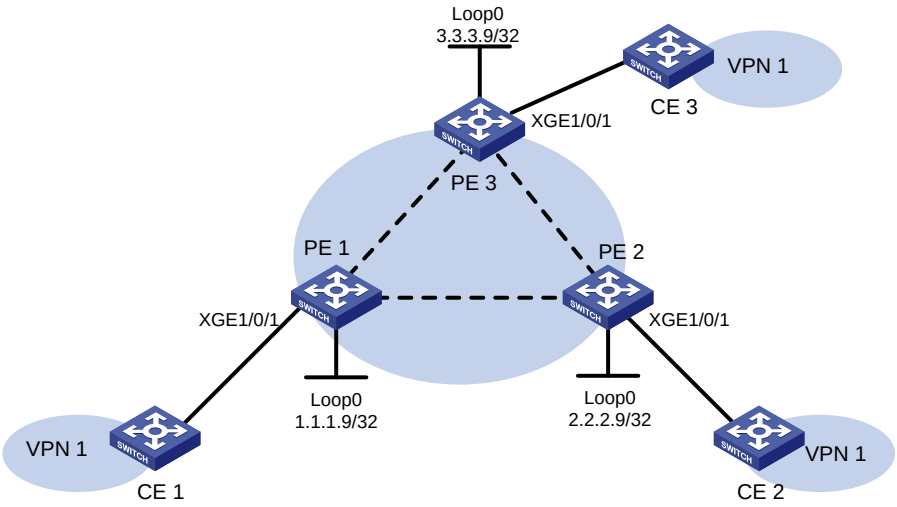
Network requirements

As shown in Figure 11, CE 1, CE 2, and CE 3 access PE 1, PE 2, and PE 3 in VLAN mode.

Configure a VSI on each PE, and establish LDP PWs between the PEs to interconnect the CEs.

Configure an Ethernet service instance on Ten-GigabitEthernet 1/0/1 of each PE to match packets with VLAN ID 100. Bind the Ethernet service instance to the VSI to forward the matching packets through the VSI.

Figure 11 Network diagram



Configuration procedure

Before configuration, disable the spanning tree feature globally or map each VLAN to an MSTI. For more information, see *Layer 2—LAN Switching Configuration Guide*.

1. Configure an IGP and public tunnels on each PE. (Details not shown.)
2. Configure PE 1:

   # Configure basic MPLS.

   ```
   <PE1> system-view
   [PE1] interface loopback 0
   [PE1-LoopBack0] ip address 1.1.1.9 32
   [PE1-LoopBack0] quit
   [PE1] mpls lsr-id 1.1.1.9
   [PE1] mpls ldp
   [PE1-ldp] quit
   ```

   # Enable L2VPN.

   ```
   [PE1] l2vpn enable
   ```

   # Configure VSI **aaa** that uses LDP as the PW signaling protocol, and establish PWs to PE 2 and PE 3.

   ```
   [PE1] vsi aaa
   [PE1-vsi-aaa] pwsignaling ldp
   [PE1-vsi-aaa-ldp] peer 3.3.3.9 pw-id 500
   [PE1-vsi-aaa-ldp-3.3.3.9-500] quit
   ```

```
[PE1-vsi-aaa-ldp] peer 2.2.2.9 pw-id 500
[PE1-vsi-aaa-ldp-2.2.2.9-500] quit
[PE1-vsi-aaa-ldp] quit
[PE1-vsi-aaa] quit
```

Create Ethernet service instance 1000 on Ten-GigabitEthernet 1/0/1 (the interface connected to CE 1), and bind the Ethernet service instance to the VSI **aaa**.

```
[PE1] interface ten-gigabitethernet 1/0/1
[PE1-Ten-GigabitEthernet1/0/1] service-instance 1000
[PE1-Ten-GigabitEthernet1/0/1-srv1000] encapsulation s-vid 100
[PE1-Ten-GigabitEthernet1/0/1-srv1000] xconnect vsi aaa
[PE1-Ten-GigabitEthernet1/0/1-srv1000] quit
[PE1-Ten-GigabitEthernet1/0/1] quit
```

3. Configure PE 2:

Configure basic MPLS.

```
<PE2> system-view
[PE2] interface loopback 0
[PE2-LoopBack0] ip address 2.2.2.9 32
[PE2-LoopBack0] quit
[PE2] mpls lsr-id 2.2.2.9
[PE2] mpls ldp
[PE2-ldp] quit
```

