

1 MPLS Basics

This chapter describes MPLS basics.

[1.1 Overview of MPLS](#)

[1.2 Understanding MPLS](#)

[1.3 Application Scenarios for MPLS](#)

[1.4 MPLS Common Configuration](#)

1.1 Overview of MPLS

Definition

The Multiprotocol Label Switching (MPLS) protocol is used on Internet Protocol (IP) backbone networks. MPLS uses connection-oriented label switching on connectionless IP networks. By combining Layer 3 routing technologies and Layer 2 switching technologies, MPLS leverages the flexibility of IP routing and the simplicity of Layer 2 switching.

MPLS is based on Internet Protocol version 4 (IPv4). The core MPLS technology can be extended to multiple network protocols, such as Internet Protocol version 6 (IPv6), Internet Packet Exchange (IPX), and Connectionless Network Protocol (CLNP). "Multiprotocol" in MPLS means that multiple network protocols are supported.

MPLS is used for tunneling but not a service or an application. MPLS supports multiple protocols and services. Moreover, it ensures security of data transmission.

Purpose

IP-based routing serves well on the Internet in the mid 90s, but IP technology can be inefficient at forwarding packets because software must search for routes using the longest match algorithm. As a result, the forwarding capability of IP technology can act as a bottleneck.

In contrast, Asynchronous transfer mode (ATM) technology uses labels of fixed length and maintains a label table that is much smaller than a routing table.

Compared to IP, ATM is more efficient at forwarding packets. ATM is a complex protocol, however, with high deployment costs, that hinder its widespread use.

Because traditional IP technology is simple and costs little to deploy, a combination of IP and ATM capabilities would be ideal. This has sparked the emergence of MPLS technology.

MPLS was created to increase forwarding rates. Unlike IP routing and forwarding, MPLS analyzes a packet header only on the edge of the network and not at each hop. MPLS therefore reduces packet processing time.

The use of hardware-based functions based on application-specific integrated circuits (ASICs) has made IP routing far more efficient, so MPLS is no longer needed for its high-speed forwarding advantages. However, MPLS does not support multi-layer labels, and its forwarding plane is connection-oriented. For these reasons, MPLS is widely used for virtual private network (VPN), and quality of service (QoS).

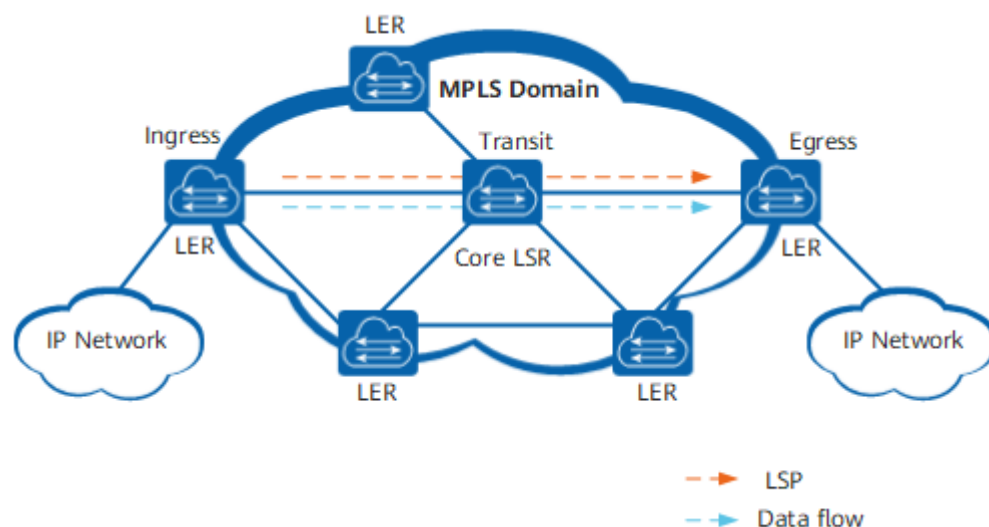
1.2 Understanding MPLS

1.2.1 Basic MPLS Architecture

MPLS Network Structure

Figure 1-1 shows a typical MPLS network structure. Packets are forwarded on an MPLS network based on labels. In **Figure 1-1**, network devices that swap MPLS labels and forward packets are label switching routers (LSRs), which form an MPLS domain. LSRs that reside at the edge of the MPLS domain and connect to other networks are called label edge routers (LERs), and LSRs within the MPLS domain are core LSRs.

Figure 1-1 MPLS network structure



When IP packets reach an MPLS network, the ingress LER analyzes the packets and then adds appropriate labels to them. All LSRs on the MPLS network forward packets based on labels. When IP packets leave the MPLS network, the egress LER pops the labels.

A path along which IP packets are transmitted on an MPLS network is called a label switched path (LSP). An LSP is a unidirectional path in the same direction data packets traverse.

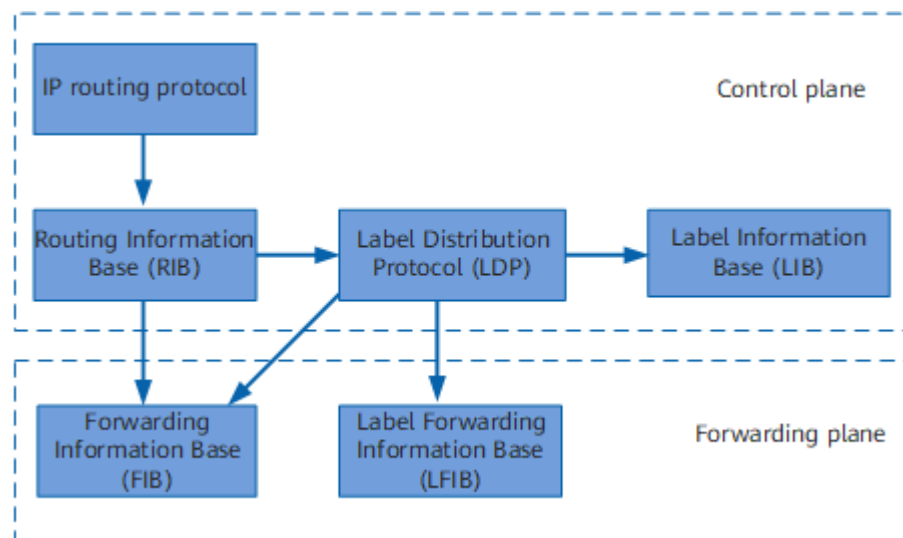
As shown in [Figure 1-1](#), the LER at the starting point of an LSP is the ingress node, and the LER at the end of the LSP is the egress node. The LSRs between the ingress node and egress node along the LSP are transit nodes. An LSP may have zero, one, or several transit nodes and only one ingress node and one egress node.

