MPLS Configuration

1. Configuring MPLS Basics
2. Configuring MPLS RAS

Contents

1 Configuring MPLS Basics

1.1 Introduction

Multiprotocol Label Switching (MPLS) is a tunneling technology that uses labels for efficient data transmission on backbone networks. MPLS supports multiple network layer protocols, such as Internet Protocol (IP), IPv6, and Internetwork Packet Exchange (IPX) and is compatible with various link layer technologies, such as Asynchronous Transfer Mode (ATM), frame relay, Ethernet, and Point-to-Point Protocol (PPP).

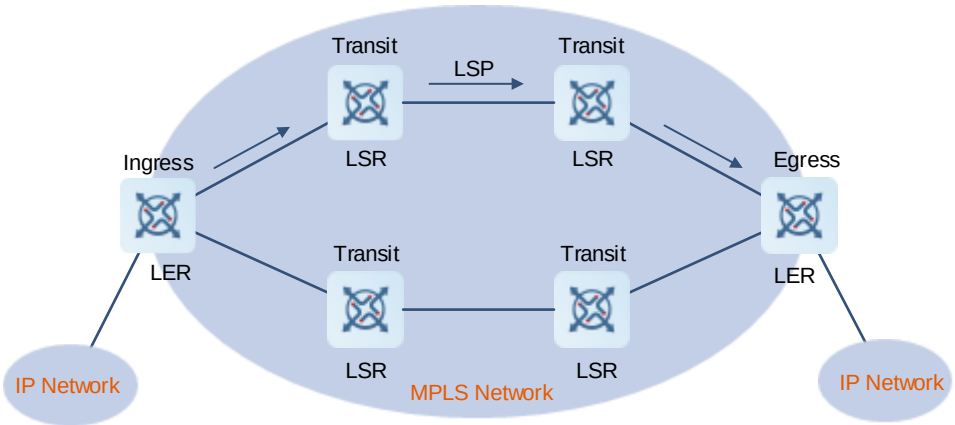
MPLS was first introduced to enhance the forwarding rate of routing devices. With MPLS, a device needs to analyze only the headers of forwarding IP packets at the MPLS network edge and does not need to analyze each hop on the MPLS network. This reduces the processing time when compared with traditional IP routing. With the development of hardware technologies and network processors, MPLS has gradually lost its appeal in efficient forwarding. However, MPLS provides connection-oriented label switching attributes to connectionless IP networks and integrates the flexibility of IP routing and the simplicity of Layer 2 switching. Due to the innate advantage of combining Layer 2 switching and Layer 3 routing technologies, MPLS still has unprecedented edges over other technologies in terms of virtual private networks (VPNs) and traffic engineering (TE). Therefore, MPLS is widely used in VPN and TE scenarios.

1.1.1 MPLS Network Structure

An MPLS network comprises label edge routers (LERs) and label switching routers (LSRs).

- LERs are located at the edges of an MPLS network. An ingress LER classifies packets entering the MPLS network, adds labels to the packets, and encapsulates the packets into MPLS packets to forward. An egress LER pops the labels off outgoing MPLS packets and restores the packets to original ones. An LER provides traffic classification, label mapping, and label removal functions.
- LSRs are located at the core of an MPLS network, run an MPLS signaling protocol, and forward packets based on labels.

Figure 1-1 MPLS Network Structure



A label-switched path (LSP) is the path along which IP packets travel through an MPLS network. It is a collection of LSRs and can be regarded as a tunnel traversing the MPLS core network.

Devices running MPLS are MPLS nodes. As shown in Figure 1-1, the LERs and LSRs on the MPLS network are MPLS nodes. MPLS nodes can identify MPLS signaling protocols, run one or more Layer 3 routing protocols (including static routing protocols), and forward packets based on MPLS labels. Generally, MPLS nodes are also capable of forwarding original Layer 3 packets (such as IP packets).