Enable L2VPN.

```
[PE2] l2vpn enable
```

Configure VSI **aaa** that uses LDP as the PW signaling protocol, and establish PWs to PE 1 and PE 3.

```
[PE2] vsi aaa
[PE2-vsi-aaa] pwsignal ldp
[PE2-vsi-aaa-ldp] peer 1.1.1.9 pw-id 500
[PE2-vsi-aaa-ldp-1.1.1.9-500] quit
[PE2-vsi-aaa-ldp] peer 3.3.3.9 pw-id 500
[PE2-vsi-aaa-ldp-3.3.3.9-500] quit
[PE2-vsi-aaa-ldp] quit
[PE2-vsi-aaa] quit
```

Create Ethernet service instance 1000 on Ten-GigabitEthernet 1/0/1 (the interface connected to CE 2), and bind the Ethernet service instance to the VSI **aaa**.

```
[PE2] interface ten-gigabitethernet 1/0/1
[PE2-Ten-GigabitEthernet1/0/1] service-instance 1000
[PE2-Ten-GigabitEthernet1/0/1-srv1000] encapsulation s-vid 100
[PE2-Ten-GigabitEthernet1/0/1-srv1000] xconnect vsi aaa
[PE2-Ten-GigabitEthernet1/0/1-srv1000] quit
[PE2-Ten-GigabitEthernet1/0/1] quit
```

4. Configure PE 3:

Configure basic MPLS.

```
<PE3> system-view
[PE3] interface loopback 0
[PE3-LoopBack0] ip address 3.3.3.9 32
[PE3-LoopBack0] quit
[PE3] mpls lsr-id 3.3.3.9
```

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

Enable L2VPN.

```
[PE3] l2vpn enable
```

Configure VSI **aaa** that uses LDP as the PW signaling protocol, and establish PWs to PE 1 and PE 2.

```
[PE3] vsi aaa
[PE3-vsi-aaa] pwsignal ldp
[PE3-vsi-aaa-ldp] peer 1.1.1.9 pw-id 500
[PE3-vsi-aaa-ldp-1.1.1.9-500] quit
[PE3-vsi-aaa-ldp] peer 2.2.2.9 pw-id 500
[PE3-vsi-aaa-ldp-2.2.2.9-500] quit
[PE3-vsi-aaa-ldp] quit
[PE3-vsi-aaa] quit
```

Create Ethernet service instance 1000 on Ten-GigabitEthernet 1/0/1 (the interface connected to CE 3), and bind the Ethernet service instance to the VSI **aaa**.

```
[PE3] interface ten-gigabitethernet 1/0/1
[PE3-Ten-GigabitEthernet1/0/1] service-instance 1000
[PE3-Ten-GigabitEthernet1/0/1-srv1000] encapsulation s-vid 100
[PE3-Ten-GigabitEthernet1/0/1-srv1000] xconnect vsi aaa
[PE3-Ten-GigabitEthernet1/0/1-srv1000] quit
[PE3-Ten-GigabitEthernet1/0/1] quit
```

Verifying the configuration

Verify that PWs in up state have been established on each PE.

```
[PE1] display l2vpn pw verbose
VSI Name: aaa
  Peer: 3.3.3.9          PW ID: 500
    Signaling Protocol  : LDP
    Link ID             : 8          PW State : Up
    In Label            : 1275       Out Label: 1272
    MTU                 : 1500
    PW Attributes       : Main
    VCCV CC             : -
    VCCV BFD            : -
    Tunnel Group ID     : 0x660000000
    Tunnel NHLFE IDs    : 1032
  Peer: 2.2.2.9          PW ID: 500
    Signaling Protocol  : LDP
    Link ID             : 9          PW State : Up
    In Label            : 1274       Out Label: 1274
    MTU                 : 1500
    PW Attributes       : Main
    VCCV CC             : -
    VCCV BFD            : -
    Tunnel Group ID     : 0x760000001
    Tunnel NHLFE IDs    : 1033
[PE2] display l2vpn pw verbose
VSI Name: aaa
```

```
  Peer: 1.1.1.9          PW ID: 500
    Signaling Protocol  : LDP
    Link ID             : 8          PW State : Up
    In Label            : 1274       Out Label: 1274
    MTU                 : 1500
    PW Attributes       : Main
    VCCV CC             : -
    VCCV BFD            : -
    Tunnel Group ID     : 0x760000000
    Tunnel NHLFE IDs    : 1033
  Peer: 3.3.3.9          PW ID: 500
    Signaling Protocol  : LDP
    Link ID             : 9          PW State : Up
    In Label            : 1273       Out Label: 1271
    MTU                 : 1500
    PW Attributes       : Main
    VCCV CC             : -
    VCCV BFD            : -
    Tunnel Group ID     : 0x860000001
    Tunnel NHLFE IDs    : 1034
[PE3] display l2vpn pw verbose
VSI Name: aaa
  Peer: 1.1.1.9          PW ID: 500
    Signaling Protocol  : LDP
    Link ID             : 8          PW State : Up
    In Label            : 1272       Out Label: 1275
    MTU                 : 1500
    PW Attributes       : Main
    VCCV CC             : -
    VCCV BFD            : -
    Tunnel Group ID     : 0x960000000
    Tunnel NHLFE IDs    : 1034
  Peer: 2.2.2.9          PW ID: 500
    Signaling Protocol  : LDP
    Link ID             : 9          PW State : Up
    In Label            : 1271       Out Label: 1273
    MTU                 : 1500
    PW Attributes       : Main
    VCCV CC             : -
    VCCV BFD            : -
    Tunnel Group ID     : 0xa60000001
    Tunnel NHLFE IDs    : 1035
```