On an LSP, MPLS packets are sent from the ingress to the egress. In this transmission direction, the ingress node is the upstream node of the transit nodes, and the transit nodes are the downstream nodes of the ingress node. Similarly, transit nodes are the upstream nodes of the egress node, and the egress node is the downstream node of the transit nodes.

MPLS Architecture

[Figure 1-2](#) shows the MPLS architecture, which consists of a control plane and a forwarding plane.

Figure 1-2 MPLS architecture



The MPLS architecture has the following parts:

- Control plane: generates and maintains routing and label information
 - Routing information base (RIB): is generated by IP routing protocols and used to select routes.
 - Label distribution protocol (LDP): allocates labels, creates a label information base (LIB), and establishes and tears down LSPs.
 - Label information base (LIB): is generated by LDP and used to manage labels.

- Forwarding plane (data plane): forwards IP packets and MPLS packets
 - Forwarding information base (FIB): is generated based on routing information obtained from the RIB and used to forward common IP packets.
 - Label forwarding information base (LFIB): is created by LDP on an LSR and used to forward MPLS packets.

1.2.2 MPLS Label

Forwarding Equivalence Class

A forwarding equivalence class (FEC) is a collection of packets with the same characteristics. Packets of the same FEC are forwarded in the same way on an MPLS network.

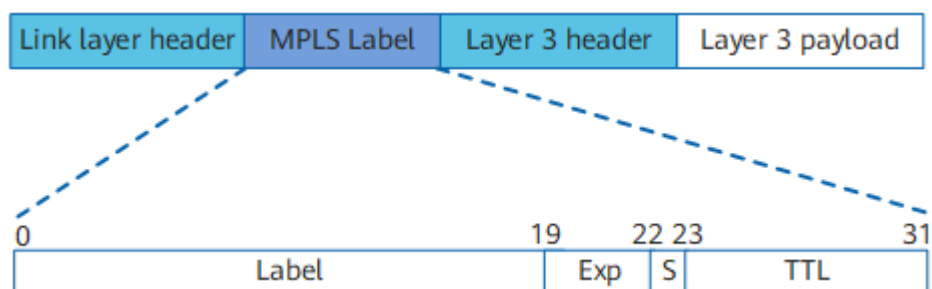
FECs can be identified by the source address, destination address, source port, destination port, and VPN. For example, in IP forwarding, packets matching the same route based on the longest match algorithm belong to an FEC.

Label

A label is a short, fixed-length (4 bytes) identifier that is only locally significant. A label identifies an FEC to which a packet belongs. In some cases, such as load balancing, an FEC can be mapped to multiple incoming labels. Each label, however, represents only one FEC on a device.

Compared with an IP packet, an MPLS packet has the additional 4-byte MPLS label. The MPLS label is between the link layer header and the network layer header, and allows use of any link layer protocol. [Figure 1-3](#) shows position of an MPLS label and fields in the MPLS label.

Figure 1-3 MPLS label encapsulation format



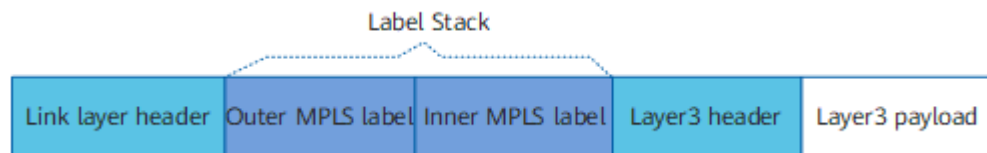
An MPLS label contains the following fields:

- Label: 20-bit label value.
- Exp: 3-bit, used as an extension value. Generally, this field is used as the class of service (CoS) field. When congestion occurs, devices prioritize packets that have a larger value in this field.
- S: 1-bit value indicating the bottom of a label stack. MPLS supports nesting of multiple labels. When the S field is 1, the label is at the bottom of the label stack.

- TTL: time to live. This 8-bit field is the same as the TTL field in IP packets.

A label stack is an arrangement of labels. In [Figure 1-4](#), the label next to the Layer 2 header is the top of the label stack (outer MPLS label), and the label next to the Layer 3 header is the bottom of the label stack (inner MPLS label). An MPLS label stack can contain an unlimited number of labels. Currently, MPLS label stacks can be applied to MPLS VPN.

Figure 1-4 Label stack



The label stack organizes labels according to the rule of Last-In, First-Out. The labels are processed from the top of the stack.

Label Space

The label space is the value range of the label, and the space is organized in the following ranges:

- 0 to 15: special labels. For details about special labels, see [Table 1-1](#).
- 16 or above: label space for dynamic signaling protocols, such as Label Distribution Protocol (LDP) and MultiProtocol Border Gateway Protocol (MP-BGP).

Table 1-1 Special labels

Label Value	Label	Description
0	IPv4 Explicit NULL Label	The label must be popped out (removed), and the packets must be forwarded based on IPv4. If the egress node allocates a label with the value of 0 to the penultimate hop LSR, the penultimate hop LSR pushes label 0 to the top of the label stack and forwards the packet to the egress node. When the egress node detects that the label of the packet is 0, the egress node pops the label out.
1	Router Alert Label	A label that is only valid when it is not at the bottom of a label stack. The label is similar to the Router Alert Option field in IP packets. After receiving such a label, the node sends it to a local software module for further processing. Packet forwarding is determined by the next-layer label. If the packet needs to be forwarded continuously, the node pushes the Router Alert Label to the top of the label stack again.