- The LER at the entry of an LSP is called the ingress LER, an LSR in the middle of the LSP is called a transit LSR, and the LER at the exit of the LSP is called the egress LER. An LSP may have no, one, or multiple transit LSRs but can have only one ingress LER and one egress LER.
- An LSP is a unidirectional path based on the data flow.
- According to the LSP direction, MPLS packets are forwarded from the ingress LER to the egress LER. Therefore, the ingress LER is an upstream node of the transit LSR, and the transit LSR is a downstream node of the ingress LER. In the same way, the transit LSR is an upstream node of the egress LER, and the egress LER is a downstream node of the transit LSR.

1.1.2 MPLS Label

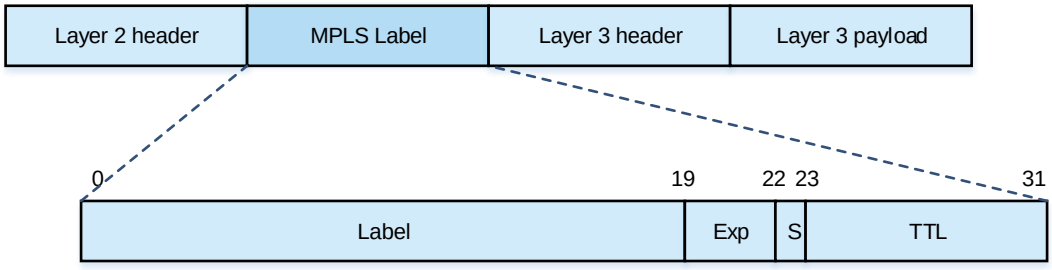
1. FEC

MPLS groups packets with the same characteristics into an FEC. In IP unicast routing, FECs are classified based on the destination address prefixes. All packets to the same destination belong to the same FEC. That is, one route corresponds to one FEC. Packets of the same FEC are handled in the same way on an MPLS network.

2. Label

A label is a short identifier with fixed length and of local significance. Labels are distributed and transmitted only between two adjacent MPLS nodes. Therefore, they are valid only between the adjacent MPLS nodes.

Figure 1-2 MPLS Label Structure



A label is 32-bit long and consists of the following four fields:

- Label field

  This field is 20-bit long and used to store the label value. Each label uniquely identifies an FEC. The Internet Engineering Task Force (IETF) defines 0 to 15 as special labels. The following table describes the meanings of these special labels.

Table 1-1 Special Labels

Label	Description
0	Indicates the IPv4 explicit null label. During IPv4 packet forwarding, if the outgoing label of the penultimate LSR is 0, the penultimate LSR must push label 0 to the top of the label stack before forwarding the packet to the next hop. When the last hop receives the packet with label 0, it pops label 0 off.
1	Indicates the router alert label. This label is not allowed at the bottom of the label stack. It is similar to the Router Alert Option of IP packets. When receiving packets with label 1, a router must send the packets to the local software module to process. Actually, the packets are forwarded based on the label below label 1. Before packet forwarding, however, label 1 must be pushed to the label stack again. Each LSR must check MPLS packets that carry label 1.
2	Indicates the IPv6 explicit null label. During IPv6 packet forwarding, if the outgoing label of the penultimate LSR is 2, the penultimate LSR must push label 2 to the top of the label stack before forwarding the packet to the next hop. When the last hop receives the packet with label 2, it pops label 2 off.
3	Indicates the implicit null label. This label can be distributed by the Label Distribution Protocol (LDP) but can never be transmitted in the label stacks of MPLS packets. When an LSR swaps the label for an MPLS packet and finds that the top label to be swapped is 3, the LSR pops the top label off rather than replacing it. Label 3 is used in the Penultimate Hop Popping (PHP) function.
4–15	Reserved

- Exp field

  This field is 3-bit long and used to store the MPLS quality of service (QoS) information.

- S tag

  This field is 1-bit long and used to identify the stack bottom. MPLS supports label nesting. When multiple labels exist, the S bit is set to **1** for the stack bottom label and to **0** for other labels. When only one label exists, the S bit is set to **1**.

