Contents

Configuring L2PT

About L2PT

Layer 2 Protocol Tunneling (L2PT) can transparently send Layer 2 protocol packets from geographically dispersed customer networks across a service provider network or drop them.

L2PT application scenario

Dedicated lines are used in a service provider network to build user-specific Layer 2 networks. As a result, a customer network contains sites located at different sides of the service provider network.

As shown in Figure 1, Customer A's network is divided into network 1 and network 2, which are connected by the service provider network. For Customer A's network to implement Layer 2 protocol calculations, the Layer 2 protocol packets must be transmitted across the service provider network.

Upon receiving a Layer 2 protocol packet, the PEs cannot determine whether the packet is from the customer network or the service provider network. They must deliver the packet to the CPU for processing. In this case, the Layer 2 protocol calculation in Customer A's network is mixed with the Layer 2 protocol calculation in the service provider network. Neither the customer network nor the service provider network can implement independent Layer 2 protocol calculations.

Figure 1 L2PT application scenario
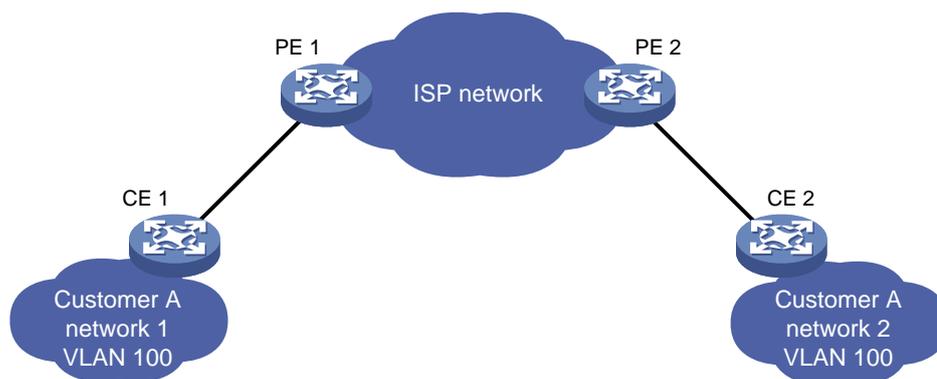
L2PT is introduced to resolve the problem. L2PT provides the following functions:

- Multicasts Layer 2 protocol packets from a customer network in a VLAN. Dispersed customer networks can complete an independent Layer 2 protocol calculation, which is transparent to the service provider network.
- Isolates Layer 2 protocol packets from different customer networks through different VLANs.

Supported protocols

H3C devices support L2PT for the following protocols:

- CDP.
- DLDP.
- EOAM.
- GVRP.
- LACP.

- LLDP.
- MVRP.
- PAgP.
- PVST.
- STP (including STP, RSTP, and MSTP).
- UDLD.
- VTP.

L2PT operating mechanism

As shown in Figure 2, L2PT operates as follows:

- When a port of PE 1 receives a Layer 2 protocol packet from the customer network in a VLAN, it performs the following operations:
  - Multicasts the packet out of all customer-facing ports in the VLAN except the receiving port.
  - Encapsulates the packet with a specified destination multicast address, and multicasts it out of all ISP-facing ports in the VLAN. The encapsulated packet is called the BPDU tunneled packet.
- When a port of PE 2 in the VLAN receives the tunneled packet from the service provider network, it performs the following operations:
  - Multicasts the packet out of all ISP-facing ports in the VLAN except the receiving port.
  - Decapsulates the packet and multicasts the decapsulated packet out of all customer-facing ports in the VLAN.

Figure 2 L2PT operating mechanism
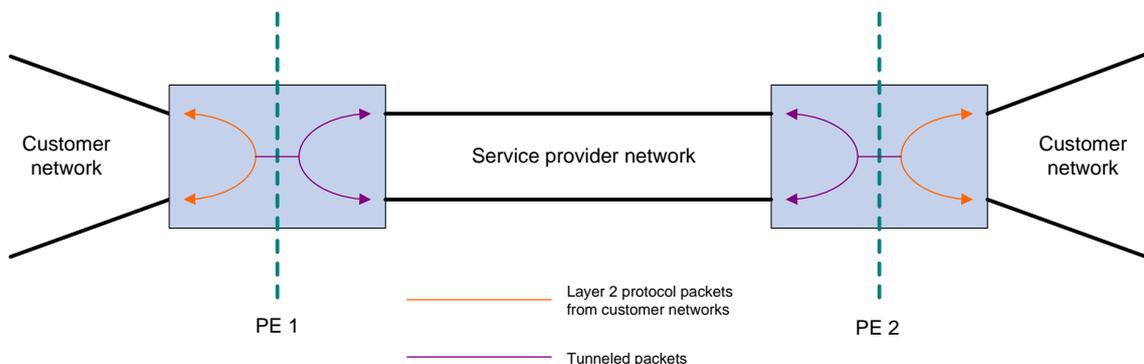
For example, as shown in Figure 3, PE 1 receives an STP packet (BPDU) from network 1 to network 2. CEs are the edge devices on the customer network, and PEs are the edge devices on the service provider network. L2PT processes the packet as follows:

1. PE 1 performs the following operations:
   a. Encapsulates the packet with a specified destination multicast MAC address (010f-e200-0003 by default).
   b. Sends the tunneled packet out of all ISP-facing ports in the packet's VLAN.
2. Upon receiving the tunneled packet, PE 2 decapsulates the packet and sends the BPDU to CE 2.

Through L2PT, both the ISP network and Customer A's network can perform independent spanning tree calculations.

Figure 3 L2PT network diagram
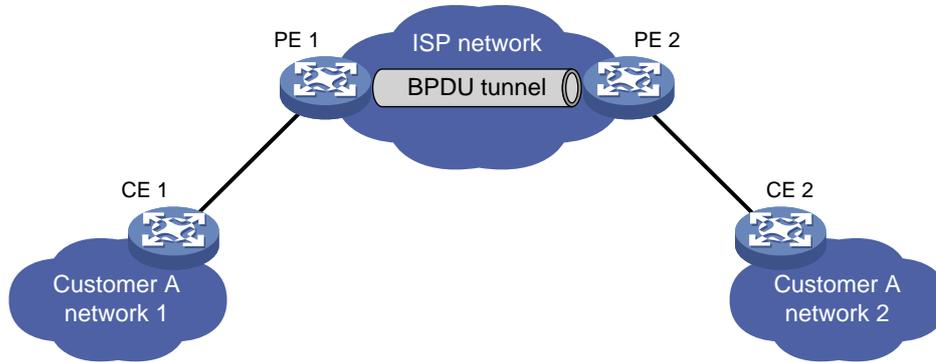
L2PT tasks at a glance

To configure L2PT, perform the following tasks:

1. Enabling L2PT or L2PT drop
   o Enabling L2PT

   This feature is applicable only to customer-facing ports.

2. (Optional.) Setting the destination multicast MAC address for tunneled packets

Enabling L2PT

Restrictions and guidelines for L2PT

- To enable L2PT for a Layer 2 protocol on a port, perform the following tasks:
  o Enable the protocol on the connected CE, and disable the protocol on the port.
  o Disable the protocol (for example, STP) on the PE ports connecting to an aggregate interface on a CE when the following conditions exist:
    − The protocol is running on the aggregate interface on the CE.
    − The aggregate interface on the CE connects to an L2PT-enabled port on the PE.
  o Enable L2PT on PE ports connected to a customer network. If you enable L2PT on ports connected to the service provider network, L2PT determines that the ports are connected to a customer network.
  o Make sure the VLAN tags of Layer 2 protocol packets are not changed or deleted for the tunneled packets to be transmitted correctly across the service provider network.
- L2PT for LLDP supports LLDP packets from only nearest bridge agents.
- You can enable L2PT on a member port of a Layer 2 aggregation group, but the configuration does not take effect.
- Do not enable L2PT on a port that is going to join a service loopback group.

Enabling L2PT for a protocol in Layer 2 Ethernet interface view

Restrictions and guidelines

LACP and EOAM require point-to-point transmission. If you enable L2PT on a Layer 2 Ethernet interface for LACP or EOAM, L2PT multicasts LACP or EOAM packets out of customer-facing ports. As a result, the transmission between two CEs is not point-to-point. To ensure point-to-point transmission for the LACP or EOAM packets, you must configure other features (for example, VLAN).

Procedure

1. Enter system view.

   system-view

2. Enter Layer 2 Ethernet interface view.

   interface *interface-type interface-number*

3. Enable L2PT for a protocol.

   l2protocol { **cdp** | **dldp** | **eoam** | **gvrp** | **lacp** | **lldp** | **mvrp** | **pagp** | **pvst** | **stp** | **udld** | **vtp** } **tunnel dot1q**

   By default, L2PT is disabled for all protocols.

Enabling L2PT for a protocol in Layer 2 aggregate interface view

1. Enter system view.

   system-view

2. Enter Layer 2 aggregate interface view.

   interface bridge-aggregation *interface-type interface-number*

3. Enable L2PT for a protocol.

   l2protocol { **gvrp** | **mvrp** | **pvst** | **stp** | **vtp** } **tunnel dot1q**

   By default, L2PT is disabled for all protocols.