Label Value	Label	Description
2	IPv6 Explicit NULL Label	The label must be popped out, and the packets must be forwarded based on IPv6. If the egress node allocates a label with the value of 2 to the LSR at the penultimate hop, the LSR pushes label 2 to the top of the label stack and forwards the packet to the egress node. When the egress node recognizes that the value of the label carried in the packet is 2, the egress node immediately pops it out.
3	Implicit NULL Label	When the label with the value of 3 is swapped on an LSR at the penultimate hop, the LSR pops the label out and forwards the packet to the egress node. Upon receiving the packet, the egress node forwards the packet in IP forwarding mode or according to the next layer label.
4 to 13	Reserved	None.
14	OAM Router Alert Label	A label for operation, administration and maintenance (OAM) packets over an MPLS network. MPLS OAM sends OAM packets to monitor LSPs and report faults. OAM packets are transparent on transit nodes and the penultimate LSR.
15	Reserved	None.

1.2.3 LSP Setup

Before forwarding packets, MPLS must allocate labels to packets and establish an LSP.

Label Distribution Protocols for Dynamic LSPs

Dynamic LSPs are established using label distribution protocols. As the control protocol or signaling protocol for MPLS, a label distribution protocol defines FECs, distributes labels, and establishes and maintains LSPs.

MPLS can use the following protocols for label distribution:

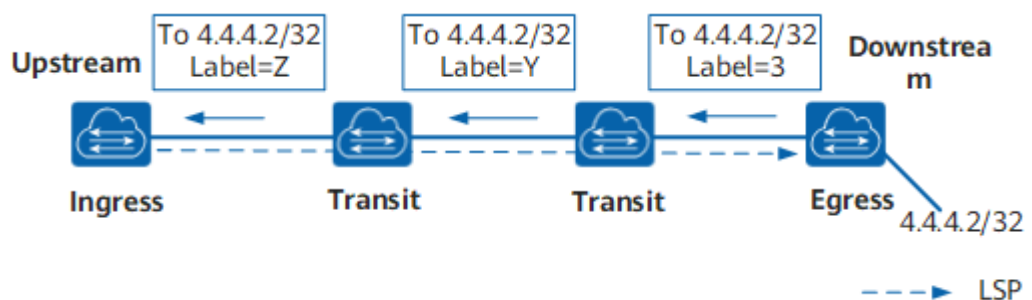
- LDP
The Label Distribution Protocol (LDP) is designed for distributing labels. It sets up an LSP hop by hop according to IGP and BGP routing information.
For details about LDP implementation, see Understanding MPLS LDP in the [2 MPLS LDP Configuration](#).
- MP-BGP
MP-BGP is an extension to BGP and allocates labels to MPLS VPN routes and inter-AS VPN routes.

For details about MP-BGP implementation, see BGP Configuration in *CloudEngine 9800, 8800, 6800, 5800 Series Switches Configuration Guide - IP Routing*.

Procedure for Establishing Dynamic LSPs

MPLS labels are distributed from downstream LSRs to upstream LSRs. As shown in [Figure 1-5](#), a downstream LSR identifies FECs based on the IP routing table, allocates a label to each FEC, and records the mapping between labels and FECs. The downstream LSR then encapsulates the mapping into a message and sends the message to the upstream LSR. As this process proceeds on all the LSRs, the LSRs create a label forwarding information base (LFIB) and establish an LSP.

Figure 1-5 Establishing a dynamic LSP



1.2.4 MPLS Forwarding

MPLS Forwarding Process

Basic Concepts

Label operations involved in MPLS packet forwarding include push, swap, and pop:

- **Push:** When an IP packet enters an MPLS domain, the ingress node adds a new label to the packet between the Layer 2 header and the IP header. Alternatively, an LSR adds a new label to the top of the label stack.
- **Swap:** When a packet is transferred within the MPLS domain, a local node swaps the label at the top of the label stack in the MPLS packet for the label allocated by the next hop according to the label forwarding table.
- **Pop:** When a packet leaves the MPLS domain, the label is popped out of (removed from) the MPLS packet.

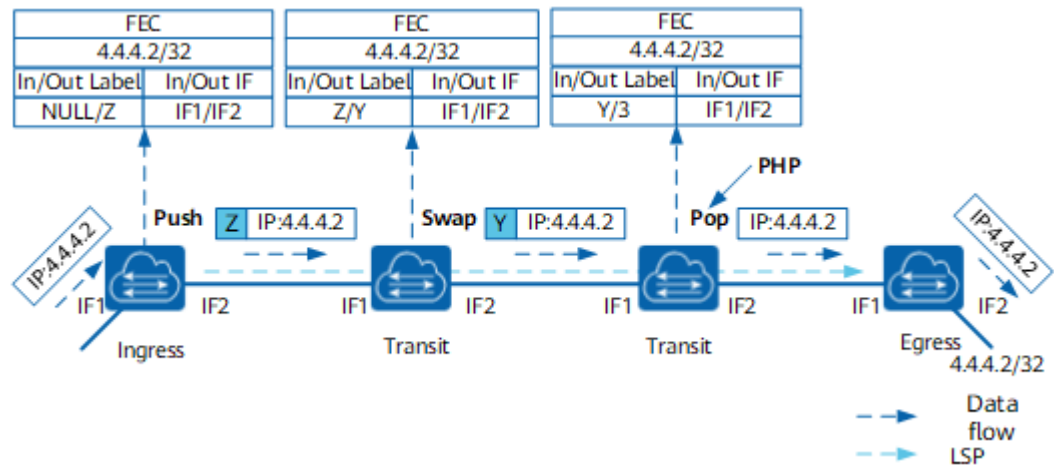
A label is invalid at the last hop of an MPLS domain. The penultimate hop popping (PHP) feature applies. On the penultimate node, the label is popped out of the packet to reduce the size of the packet that is forwarded to the last hop. Then, the last hop directly forwards the IP packet or forwards the packet by using the second label.

By default, PHP is configured on the egress node. The egress node supporting PHP allocates the label with the value of 3 to the penultimate hop.

Basic Forwarding Process

LSPs that support PHP are used in the following example to describe how MPLS packets are forwarded.

Figure 1-6 Basic MPLS forwarding process



As shown in [Figure 1-6](#), the LSRs have distributed MPLS labels and set up an LSP with the destination address of 4.4.4.2/32. MPLS packets are forwarded as follows:

1. The ingress node receives an IP packet destined for 4.4.4.2. Then, the ingress node adds Label Z to the packet and forwards it.
2. When the downstream transit node receives the labeled packet, the node replaces Label Z by Label Y.
3. When the transit node at the penultimate hop receives the packet with Label Y, the node pops out Label Y because the label value is 3. The transit node then forwards the packet to the egress node as an IP packet.
4. The egress node receives the IP packet and forwards it to 4.4.4.2/32.