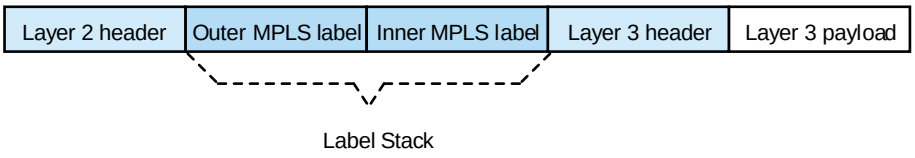
- TTL

  This field is 8-bit long and similar to the time to live (TTL) value in IP packet headers.

3. Label Stack

An MPLS packet can carry multiple layers of labels, that is, a label stack. The label stack enables MPLS to support hierarchical network systems. As shown in Figure 1-3, the label that is close to the link layer header is the top label, and the label that is next to the IP header is the bottom label. An LSR always swaps labels based on the top label. When multiple labels exist, each label must be complete and have 32 bits.

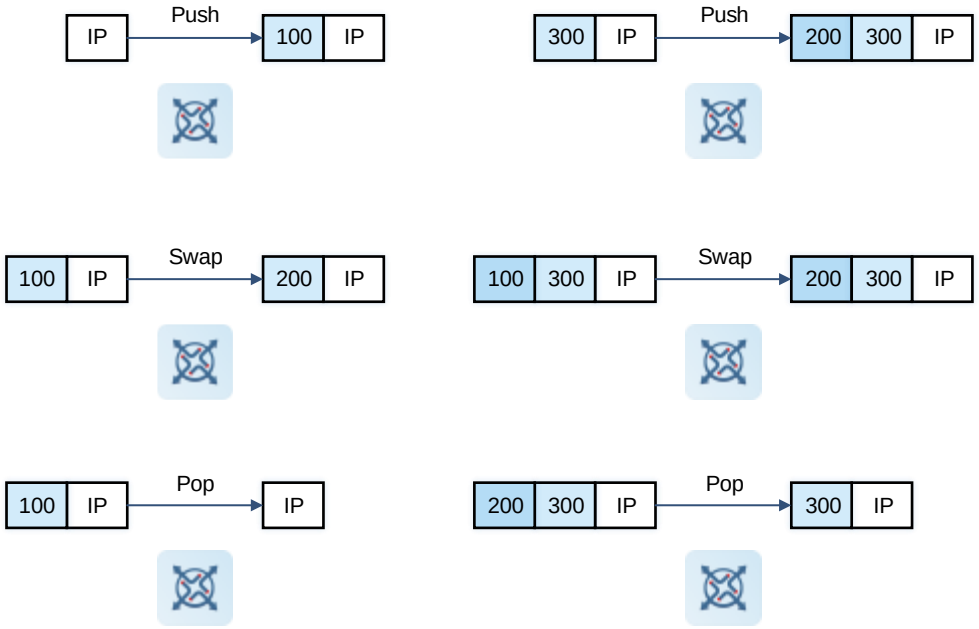
Figure 1-3 MPLS Label Stack



4. Operation Methods of Labels

MPLS nodes can push, swap, and pop labels.

Figure 1-4 Basic Label Operations



- Push

  The ingress LER inserts a label between the link layer header and network layer header, or a transit LSR pushes a new label to the stack top of an MPLS packet.

- Swap

  A transit LSR swaps the top label of an MPLS packet based on the incoming label map (ILM).

- Pop

  The egress LER pops labels off an MPLS packet to restore the IP packet, or a transit LSR pops the top label off to reduce the layers of a label stack.

1.1.3 MPLS Forwarding

1. MPLS Forwarding Tables

During MPLS forwarding, three tables are involved: Next Hop Label Forwarding Entry (NHLFE), FEC-To-NHLFE (FTN), and Incoming Label Map (ILM).

- NHLFE

The NHLFE table is used to store the next-hop information of MPLS packets. Generally, it contains the following content:

- Next hop of data packets
- Link layer encapsulation of data packets to be forwarded
- Encoding method in the label stack of data packets to be forwarded
- Operations to the label stack of data packets

- FTN

  The FTN table maps each FEC to a series of NHLFEs (multiple NHLFEs indicate multiple paths). The FTN table is used when an LER receives packets to be forwarded without labels. When an LER receives an IP data packet without labels, the LER matches the destination address of the IP data packet using the maximum matching rule according to the FTN table. If a next hop is found, the LER encapsulates the IP data packet with a label and forwards it.