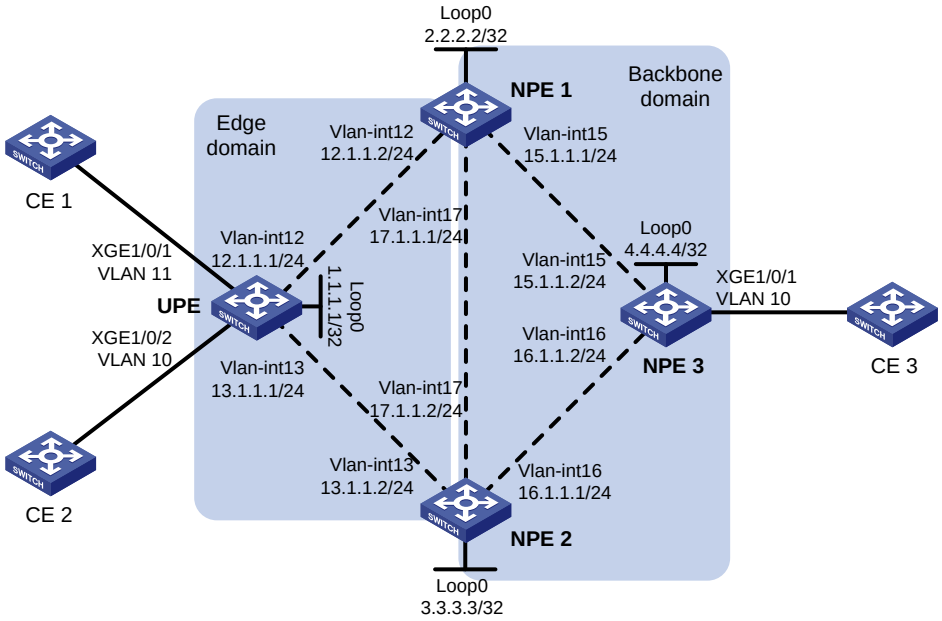
H-VPLS UPE dual homing configuration example

Network requirements

To improve reliability of the H-VPLS network, the UPE establishes a U-PW with NPE 1 and NPE 2. The U-PW between UPE and NPE 1 is the primary PW and that between UPE and NPE 2 is the backup PW. The backup PW works only when the primary PW fails.

The H-VPLS uses LDP as the PW signaling protocol.

Figure 12 Network diagram



Configuration procedure

Before configuration, disable the spanning tree feature globally or map each VLAN to an MSTI. For more information, see *Layer 2—LAN Switching Configuration Guide*.

1. Configure an IGP and public tunnels on each PE. (Details not shown.)
2. Configure UPE:

   # Configure basic MPLS.

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

   # Enable L2VPN.

   ```
   [UPE] l2vpn enable
   ```

   # Configure VSI **aaa** that uses LDP as the PW signaling protocol, and establish the primary PW to NPE 1 and the backup PW to NPE 2.

   ```
   [UPE] vsi aaa
   [UPE-vsi-aaa] pwsignaling ldp
   [UPE-vsi-aaa-ldp] peer 2.2.2.2 pw-id 500
   [UPE-vsi-aaa-ldp-2.2.2.2-500] backup-peer 3.3.3.3 pw-id 500
   ```

```
[UPE-vsi-aaa-ldp-3.3.3.3-500-backup] quit
[UPE-vsi-aaa-ldp-2.2.2.2-500] quit
[UPE-vsi-aaa-ldp] quit
[UPE-vsi-aaa] quit
```