MPLS TTL Processing

This section describes how MPLS processes the TTL and responds to TTL timeout.

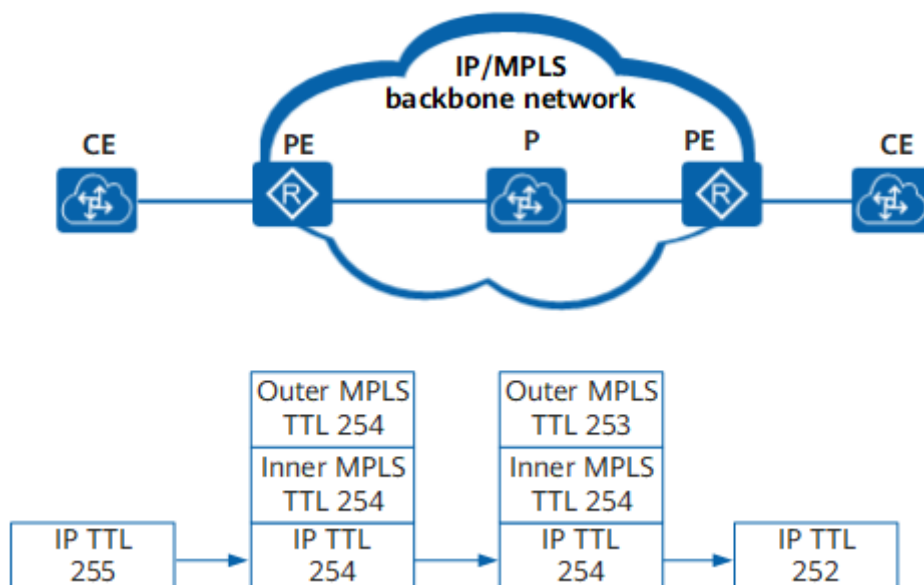
MPLS TTL Processing Modes

The TTL field in an MPLS label is 8 bits long. The TTL field is the same as that in an IP packet header. MPLS processes the TTL to prevent loops and implement traceroute.

MPLS TTL processing modes include: Uniform and Pipe modes. By default, MPLS processes the TTL in Uniform mode. The two modes work as follows:

- Uniform mode
When IP packets enter an MPLS network, the ingress node decreases the IP TTL by one and copies this new value to the MPLS TTL field. The TTL field in MPLS packets is processed in standard mode. The egress node decreases the MPLS TTL by one and maps this new value to the IP TTL field. [Figure 1-7](#) shows how the TTL field is processed on the transmission path.

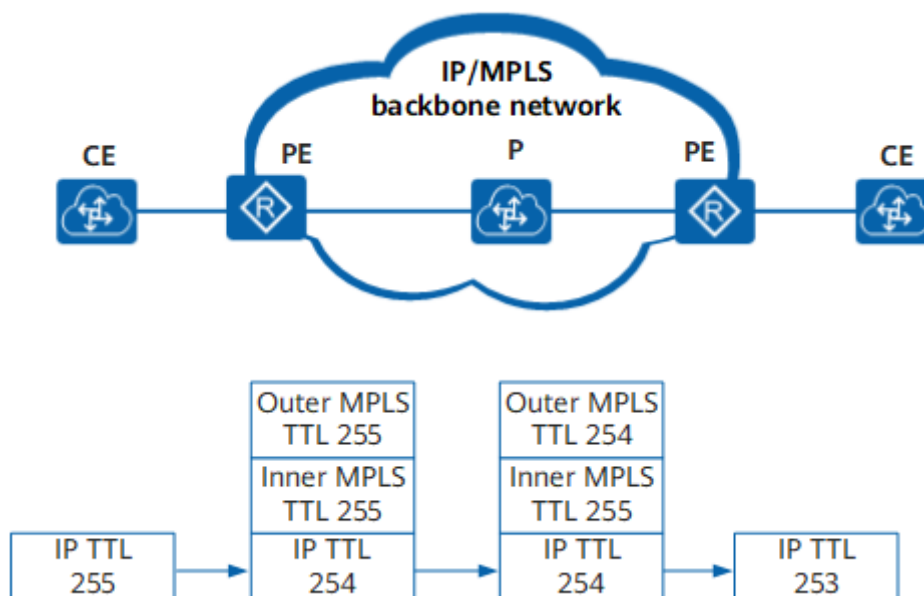
Figure 1-7 TTL processing in Uniform mode



- Pipe mode

As shown in [Figure 1-8](#), the ingress node decreases the IP TTL by one and the MPLS TTL remains constant. The TTL field in MPLS packets is processed in standard mode. The egress node decreases the IP TTL by one. In Pipe mode, the IP TTL only decreases by one on the ingress node and one on the egress node when packets travel across an MPLS network.

Figure 1-8 TTL processing in Pipe mode



In MPLS VPN applications, the MPLS backbone network needs to be shielded to ensure network security. The Pipe mode is recommended for private network packets.

ICMP Response Packet

On an MPLS network, when an LSR receives an MPLS packet with the TTL value of 1, the LSR generates an ICMP response packet.

The LSR returns the ICMP response packet to the sender in the following ways:

- If the LSR has a reachable route to the sender, the LSR directly sends the ICMP response packet to the sender through the IP route.
- If the LSR has no reachable route to the sender, the LSR forwards the ICMP response packet along the LSP. The egress node forwards the ICMP response packet to the sender.

In most cases, the received MPLS packet contains only one label and the LSR responds to the sender with the ICMP response packet using the first method. If the MPLS packet contains multiple labels, the LSR uses the second method.

The MPLS VPN packets may contain only one label when they arrive at an autonomous system boundary router (ASBR) on the MPLS VPN. These devices have no IP routes to the sender, so they use the second method to reply to the ICMP response packets.