- ILM

  The ILM table maps each incoming label to a series of NHLFEs (multiple NHLFEs indicate multiple paths). The ILM table is applied when an LSR receives and forwards labeled MPLS packets.

2. MPLS LSP Setup

MPLS nodes can forward packets between each other only after they have reached a consensus on the labels used for the packets and set up an LSP. LSPs can be manually configured or dynamically set up using an MPLS signaling protocol.

- Static LSPs

  Static LSPs are set up by manually distributing labels on MPLS nodes. Static LSPs do not need control packet exchange and consume fewer resources than dynamic LSPs. However, you need to manually configure static LSPs one by one. In addition, static LSPs cannot automatically adapt to network topology changes. Therefore, static LSPs are suitable only for small-scale networks with simple and stable topologies.

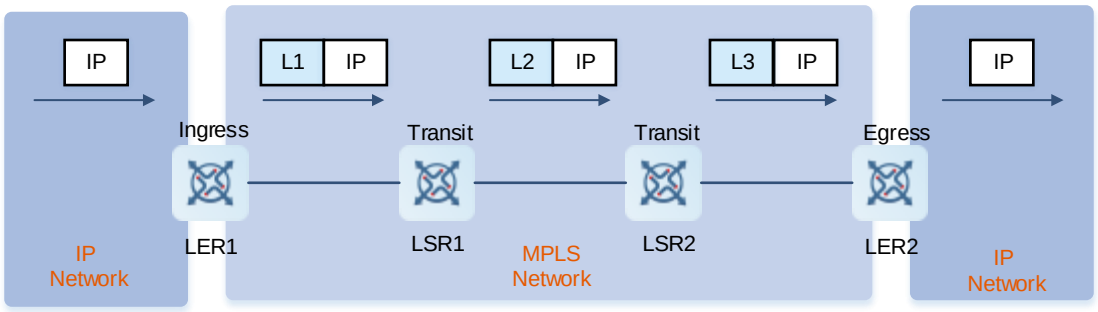
- Dynamic LSPs

  MPLS signaling protocols classify FECs, distribute labels, and set up and maintain LSPs. MPLS signaling protocols include protocols designed specifically for label distribution, such as LDP, and protocols extended to support label distribution, such as Multiprotocol Border Gateway Protocol (MP-BGP).

3. MPLS Packet Forwarding Process

On an MPLS network, the MPLS nodes enable traditional IP routing protocols (such as OSPF and IS-IS) and create IP routing tables. The LDP creates LSPs based on IP routing tables and distributes labels to MPLS nodes.

Figure 1-5 MPLS Packet Forwarding Process



As shown in Figure 1-5, the MPLS packet forwarding process is as follows:

(1) The ingress LER (LER1) receives an IP packet, analyses the packet header, associates it with an FEC, adds label L1 corresponding to the FEC to the packet, and sends the labeled packet to the next-hop LSR through the LSP of Layer 1.

(2) After receiving the labeled packet, the next-hop transit LSR (LSR1) searches the ILM based on the top label L1, replaces L1 with new label L2, and forwards the packet to the next-hop LSR (LSR2).

(3) LSR2 processes the packet similar to LSR1.

(4) After receiving the labeled packet, the egress LER (LER2) pops the label off the packet and forwards the packet based on the IP routing table.

4. PHP

After receiving a labeled packet, the egress LER on an MPLS network needs to search the ILM and pop the label off before forwarding the packet. To reduce the burden of the egress LER, the PHP function is introduced. The PHP function is implemented by assigning a null label. It ensures that labels are popped off on the penultimate LSR. In this case, the egress LER only needs to perform one table lookup. PHP-assigned null labels include explicit and implicit null labels.

- The explicit null label is 0. When the penultimate LSR receives a labeled packet and finds that the outgoing label of the packet is 0 according to the ILM, the penultimate LSR replaces the outermost label of the packet with label 0 and sends the packet to the egress LER. After receiving the packet with label 0, the egress LER pops label 0 off the packet and forwards the packet based on the IP routing table.
- The implicit null label is 3. When the penultimate LSR receives a labeled packet and finds that the outgoing label of the packet is 3 according to the ILM, the penultimate LSR pops the label off and sends the original IP packet to the egress LER. After receiving the original IP packet, the egress LER forwards the packet based on the IP routing table.