Setting the destination multicast MAC address for tunneled packets

About the destination multicast MAC address for tunneled packets

The available multicast MAC addresses are 010f-e200-0003, 0100-0ccd-cdd0, 0100-0ccd-cdd1, and 0100-0ccd-cdd2.

Restrictions and guidelines

For tunneled packets to be recognized, set the same destination multicast MAC addresses on PEs that are connected to the same customer network.

As a best practice, set different destination multicast MAC addresses on PEs connected to different customer networks. It prevents L2PT from sending packets of a customer network to another customer network.

Procedure

1. Enter system view.

   system-view

2. Set the destination multicast MAC address for tunneled packets.

   l2protocol tunnel-dmac *mac-address*

   By default, 010f-e200-0003 is used for tunneled packets.

Display and maintenance commands for L2PT

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

Task	Command
Display L2PT statistics.	**display l2protocol statistics** [**interface** *interface-type interface-number*]
Clear L2PT statistics.	**reset l2protocol statistics** [**interface** *interface-type interface-number*]

# L2PT configuration examples

Example: Configuring L2PT for STP

Network configuration

As shown in Figure 4, the MAC addresses of CE 1 and CE 2 are 00e0-fc02-5800 and 00e0-fc02-5802, respectively. MSTP is enabled in Customer A's network, and default MSTP settings are used.

Perform the following tasks on the PEs:

- Configure the ports that connect to CEs as access ports, and configure the ports in the service provider network as trunk ports. Configure ports in the service provider network to allow packets from any VLAN to pass.
- Enable L2PT for STP to enable Customer A's network to implement independent spanning tree calculation across the service provider network.
- Set the destination multicast MAC address to 0100-0ccd-cdd0 for tunneled packets.

Figure 4 Network diagram
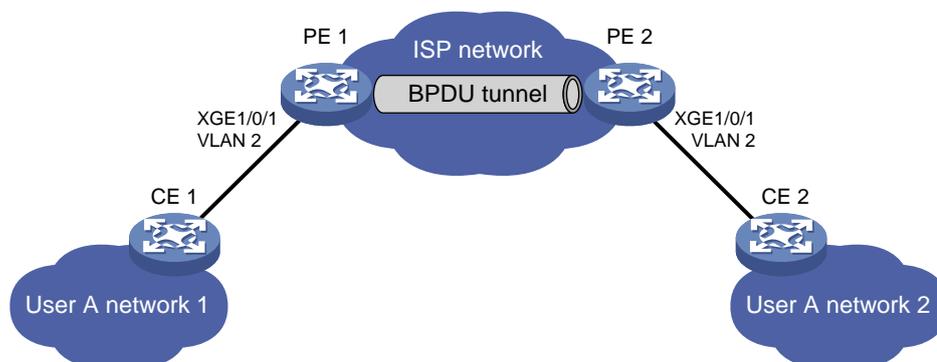
Procedure

1. Configure PE 1:

   # Set the destination multicast address to 0100-0ccd-cdd0 for tunneled packets.
   ```
   <PE1> system-view
   [PE1] l2protocol tunnel-dmac 0100-0ccd-cdd0
   ```
   # Create VLAN 2.
   ```
   [PE1] vlan 2
   [PE1-vlan2] quit
   ```
   # Configure Ten-GigabitEthernet 1/0/1 as an access port and assign the port to VLAN 2.
   ```
   [PE1] interface ten-gigabitethernet 1/0/1
   [PE1-Ten-GigabitEthernet1/0/1] port access vlan 2
   ```
   # Disable STP and enable L2PT for STP on Ten-GigabitEthernet 1/0/1.
   ```
   [PE1-Ten-GigabitEthernet1/0/1] undo stp enable
   [PE1-Ten-GigabitEthernet1/0/1] l2protocol stp tunnel dot1q
   [PE1-Ten-GigabitEthernet1/0/1] quit
   ```
   # Configure Ten-GigabitEthernet 1/0/2 connected to the service provider network as a trunk port, and assign the port to all VLANs.
   ```
   [PE1] interface ten-gigabitethernet 1/0/2
   [PE1-Ten-GigabitEthernet1/0/2] port link-type trunk
   [PE1-Ten-GigabitEthernet1/0/2] port trunk permit vlan all
   [PE1-Ten-GigabitEthernet1/0/2] quit
   ```
2. Configure PE 2 in the same way PE 1 is configured. (Details not shown.)