1.2.5 LSP Connectivity Check

Overview of LSP Connectivity Check

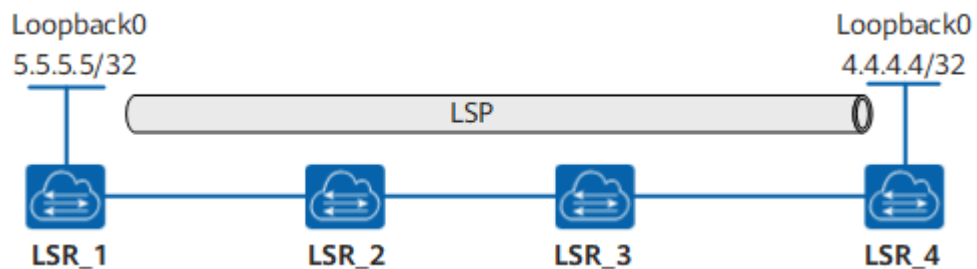
On an MPLS network, the control panel used for setting up an LSP cannot detect the failure in data forwarding of the LSP. This makes network maintenance difficult. The MPLS ping and tracer mechanisms detect LSP errors and locate faulty nodes.

MPLS ping is used to check network connectivity. MPLS tracer is used to check the network connectivity, and to locate network faults. Similar to IP ping and tracer, MPLS ping and tracer use MPLS echo request packets and MPLS echo reply packets to check LSP availability. MPLS echo request packets and echo reply packets are both encapsulated into User Datagram Protocol (UDP) packets. The UDP port number of the MPLS echo request packet is 3503, which can be identified only by MPLS-enabled devices.

An MPLS echo request packet carries FEC information to be detected, and is sent along the same LSP as other packets with the same FEC. In this manner, the connectivity of the LSP is checked. MPLS echo request packets are forwarded to the destination end using MPLS, while MPLS echo reply packets are forwarded to the source end using IP. Routers set the destination address in the IP header of the MPLS echo request packets to 127.0.0.1/8 (local loopback address) and the TTL value is 1. In this way, MPLS echo request packets are not forwarded using IP forwarding when the LSP fails so that the failure of the LSP can be detected.

MPLS Ping

Figure 1-9 MPLS network



As shown in [Figure 1-9](#), LSR_1 establishes an LSP to LSR_4. LSR_1 performs MPLS ping on the LSP by performing the following steps:

1. LSR_1 checks whether the LSP exists. If the LSP does not exist, an error message is displayed and the MPLS ping stops. If the LSP exists, LSR_1 performs the following operations.
2. LSR_1 creates an MPLS echo request packet and adds 4.4.4.4 to the destination FEC in the packet. In the IP header of the MPLS echo request packet, the destination address is 127.0.0.1/8 and the TTL value is 1. LSR_1 searches for the corresponding LSP, adds the LSP label to the MPLS echo request packet, and sends the packet to LSR_2.
3. Transit nodes LSR_2 and LSR_3 forward the MPLS echo request packet based on MPLS. If MPLS forwarding on a transit node fails, the transit node returns an MPLS echo reply packet carrying the error code to LSR_1.
4. If no fault exists along the MPLS forwarding path, the MPLS echo request packet reaches the LSP egress node LSR_4. LSR_4 returns a correct MPLS echo reply packet after verifying that the destination IP address 4.4.4.4 is the loopback interface address. MPLS ping is complete.

MPLS Tracert

As shown in [Figure 1-9](#), LSR_1 performs MPLS tracert on LSR_4 (4.4.4.4/32) by performing the following steps:

1. LSR_1 checks whether an LSP exists to LSR_4. If the LSP does not exist, an error message is displayed and the tracert stops. If the LSP exists, LSR_1 performs the following operations.
2. LSR_1 creates an MPLS echo request packet and adds 4.4.4.4 to the destination FEC in the packet. In the IP header of the MPLS echo request packet, the destination address is 127.0.0.1/8. Then LSR_1 adds the LSP label to the packet, sets the MPLS TTL value to 1, and sends the packet to LSR_2. The MPLS echo request packet contains a downstream mapping type-length-value (TLV) that carries downstream information about the LSP at the current node, such as next-hop address and outgoing label.
3. Upon receiving the MPLS echo request packet, LSR_2 decreases the MPLS TTL by one and finds that TTL times out. LSR_2 then checks whether the LSP exists and the next-hop address and whether the outgoing label of the

downstream mapping TLV in the packet is correct. If so, LSR_2 returns a correct MPLS echo reply packet that carries the downstream mapping TLV of LSR_2. If not, LSR_2 returns an incorrect MPLS echo reply packet.

4. After receiving the correct MPLS echo reply packet, LSR_1 resends the MPLS echo request packet that is encapsulated in the same way as step 2 and sets the MPLS TTL value to 2. The downstream mapping TLV of this MPLS echo request packet is replicated from the MPLS echo reply packet. LSR_2 performs common MPLS forwarding on this MPLS echo request packet. If TTL times out when LSR_3 receives the MPLS echo request packet, LSR_3 processes the MPLS echo request packet and returns an MPLS echo reply packet in the same way as step 3.
5. After receiving a correct MPLS echo reply packet, LSR_1 repeats step 4, sets the MPLS TTL value to 3, replicates the downstream mapping TLV in the MPLS echo reply packet, and sends the MPLS echo request packet. LSR_2 and LSR_3 perform common MPLS forwarding on this MPLS echo request packet. Upon receiving the MPLS echo request packet, LSR_4 repeats step 3 and verifies that the destination IP address 4.4.4.4 is the loopback interface address. LSR_4 returns an MPLS echo reply packet that does not carry the downstream mapping TLV. MPLS tracer is complete.

When routers return the MPLS echo reply packet that carries the downstream mapping TLV, LSR_1 obtains information about each node along the LSP.