5. TTL Processing Mode

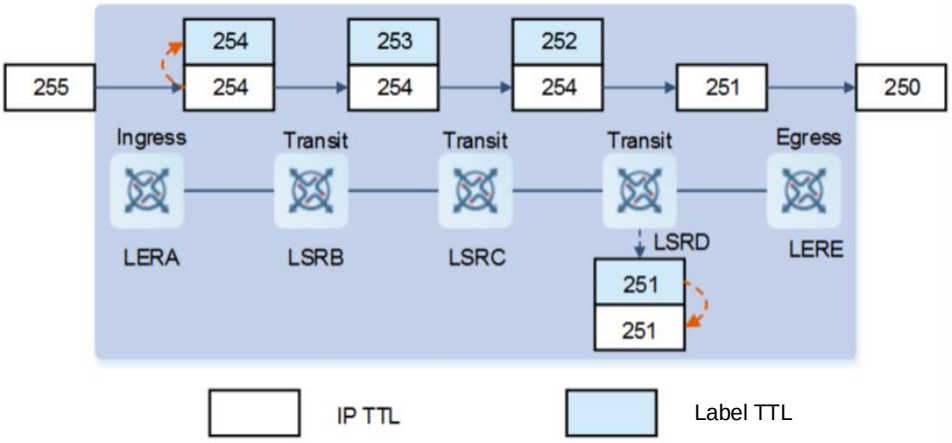
The TTL field in MPLS packets is processed using two modes: Uniform mode and Pipe mode.

- Uniform mode

  When an IP packet enters an MPLS network, the ingress LER pushes a label to the IP packet by decreasing the TTL value of the IP packet by 1 and then copying the TTL value to the TTL field of the new label. The TTL value in the top label is decreased by 1 each time the packet passes through an LSR. When the egress LER pops the label off, it decreases the TTL value in the label by 1 and copies the TTL value to

the TTL field of the IP packet. In Uniform mode, the TTL value of the inner header is not copied but retained if it is smaller than the TTL value of the outer header.

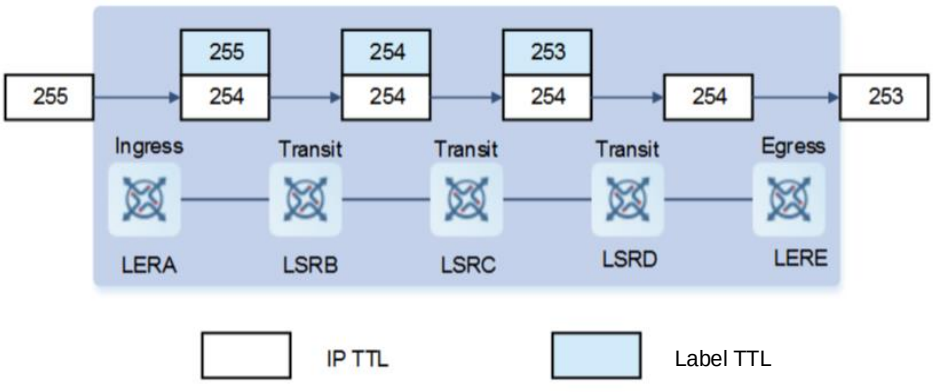
Figure 1-6 Packet Processing in Uniform Mode



- Pipe mode

  When an IP packet enters an MPLS network, the ingress LER pushes a label to the IP packet by decreasing the TTL value in the IP packet by 1 and setting the TTL value in the new label to 255. The TTL value in the top label is decreased by 1 each time the packet passes through an LSR, and the TTL value of the IP packet remains unchanged. When the egress LER pops the label off, it decreases the TTL value of the IP packet by 1.