Create Ethernet service instance 1000 on Ten-GigabitEthernet 1/0/1 (the interface connected to CE 1), and bind the Ethernet service instance to the VSI **aaa**.

```
[UPE] interface ten-gigabitethernet 1/0/1
[UPE-Ten-GigabitEthernet1/0/1] service-instance 1000
[UPE-Ten-GigabitEthernet1/0/1-srv1000] encapsulation s-vid 10
[UPE-Ten-GigabitEthernet1/0/1-srv1000] xconnect vsi aaa
[UPE-Ten-GigabitEthernet1/0/1-srv1000] quit
```

Create Ethernet service instance 1000 on Ten-GigabitEthernet 1/0/2 (the interface connected to CE 2), and bind the Ethernet service instance to the VSI **aaa**.

```
[UPE] interface ten-gigabitethernet 1/0/2
[UPE-Ten-GigabitEthernet1/0/2] service-instance 1000
[UPE-Ten-GigabitEthernet1/0/2-srv1000] encapsulation s-vid 11
[UPE-Ten-GigabitEthernet1/0/2-srv1000] xconnect vsi aaa
[UPE-Ten-GigabitEthernet1/0/2-srv1000] quit
```

3. Configure NPE 1:

Configure basic MPLS.

```
<NPE1> system-view
[NPE1] interface loopback 0
[NPE1-LoopBack0] ip address 2.2.2.2 32
[NPE1-LoopBack0] quit
[NPE1] mpls lsr-id 2.2.2.2
[NPE1] mpls ldp
[NPE1–ldp] quit
```

Enable L2VPN.

```
[NPE1] l2vpn enable
```

Configure VSI **aaa** that uses LDP as the PW signaling protocol, and establish PWs to UPE, NPE 2, and NPE 3.

```
[NPE1] vsi aaa
[NPE1-vsi-aaa] pwsignaling ldp
[NPE1-vsi-aaa-ldp] peer 1.1.1.1 pw-id 500 no-split-horizon
[NPE1-vsi-aaa-ldp-1.1.1.1-500] quit
[NPE1-vsi-aaa-ldp] peer 3.3.3.3 pw-id 500
[NPE1-vsi-aaa-ldp-3.3.3.3-500] quit
[NPE1-vsi-aaa-ldp] peer 4.4.4.4 pw-id 500
[NPE1-vsi-aaa-ldp-4.4.4.4-500] quit
[NPE1-vsi-aaa-ldp] quit
[NPE1-vsi-aaa] quit
```

4. Configure NPE 2:

Configure basic MPLS.

```
<NPE2> system-view
[NPE2] interface loopback 0
[NPE2-LoopBack0] ip address 3.3.3.3 32
[NPE2-LoopBack0] quit
[NPE2] mpls lsr-id 3.3.3.3
```

```
[NPE2] mpls ldp
[NPE2–ldp] quit
```

Enable L2VPN.

```
[NPE2] l2vpn enable
```

Configure VSI **aaa** that uses LDP as the PW signaling protocol, and establish PWs to UPE, NPE 2, and NPE 3.

```
[NPE2] vsi aaa
[NPE2-vsi-aaa] pwsignaling ldp
[NPE2-vsi-aaa-ldp] peer 1.1.1.1 pw-id 500 no-split-horizon
[NPE2-vsi-aaa-ldp-1.1.1.1-500] quit
[NPE2-vsi-aaa-ldp] peer 2.2.2.2 pw-id 500
[NPE2-vsi-aaa-ldp-2.2.2.2-500] quit
[NPE2-vsi-aaa-ldp] peer 4.4.4.4 pw-id 500
[NPE2-vsi-aaa-ldp-4.4.4.4-500] quit
[NPE2-vsi-aaa-ldp] quit
[NPE2-vsi-aaa] quit
```

5. Configure NPE 3:

Configure basic MPLS.

```
<NPE3> system-view
[NPE3] interface loopback 0
[NPE3-LoopBack0] ip address 4.4.4.4 32
[NPE3-LoopBack0] quit
[NPE3] mpls lsr-id 4.4.4.4
[NPE3] mpls ldp
[NPE3–ldp] quit
```

Enable L2VPN.

```
[NPE3] l2vpn enable
```

Configure VSI **aaa** that uses LDP as the PW signaling protocol, and establish PWs to NPE 1 and NPE 2.

```
[NPE3] vsi aaa
[NPE3-vsi-aaa] pwsignaling ldp
[NPE3-vsi-aaa-ldp] peer 2.2.2.2 pw-id 500
[NPE3-vsi-aaa-ldp-2.2.2.2-500] quit
[NPE3-vsi-aaa-ldp] peer 3.3.3.3 pw-id 500
[NPE3-vsi-aaa-ldp-3.3.3.3-500] quit
[NPE3-vsi-aaa-ldp] quit
[NPE3-vsi-aaa] quit
```