1.3 Application Scenarios for MPLS

1.3.1 MPLS VPN

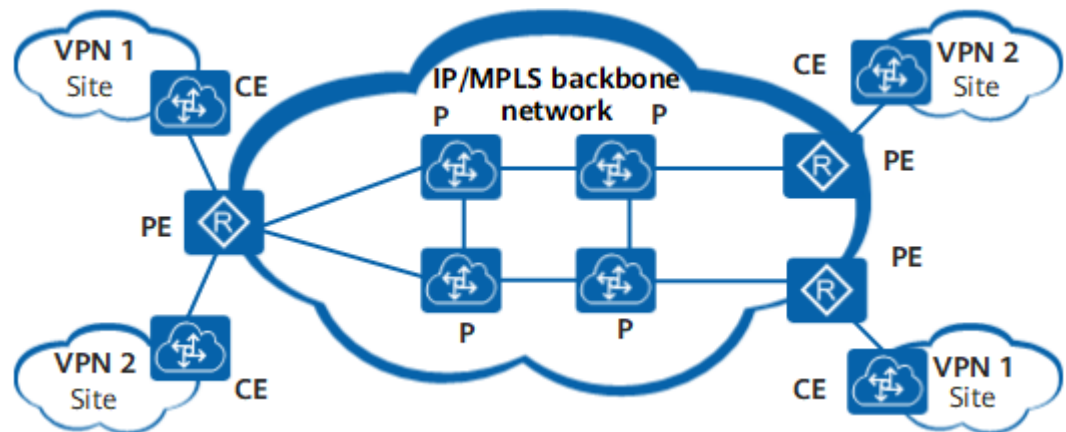
Traditional VPNs transmit private network data over the public network using tunneling protocols, such as the Generic Routing Encapsulation (GRE), Layer 2 Tunneling Protocol (L2TP), and Point to Point Tunneling Protocol (PPTP). MPLS LSPs are set up by swapping labels, and data packets are not encapsulated or encrypted. Therefore, MPLS is an appropriate technology for VPN implementation.

MPLS VPN can build a private network with security similar to a Frame Relay (FR) network. On MPLS VPN networks, customer devices do not need to set up tunnels such as GRE and L2TP tunnels, so the network delay is minimized.

As shown in [Figure 1-10](#), the MPLS VPN connects private network branches through LSPs to form a unified network. The MPLS VPN also controls the interconnection between VPNs. [Figure 1-10](#) shows the devices on an MPLS VPN network.

- A customer edge (CE) is deployed on the edge of a customer network. It can be a router, a switch, or a host.
- A provider edge (PE) is deployed on the edge of an IP/MPLS backbone network.
- A provider (P) device on an IP/MPLS backbone network is not directly connected to CEs. The provider device only needs to provide basic MPLS forwarding capabilities and does not maintain VPN information.

Figure 1-10 MPLS VPN



An MPLS VPN has the following characteristics:

- PEs manage VPN users, set up LSPs between PEs, and advertise routing information between users in a VPN.
- PEs use MP-BGP to advertise VPN routing information.
- The MPLS-based VPN supports IP address multiplexing between sites as well as the interconnection of different VPNs.

1.4 MPLS Common Configuration

1.4.1 (Optional) Configuring the MPLS TTL Processing Mode

Context

MPLS processes the TTL in the following modes:

- MPLS TTL processing modes
In MPLS applications, the MPLS backbone network needs to be shielded to ensure network security. The MPLS Pipe mode on the ingress node is recommended for private network packets. To reflect the path where packets pass, use the MPLS Uniform mode on the ingress node.
- Path where ICMP response packets are transmitted
By default, when the received MPLS packet contains only one label, the LSR directly sends an ICMP response packet to the sender using an IP route. When the received MPLS packet contains multiple labels, the LSR sends an ICMP response packet to the sender along an LSP.
However, MPLS packets received by the devices may contain only one label in some cases. The devices have no IP routes to the sender, so they forward the ICMP response packets along an LSP.

Procedure

- Configuring the MPLS TTL processing mode.
For the CE6870EI, run the following commands.

- a. Run **system-view**
The system view is displayed.
- b. Run **mpls mode { short-pipe [ttl *ttlvalue* exp *expvalue*] | uniform }**
The MPLS TTL processing mode is configured.
By default, the MPLS TTL processing mode is Uniform.
- c. Run **commit**
The configuration is committed.

For non-CE6870EI, run the following commands.

- a. Run **system-view**
The system view is displayed.
 - b. Run **mpls**
The MPLS view is displayed.
 - c. Run **mpls ldp ttl-mode { pipe | uniform }**
The mode for MPLS LDP to process TTLs in packets is configured.
By default, MPLS LDP processes TTLs in packets in uniform mode.
 - d. Run **quit**
The system view is displayed.
 - e. Run **commit**
The configuration is committed.
- Configuring the path where ICMP response packets are transmitted
 - a. Run **system-view**
The system view is displayed.
 - b. Run **mpls**
The MPLS view is displayed.
 - c. Run **ttl expiration pop disable**
The device is configured to transmit ICMP response packets along an LSP.

Or run **undo ttl expiration pop disable**:

The device is configured to transmit ICMP response packets using an IP route.

By default, the LSR returns an ICMP packet using the local IP route if the received MPLS TTL-expired packet contains one label.
 - d. Run **quit**
The system view is displayed.
 - e. Run **commit**
The configuration is committed.

----End

1.4.2 (Optional) Configuring MPLS MTU

Context

The size of the maximum transmission unit (MTU) determines the maximum number of bytes that can be transmitted by the sender at a time. If the MTU exceeds the maximum number of bytes supported by the receiver or a transit device, packets are fragmented or even discarded, which increases the network transmission load. In this manner, devices have to calculate the MTU before the communication to ensure that sent packets reach the receiver successfully.

$$\text{LDP MTU} = \text{Min} \{ \text{All MTUs advertised by all downstream devices, MTU of the local outbound interface} \}$$

A downstream LSR uses the preceding formula to calculate an MTU, adds it to the MTU TLV in a Label Mapping message, and sends the Label Mapping message to the upstream device. If an MTU value changes (such as when the local outbound interface or its configuration is changed), an LSR recalculates an MTU and sends a Label Mapping message carrying the new MTU to its upstream LSR. The relationships between the MPLS MTU and the interface MTU are as follows:

- If an interface MTU but not an MPLS MTU is configured on an interface, the interface MTU is used.
- If both an MPLS MTU and an interface MTU are configured on an interface, the smaller value between the MPLS MTU and the interface MTU is used.

MPLS determines the size of MPLS packets on the ingress node according to the LDP MTU to prevent the transit node from forwarding large-sized MPLS packets.

Procedure

Step 1 Run **system-view**

The system view is displayed.

Step 2 Run **mpls ldp**

The MPLS LDP view is displayed.

Step 3 Run the following commands as required.

- Run **mtu-signalling disable**

The LSR is disabled from sending Label Mapping messages carrying MTU TLVs.

By default, the switch enables Label Mapping messages from carrying an MTU TLV.