Figure 1-7 Packet Processing in Pipe Mode



In Pipe mode, a customer edge (CE) can use the tracert tool to trace all nodes that a packet passes through on an MPLS backbone network. To ensure network security, you are advised to use the Pipe mode. In this case, the TTL value of an IP packet is decreased by 1 only at the ingress LER and egress LER regardless of how many hops the packet passes through on an MPLS network. This helps hide the MPLS network structure.

6. LSP Connectivity Test

When a data forwarding fault occurs along an LSP on an MPLS network, the control plane that is responsible for establishing the LSP cannot perceive the fault. This results in complex network maintenance. To reduce the

network maintenance costs and improve the MPLS network availability, two LSP connectivity test tools are introduced, that is, MPLS ping and MPLS traceroute.

Similar to traditional ping and traceroute, LSP connectivity test is based on the echo request and echo reply mode. The only difference is that MPLS ping and MPLS traceroute are implemented based on User Datagram Protocol (UDP) instead of Internet Control Message Protocol (ICMP). Echo requests use UDP port 3503, and only devices with MPLS enabled can identify this port.

- MPLS ping

  MPLS ping is used to check the LSP connectivity. The ingress LER pushes the label of the LSP to be tested to an MPLS Echo Request packet and forwards the packet to the egress LER along the LSP. The egress LER returns an MPLS Echo Reply packet. If the MPLS Echo Reply packet received by the ingress LER is normal, the LSP forwards data normally. If the MPLS Echo Reply packet received by the ingress LER carries an error code, the LSP is faulty.

- MPLS traceroute

  MPLS traceroute is used to trace LSRs between the ingress LER and egress LER. In addition to checking the LSP connectivity, MPLS traceroute can locate the network fault. The ingress LER sends MPLS Echo Request packets continuously along the LSP. Each LSR along the LSP returns an MPLS Echo Reply packet after receiving a Request packet. Therefore, the ingress LER can collect information of each LSR and locate the fault position. In addition, MPLS traceroute can collect labels assigned to LSRs and other important information.

1.1.4 MPLS Static LSPs

To implement basic MPLS forwarding functions, you can statically configure LSPs rather than using the LDP. On each hop of an MPLS network, you can statically configure the incoming and outgoing labels, next hop, and other information to generate an ILM and set up an MPLS LSP, which is called a static LSP.

Note

Static LSP configuration is independent of the LDP and does not rely on IPv4 routes. Even if no IPv4 routes exist on a network, a static LSP takes effect as long as the physical network is reachable.

A static LSP is set up as follows:

(1) Create a static FTN entry (including the outgoing label of the destination network segment and LSP next hop or the outbound interface to the next hop) for an FEC on the ingress LER and bind the FEC to a label. When receiving an IP data packet, the ingress LER queries the FTN table for the next hop using the maximum matching rule based on the destination address of the packet. If a next hop is found, the ingress LER adds the outgoing label of the FEC to the packet, imports the IP traffic to the LSP, and forwards the packet to the specified next hop or through the outbound interface.

(2) Create a static ILM entry (including the outgoing label corresponding to the incoming label and LSP next hop or the outbound interface to the next hop) on the transit LSR and map the incoming label to the outgoing label. When the transit LSR receives a labeled data packet, it queries the ILM table for the next hop based on the label value carried in the packet. If a next hop is found, the transit LSR replaces the label in the packet with the outgoing label corresponding to this label and forwards the packet to the specified next hop or through the outbound interface. If PHP is enabled on the penultimate LSR (that is, the ILM outgoing label on the LSR is the implicit null label 3), the penultimate LSR pops the label off before forwarding the packet.

(3) If the outgoing label of the penultimate LSR is not set to 0 or 3, configure a static ILM entry on the egress LER. The packet received by the egress LER still carries a label value. The egress LER needs to pop the label off based on the ILM entry and forward the packet. If the outgoing label of the penultimate LSR is set to 0 or 3, the egress LER receives a common IP packet and can directly forward it.

1.1.5 MPLS LDP

1. Introduction

LDP is a process of reaching a consensus on the meaning of labels used for traffic transmission between two LSRs. With the LDP, an LSR can map IP routing information to an MPLS LSP and advertise the label binding information to the adjacent LSR to establish a dynamic LSP.