Create Ethernet service instance 1000 on Ten-GigabitEthernet 1/0/1 (the interface connected to CE 3), and bind the Ethernet service instance to the VSI **aaa**.

```
[NPE3] interface ten-gigabitethernet 1/0/1
[NPE3-Ten-GigabitEthernet1/0/1] service-instance 1000
[NPE3-Ten-GigabitEthernet1/0/1-srv1000] encapsulation s-vid 10
[NPE3-Ten-GigabitEthernet1/0/1-srv1000] xconnect vsi aaa
[NPE3-Ten-GigabitEthernet1/0/1-srv1000] quit
```

Verifying the configuration

Verify that PWs in up state have been established on each PE.

```
[UPE] display l2vpn pw verbose
VSI Name: aaa
```

```
  Peer: 2.2.2.2          PW ID: 500
    Signaling Protocol  : LDP
    Link ID             : 8          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    : 1027
  Peer: 3.3.3.3          PW ID: 500
    Signaling Protocol  : LDP
    Link ID             : 8          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    : 1025
[NPE1] display l2vpn pw verbose
VSI Name: aaa
  Peer: 1.1.1.1          PW ID: 500
    Signaling Protocol  : LDP
    Link ID             : 8          PW State : Up
    In Label            : 1279       Out Label: 1151
    MTU                 : 1500
    PW Attributes       : Main, No-split-horizon
    VCCV CC             : -
    VCCV BFD            : -
    Tunnel Group ID     : 0x60000000
    Tunnel NHLFE IDs    : 1026
  Peer: 3.3.3.3          PW ID: 500
    Signaling Protocol  : LDP
    Link ID             : 9          PW State : Up
    In Label            : 1280       Out Label: 1290
    MTU                 : 1500
    PW Attributes       : Main
    VCCV CC             : -
    VCCV BFD            : -
    Tunnel Group ID     : 0x160000005
    Tunnel NHLFE IDs    : 1027
  Peer: 4.4.4.4          PW ID: 500
    Signaling Protocol  : LDP
    Link ID             : 10         PW State : Up
    In Label            : 1278       Out Label: 1279
    MTU                 : 1500
```

```
    PW Attributes       : Main
    VCCV CC             : -
    VCCV BFD            : -
    Tunnel Group ID     : 0x160000001
    Tunnel NHLFE IDs    : 1028
[NPE2] display l2vpn pw verbose
VSI Name: aaa
  Peer: 1.1.1.1          PW ID: 500
    Signaling Protocol  : LDP
    Link ID             : 8          PW State : Up
    In Label            : 1279       Out Label: 1150
    MTU                 : 1500
    PW Attributes       : Main, No-split-horizon
    VCCV CC             : -
    VCCV BFD            : -
    Tunnel Group ID     : 0x60000000
    Tunnel NHLFE IDs    : 1026
  Peer: 2.2.2.2          PW ID: 500
    Signaling Protocol  : LDP
    Link ID             : 9          PW State : Up
    In Label            : 1290       Out Label: 1280
    MTU                 : 1500
    PW Attributes       : Main
    VCCV CC             : -
    VCCV BFD            : -
    Tunnel Group ID     : 0x160000008
    Tunnel NHLFE IDs    : 1027
  Peer: 4.4.4.4          PW ID: 500
    Signaling Protocol  : LDP
    Link ID             : 10         PW State : Up
    In Label            : 1278       Out Label: 1278
    MTU                 : 1500
    PW Attributes       : Main
    VCCV CC             : -
    VCCV BFD            : -
    Tunnel Group ID     : 0x160000001
    Tunnel NHLFE IDs    : 1028
[NPE3] display l2vpn pw verbose
VSI Name: aaa
  Peer: 2.2.2.2          PW ID: 500
    Signaling Protocol  : LDP
    Link ID             : 8          PW State : Up
    In Label            : 1279       Out Label: 1278
    MTU                 : 1500
    PW Attributes       : Main
    VCCV CC             : -
    VCCV BFD            : -
    Tunnel Group ID     : 0x60000000
```

```
  Tunnel NHLFE IDs    : 1026
Peer: 3.3.3.3          PW ID: 500
  Signaling Protocol  : LDP
  Link ID             : 9          PW State : Up
  In Label            : 1278       Out Label: 1278
  MTU                 : 1500
  PW Attributes       : Main
  VCCV CC             : -
  VCCV BFD            : -
  Tunnel Group ID     : 0x160000001
  Tunnel NHLFE IDs    : 1027
```