- Run **mtu-signalling apply-tlv**

The LSR is configured to send Label Mapping messages carrying MTU TLVs that comply with RFC 3988.

By default, the switch sends Label Mapping messages carrying Huawei proprietary MTU TLV.

Step 4 Run **quit**

The system view is displayed.

Step 5 Run **interface** *interface-type interface-number*

The view of an MPLS-enabled interface is displayed.

Step 6 On an Ethernet interface, run **undo portswitch**

The interface is switched to Layer 3 mode.

By default, an Ethernet interface works in Layer 2 mode.

The mode switching function takes effect when the interface only has attribute configurations (for example, **shutdown** and **description** configurations). Alternatively, if configuration information supported by both Layer 2 and Layer 3 interfaces exists (for example, **mode lacp** and **lacp system-id** configurations), no configuration that is not supported after the working mode of the interface is switched can exist. If unsupported configurations exist on the interface, delete the configurations first and then run the **undo portswitch** command.

 NOTE

If many Ethernet interfaces need to be switched to Layer 3 mode, run the **undo portswitch batch interface-type { interface-number1 [to interface-number2] } <1-10>** command in the system view to switch these interfaces to Layer 3 mode in batches.

Step 7 Run **mpls mtu mtu**

An MPLS MTU is configured on the interface.

By default, the MTU of MPLS packets is equal to the interface MTU.

Step 8 Run **commit**

The configuration is committed.

----End

1.4.3 (Optional) Configuring the PHP Feature

Context

No label needs to be swapped on the egress node of an LSP. PHP can be configured on the egress node to allow the LSR at the penultimate hop to pop out the label from an MPLS packet and send the packet to the egress node. After receiving the packet, the egress node directly forwards the packet through an IP link or according to the next layer label. PHP helps reduce the burden on the egress node.

Procedure

Step 1 Run **system-view**

The system view is displayed.

Step 2 Run **mpls**

The MPLS view is displayed.

Step 3 Run **label advertise { explicit-null | implicit-null | non-null }**

The label allocated to the LSR at the penultimate hop is configured.

The egress node can allocate different labels to the PHP based on the parameter setting.

- **implicit-null**: default value, which indicates that PHP is supported. If this parameter is configured, the egress node allocates an implicit null label with the value of 3 to the LSR at the penultimate hop.
- **explicit-null**: PHP is not supported. If this parameter is configured, the egress node allocates an explicit null label with the value of 0 to the LSR at the penultimate hop. The **explicit-null** parameter can be configured when MPLS QoS attributes are used.
- **non-null**: PHP is not supported. If this parameter is configured, the egress allocates a common label with a value greater than or equal to 16 to the LSR at the penultimate hop. The **non-null** parameter can be configured when MPLS QoS attributes are used.

 NOTE

After removing MPLS labels, switches except CE6870EI does not load balance MPLS packets through an Eth-Trunk based on the IP header by default. In the PHP scenario, you can configure the **mpls top-label src-ip dst-ip 2nd-label** command on the penultimate hop to load balance traffic to an Eth-Trunk. You can modify the load balancing profile based on the traffic characteristics to optimize the load balancing effect.

After the **label advertise** command is run to change the label distribution mode on the egress node, the modification takes effect on new LSPs but not on existing LSPs. To enable the modification to take effect on the existing LSPs, run the **reset mpls ldp** or **lsp-trigger** command.

Step 4 Run **commit**

The configuration is committed.

----End

1.4.4 Enabling the MPLS Trap Function

Context

To facilitate operation and maintenance and determine the running status of the MPLS network, configure the MPLS trap function so that the device can notify the NMS of the LDP session status.

Procedure

- Configure the trap function for LDP.
 - a. Run **system-view**
The system view is displayed.
 - b. Run **snmp-agent trap enable feature-name ldp [trap-name trapname]**
The trap function is enabled for the MPLS LDP module.
By default, the trap function is disabled for the MPLS LDP module.
- Configure the trap function for LSPM.

a. Run **system-view**

The system view is displayed.

b. Run **snmp-agent trap enable feature-name mpls_lspm [trap-name trapname]**

The trap function is enabled for the MPLS LSPM module.

By default, the trap function is disabled for the MPLS LSPM module.

When performing the following steps to configure alarm thresholds, pay attention to the following points:

- To configure the alarm function for dynamic label usage, specify **hwmplsdynamiclabelthresholdexceed** and **hwmplsdynamiclabelthresholdexceedclear** to enable the threshold exceeding alarm and clear alarm when configuring **trap-name**. When the usage of dynamic labels exceeds the upper threshold or falls below the lower threshold, the system generates a threshold exceeding alarm or clear alarm.
- To configure the LSP usage alarm function, specify **hwmplslspthresholdexceed** and **hwmplslspthresholdexceedclear** to enable the threshold exceeding alarm and clear alarm when configuring **trap-name**. When the LSP usage exceeds the upper threshold or falls below the lower threshold, the system generates a threshold exceeding alarm or clear alarm.
- To configure the alarm function for MPLS resource usage, specify **hwmplsresourcethresholdexceed** and **hwmplsresourcethresholdexceedclear** to enable the threshold exceeding alarm and clear alarm when configuring **trap-name**. When the usage of MPLS resources exceeds the upper threshold or falls below the lower threshold, the system generates a threshold exceeding alarm or clear alarm.

c. Run **mpls**

The MPLS view is displayed.

d. Run **mpls dynamic-label-number threshold-alarm upper-limit upper-limit-value lower-limit lower-limit-value**

The upper and lower thresholds for dynamic label usage are set.

You can set the following parameters:

- *upper-limit-value*: a percent indicating the upper limit of dynamic labels. If dynamic label usage reaches the upper limit, an alarm is generated. An upper limit less than or equal to 95% is recommended.
- *lower-limit-value*: a percent indicating the lower limit of dynamic labels. If dynamic label usage falls below the lower limit, a clear alarm is generated.
- The value of *upper-limit-value* must be greater than that of *lower-limit-value*.

By default, the upper limit is 80%, and the lower limit is 70%, which are recommended.