2. Basic Concepts

- LDP peers

  LDP peers are LDP instances on two LSRs that exchange label binding information.

- LDP router ID

  An LDP router ID, that is, an LSR ID, uniquely identifies an LSR in a domain. It is expressed in IPv4 address format. The system router ID is used as the LDP router ID by default. The LDP router ID must be globally unique.

- LDP session

  An LDP session is established between LDP peers to exchange label binding information. Transmission Control Protocol (TCP) connections are used to establish LDP sessions.

3. Working Process

The LDP working process includes three phases: LDP peer discovery and maintenance, LDP session establishment and maintenance, and LSP setup.

- LDP peer discovery and maintenance

  An LDP instance periodically sends Hello packets to advertise itself and monitors the Hello packets to discover LDP peers. If no Hello packet is received from an LDP peer within a specified time, it is regarded that the LDP peer is invalid. This period is called the hold time of Hello packets.

- LDP session establishment and maintenance

  After an LDP instance finds an LDP peer by using Hello packets, the LDP instance establishes a TCP connection based on the transport address advertised in the Hello packets and exchanges initial messages on the connection to negotiate LDP session parameters and establish an LDP session.

  After an LDP session is established, both parties periodically send keepalive packets to monitor the TCP connection. If no keepalive packet is received from the peer within a specified time, the other party regards that the connection is invalid and proactively disconnects the session. This period is called the hold time of keepalive packets.

  To enhance the security of LDP sessions, you can configure the MD5 authentication for the TCP connections used by the LDP sessions.

- LSP setup

  After an LDP session is established, the LDP peers exchange label messages and bind labels to create LSPs for FECs.

LSP setup is in fact the process of binding FECs to labels and notifying adjacent LSRs of the bindings. For details about the LDP implementation process, see RFC 3036.

4. LDP Label Management Policy

LDP label management policies include the label distribution control policy and label reception control policy.

- Label distribution control

  The LDP distributes labels to all valid interior gateway protocol (IGP) routes (excluding BGP routes) by default. In some special situations, you may want to distribute labels only to some routes or only to certain LDP peers. To reduce the device and network burden, you can use the label distribution control policy to reduce the using of labels and the number of LSPs. The label distribution control policy achieves the following effects:

  - The policy distributes label mapping messages only for FECs corresponding to specified IP routes.
  - The policy distributes label mapping messages only to specified LDP peers.
  - The policy achieves both of the preceding two effects at the same time.

- Label reception control

  By default, an LDP instance receives all label mapping messages in LDP sessions regardless of the session mode (DU or DoD). For sessions in DoD mode, the LDP will send label request messages for LDP peers to an LDP peer with this peer as the next hop. The label reception control policy achieves the following effects:

  - The policy receives only label mapping messages of FECs corresponding to specified IP routes from specified peers.
  - The policy sends label request messages of specified FECs only to specified LDP peers.
  - The policy rejects label mapping messages from specified peers.
  - The policy does not send label request messages to specified peers.

5. LSP Traffic Diversion Policy Control

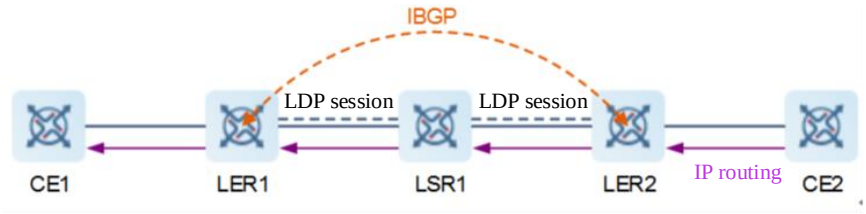
LDP diverts traffic of all valid IGP routes (except BGP routes) to LSPs by default. In some specific situations, LDP diverts traffic of specific routes to reduce the number of LSPs and reduce the workload of devices and the network. Traffic diversion policies can be configured to achieve the following effects:

- Divert traffic only for specific IP routes matched by ACL.
- Divert traffic only for host routes.
- Divert traffic for all routes.
- Do not divert traffic for any routes.