Verifying the configuration

Verify that the root bridge of Customer A's network is CE 1.
```
<CE2> display stp root
 MST ID   Root Bridge ID      ExtPathCost IntPathCost Root Port
 0        32768.00e0-fc02-5800 0           0
```
Verify that the root bridge of the service provider network is not CE 1.
```
[PE1] display stp root
 MST ID   Root Bridge ID      ExtPathCost IntPathCost Root Port
 0        32768.0cda-41c5-ba50 0           0
```

Example: Configuring L2PT for LACP

Network configuration

As shown in Figure 5, the MAC addresses of CE 1 and CE 2 are 0001-0000-0000 and 0004-0000-0000, respectively.

Perform the following tasks:

- Configure Ethernet link aggregation on CE 1 and CE 2.
- Configure Ten-GigabitEthernet 1/0/1 and Ten-GigabitEthernet 1/0/2 on CE 1 to form aggregate links with Ten-GigabitEthernet 1/0/1 and Ten-GigabitEthernet 1/0/2 on CE 2, respectively.
- Enable L2PT for LACP to enable CE 1 and CE 2 to implement Ethernet link aggregation across the service provider network.

Figure 5 Network diagram
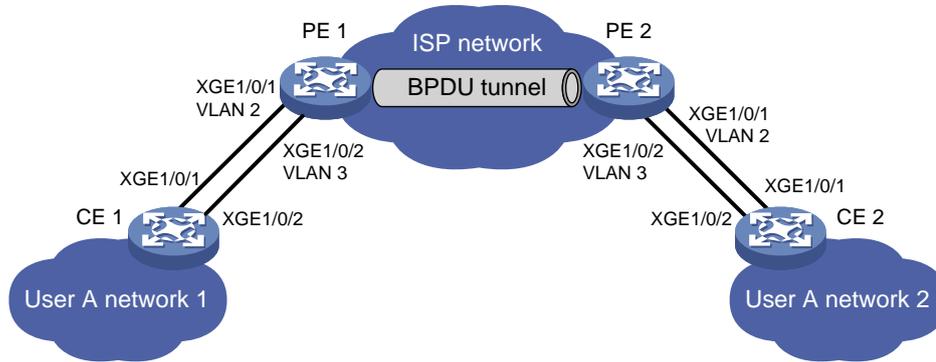
Requirements analysis

To meet the network requirements, perform the following tasks:

- For Ethernet link aggregation to operate correctly, configure VLANs on the PEs to ensure point-to-point transmission between CE 1 and CE 2 in an aggregation group.
  - Set the PVIDs to VLAN 2 and VLAN 3 for Ten-GigabitEthernet 1/0/1 and Ten-GigabitEthernet 1/0/2 on PE 1, respectively.
  - Configure PE 2 in the same way PE 1 is configured.
  - Configure ports that connect to the CEs as trunk ports.
- To retain the VLAN tag of the customer network, enable QinQ on Ten-GigabitEthernet 1/0/1 and Ten-GigabitEthernet 1/0/2 on both PE 1 and PE 2.
- For packets from any VLAN to be transmitted, configure all ports in the service provider network as trunk ports.

Procedure

1. Configure CE 1:

   # Configure Layer 2 aggregation group Bridge-Aggregation 1 to operate in dynamic aggregation mode.

   ```
   <CE1> system-view
   [CE1] interface bridge-aggregation 1
   [CE1-Bridge-Aggregation1] port link-type access
   [CE1-Bridge-Aggregation1] link-aggregation mode dynamic
   [CE1-Bridge-Aggregation1] quit
   ```

   # Assign Ten-GigabitEthernet 1/0/1 and Ten-GigabitEthernet 1/0/2 to Bridge-Aggregation 1.

   ```
   [CE1] interface ten-gigabitethernet 1/0/1
   [CE1-Ten-GigabitEthernet1/0/1] port link-aggregation group 1
   [CE1-Ten-GigabitEthernet1/0/1] quit
   [CE1] interface ten-gigabitethernet 1/0/2
   [CE1-Ten-GigabitEthernet1/0/2] port link-aggregation group 1
   [CE1-Ten-GigabitEthernet1/0/2] quit
   ```