After the **snmp-agent trap enable feature-name mpls_lspm trap-name { hwmplsdynamiclabeltotalcountexceed | hwmplsdynamiclabeltotalcountexceedclear }** command is run to enable the device to generate limit-reaching alarms and their clear alarms, the following situations occur:

- If the number of dynamic labels reaches the maximum number of dynamic labels supported by a device, a limit-reaching alarm is generated.
 - If the number of dynamic labels falls below 95% of the maximum number of dynamic labels supported by the device, a clear alarm is generated.
- e. Run **mpls ldp-lsp-number threshold-alarm upper-limit *upper-limit-value* lower-limit *lower-limit-value***

The upper and lower thresholds of alarms for LDP LSP usage are configured.

The parameters in this command are described as follows:

- *upper-limit-value* specifies the upper threshold of alarms for LDP LSP usage. An alarm is generated when the proportion of established LDP LSPs to total supported LDP LSPs reaches the upper limit.
- *lower-limit-value* specifies the lower threshold of clear alarms for LDP LSP usage. A clear alarm is generated when the proportion of established LDP LSPs to total supported LDP LSPs falls below the lower limit.
- The value of *upper-limit-value* must be greater than that of *lower-limit-value*.

By default, the upper limit of the alarm threshold for LDP LSP usage is 80%, the lower limit of the clear alarm threshold for LDP LSP usage is 75%, which are recommended.

After the **snmp-agent trap enable feature-name mpls_lspm trap-name { hwmplslsptotalcountexceed | hwmplslsptotalcountexceedclear }** command is run to enable LSP limit-crossing alarm and LSP limit-crossing clear alarm, an alarm is generated in the following situations:

- If the total number of LDP LSPs reaches the upper limit, a limit-crossing alarm is generated.
 - If the total number of LDP LSPs falls below 95% of the upper limit, a limit-crossing clear alarm is generated.
- f. Run **mpls remote-adjacency-number threshold-alarm upper-limit *upper-limit-value* lower-limit *lower-limit-value***

The conditions that trigger the threshold-reaching alarm and its clear alarm for remote LDP adjacencies are configured.

Note the following issues when configuring trigger conditions:

- *upper-limit-value*: upper alarm threshold for the proportion of established remote LDP adjacencies to all supported ones.
- *lower-limit-value*: lower alarm threshold for the proportion of established remote LDP adjacencies to all supported ones.
- The value of *upper-limit-value* must be greater than that of *lower-limit-value*.

By default, the upper alarm threshold is 80%, and the lower alarm threshold is 75%, which are recommended.

When the number of remote LDP adjacencies exceeds the upper threshold or falls below the lower threshold, the system generates a threshold exceeding alarm or clear alarm.

- g. Run **mpls outsegment-number threshold-alarm upper-limit *upper-limit-value* lower-limit *lower-limit-value***

The alarm threshold for LDP OutSegment number is configured.

The parameters in this command are described as follows:

- *upper-limit-value* specifies the upper limit of the alarm threshold for LDP OutSegment number.
- *lower-limit-value* specifies the lower limit of the clear alarm threshold for LDP OutSegment number.
- The value of *upper-limit-value* must be greater than that of *lower-limit-value*.

By default, the upper limit of the alarm threshold for LDP OutSegment number is 80%, the lower limit of the clear alarm threshold for LDP OutSegment number is 75%, which are recommended.

When the LDP OutSegment number exceeds the upper threshold or falls below the lower threshold, the system generates a threshold exceeding alarm or clear alarm.

----End

Checking the Configuration

- Run the **display snmp-agent trap feature-name ldp all** command to check the status of all traps on the MPLS LDP module.
- Run the **display snmp-agent trap feature-name mpls lspm all** command to check all trap messages on the MPLS LSPM module.
- Run the **display default-parameter mpls management** command to check default configurations of the MPLS management module.

1.4.5 (Optional) Configuring the Function of Removing MPLS Labels

Context

In some scenarios, an MPLS-incapable device needs to be able to remove MPLS labels to obtain IP packet information in MPLS packets and redirect the IP packet information to the analyzer for traffic analysis.

To meet this requirement, configure the function of removing MPLS labels on the interfaces of the device. Then the device offsets MPLS packets. If the packets match the traffic policy on the device, the device removes the MPLS labels from the packets and forwards the packets through the outbound interface.

Procedure

Step 1 Run **system-view**

The system view is displayed.

Step 2 Enter the interface view.

- Run **interface** *interface-type interface-number*
The Ethernet interface view is displayed.
- Run **interface Eth-trunk** *trunk-id*
The Eth-Trunk interface view is displayed.

Step 3 Run **mpls pop-label all**

The function of removing MPLS labels is enabled on the interface. By default, the function of removing MPLS labels is disabled.

NOTE

Only the CE5881, CE6820, CE6881, CE6881E, CE6881K, CE6863, CE6863K and CE6863E support this command.

 NOTE

- MPLS label removal is supported only for L3VPN MPLS+IPv4 (without Header Options) and L2VPN MPLS+ETH+IPv4 (without Header Options). These packets may be incorrectly identified as IPv4 packets during strong verification. A maximum of five layers of labels can be removed.
- MPLS label removal is not supported for MPLS+IPv4 (with Header Options) and MPLS+ETH (without the IP header) packets.
- MPLS labels with the control word cannot be removed. The control word is used in the ping trace, BFD, and VPLS scenarios to detect the PW connectivity. In practice, the control word is seldom used for L3VPN data traffic.
- MPLS label removal is supported only for MPLS UC packets (with the outer Ethernet header being 0x8847) but not for MPLS MC packets (with the outer Ethernet header being 0x8848).
- MPLS labels can be removed from MPLS packets only when MPLS label removal is enabled on inbound interfaces and the action of redirecting inner IPv4 packets matching an ACL rule to a physical interface or an LAG interface is configured.
- Only Layer 2 interfaces (physical interfaces and LAG interfaces) support MPLS label removal. VLANIF interfaces, sub-interfaces, Layer 3 main interfaces, stack interfaces, peer-link interfaces, and LAG member interfaces do not support this function.
- In the MPLS label removal scenario, an ACL rule **if-match-any** needs to be configured. This rule has the lowest priority, and packets matching this rule will be redirected to the specified physical interface or LAG interface. If this rule is not configured, the forwarding behavior of the packets that do not match ACLs is unpredictable.
- For the MPLS packets received by the interface that has MPLS label removal enabled, other services such as VLAN check, incoming statistics collection, and MAC address learning are processed normally.

Step 4 Run commit

The configuration is committed.

----**End**