2. Configure CE 2 in the same way CE 1 is configured. (Details not shown.)

3. Configure PE 1:

   # Create VLANs 2 and 3.

   ```
   <PE1> system-view
   [PE1] vlan 2
   [PE1-vlan2] quit
   [PE1] vlan 3
   ```

```
[PE1-vlan3] quit
```
Configure Ten-GigabitEthernet 1/0/1 as a trunk port, assign the port to VLAN 2, and set the PVID to VLAN 2.
```
[PE1] interface ten-gigabitethernet 1/0/1
[PE1-Ten-GigabitEthernet1/0/1] port link-mode bridge
[PE1-Ten-GigabitEthernet1/0/1] port link-type trunk
[PE1-Ten-GigabitEthernet1/0/1] port trunk permit vlan 2
[PE1-Ten-GigabitEthernet1/0/1] port trunk pvid vlan 2
```
Enable QinQ on Ten-GigabitEthernet 1/0/1.
```
[PE1-Ten-GigabitEthernet1/0/1] qinq enable
```
Enable L2PT for LACP on Ten-GigabitEthernet 1/0/1.
```
[PE1-Ten-GigabitEthernet1/0/1] l2protocol lacp tunnel dot1q
[PE1-Ten-GigabitEthernet1/0/1] quit
```
Configure Ten-GigabitEthernet 1/0/2 as a trunk port, assign the port to VLAN 3, and set the PVID to VLAN 3.
```
[PE1] interface ten-gigabitethernet 1/0/2
[PE1-Ten-GigabitEthernet1/0/2] port link-mode bridge
[PE1-Ten-GigabitEthernet1/0/2] port link-type trunk
[PE1-Ten-GigabitEthernet1/0/2] port trunk permit vlan 3
[PE1-Ten-GigabitEthernet1/0/2] port trunk pvid vlan 3
```
Enable QinQ on Ten-GigabitEthernet 1/0/2.
```
[PE1-Ten-GigabitEthernet1/0/2] qinq enable
```
Enable L2PT for LACP on Ten-GigabitEthernet 1/0/2.
```
[PE1-Ten-GigabitEthernet1/0/2] l2protocol lacp tunnel dot1q
[PE1-Ten-GigabitEthernet1/0/2] quit
```
4. Configure PE 2 in the same way PE 1 is configured. (Details not shown.)

Verifying the configuration

Verify that CE 1 and CE 2 have completed Ethernet link aggregation successfully.
```
[CE1] display link-aggregation member-port
Flags: A -- LACP_Activity, B -- LACP_Timeout, C -- Aggregation,
       D -- Synchronization, E -- Collecting, F -- Distributing,
       G -- Defaulted, H -- Expired

Ten-GigabitEthernet1/0/1:
Aggregate Interface: Bridge-Aggregation1
Local:
    Port Number: 3
    Port Priority: 32768
    Oper-Key: 1
    Flag: {ACDEF}
Remote:
    System ID: 0x8000, 0004-0000-0000
    Port Number: 3
    Port Priority: 32768
    Oper-Key: 1
    Flag: {ACDEF}
Received LACP Packets: 23 packet(s)
```

8

```
Illegal: 0 packet(s)
Sent LACP Packets: 26 packet(s)


Ten-GigabitEthernet1/0/2:
Aggregate Interface: Bridge-Aggregation1
Local:
    Port Number: 4
    Port Priority: 32768
    Oper-Key: 1
    Flag: {ACDEF}
Remote:
    System ID: 0x8000, 0004-0000-0000
    Port Number: 4
    Port Priority: 32768
    Oper-Key: 1
    Flag: {ACDEF}
Received LACP Packets: 10 packet(s)
Illegal: 0 packet(s)
Sent LACP Packets: 13 packet(s)
[CE2] display link-aggregation member-port
Flags: A -- LACP_Activity, B -- LACP_Timeout, C -- Aggregation,
      D -- Synchronization, E -- Collecting, F -- Distributing,
      G -- Defaulted, H -- Expired


Ten-GigabitEthernet1/0/1:
Aggregate Interface: Bridge-Aggregation1
Local:
    Port Number: 3
    Port Priority: 32768
    Oper-Key: 1
    Flag: {ACDEF}
Remote:
    System ID: 0x8000, 0001-0000-0000
    Port Number: 3
    Port Priority: 32768
    Oper-Key: 1
    Flag: {ACDEF}
Received LACP Packets: 23 packet(s)
Illegal: 0 packet(s)
Sent LACP Packets: 26 packet(s)


Ten-GigabitEthernet1/0/2:
Aggregate Interface: Bridge-Aggregation1
Local:
    Port Number: 4
    Port Priority: 32768
    Oper-Key: 1
    Flag: {ACDEF}
```

```
Remote:
    System ID: 0x8000, 0001-0000-0000
    Port Number: 4
    Port Priority: 32768
    Oper-Key: 1
    Flag: {ACDEF}
Received LACP Packets: 10 packet(s)
Illegal: 0 packet(s)
Sent LACP Packets: 13 packet(s)
```