6. Iterating IP Routes to LDP LSPs

The next hop of an IP route is not always directly connected. For example, the next hops between IBGP neighbors are the router IDs of two BGP nodes. Because the network between IBGP neighbors and the BGP routes are isolated, traffic match the BGP routes cannot be directly forwarded to the remote BGP neighbors. In this case, a tunnel needs to be established between IBGP neighbors to ensure that traffic match the route can be forwarded to the remote BGP neighbors through the tunnel. An MPLS LSP is a natural tunnel that can meet this requirement.

Figure 1-8 Iterating IGP Routes to LDP LSPs



As shown in Figure 1-8, LER2 learns the route of CE2 through the IBGP or static routing protocol and advertises the CE2 route to LER1 using IBGP. LER1 releases the CE2 route to CE1. A route entry is generated on LER1 for the CE2 route, and the next hop is the next-hop address advertised by the IBGP neighbor. Because LSR1 does not learn the CE2 route, it cannot forward the traffic from LER1 to CE2 based on IP routing. In this case, an MPLS LSP needs to be set up between LER1 and LER2 to forward traffic from LER1 to LER2. Then, IP routing is performed to send the traffic to CE2.

The process of iterating IP routes to LDP LSPs is as follows:

(1) Set up an LDP LSP. Establish LDP neighbor relationship among LER1, LSR1, and LER2 and set up an LDP LSP. For the detailed process, see 1.1.5 MPLS LDP.

(2) Iterate IP routes to the LDP LSP.

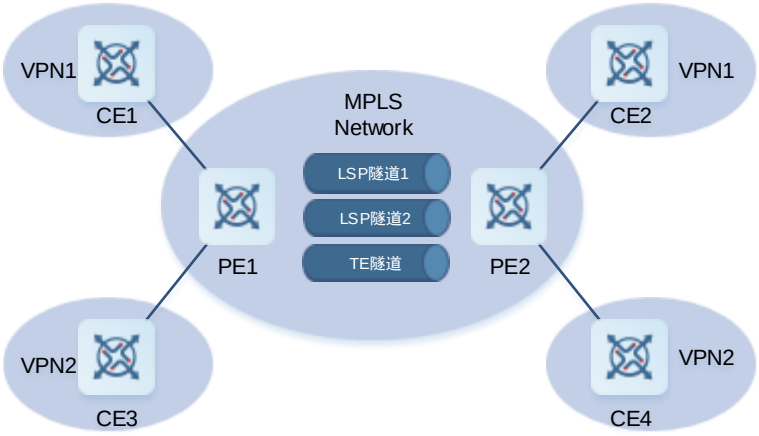
(3) Enable the function of iterating IP routes to LDP LSPs on LER1 to iterate the CE2 route on LER1 to the LDP LSP. To ensure successful iteration, an FTN entry with the IP route next hop as the FEC must exist on LER1.

1.1.6 MPLS Tunnel Policies

Tunnel policies instruct VPN routes to select dependent public network tunnels.

As shown in Figure 1-1, there are two types of labeled tunnels on the MPLS core network: LSP tunnel and TE tunnel. Generally, a common LSP is used as the carrier tunnel for VPN traffic, but the LSP tunnel cannot guarantee the bandwidth. To meet the bandwidth requirements of VPN services, the tunnel selection method can be used to select a TE tunnel. However, one TE tunnel can be selected by different VPNs, so some bandwidth will be consumed by other VPNs.

Figure 1-1 MPLS Labeled Tunnels



1. LSP Tunnel

LSP tunnels are common labeled tunnels established by a label distribution protocol (such as LDP or BGP) to IP unicast routes.

2. GRE Tunnel

GRE tunnels are common IP tunnels. Generally, the MPLS network is rarely deployed in the public network environment, and VPN cannot traverse the IP public network. A binding policy for a tunnel policy can implement VPN over GRE to allow VPN to traverse the IP public network.

3. Tunnel Selection Method

The tunnel selection method is used on the MPLS core network. You can configure tunnel priorities based on which VPN services select public network tunnels. LSP tunnels and MPLS TE tunnels are available for selection. Tunnels of a type with high priority are selected preferentially by VPN routes.

1.1.7 GTSM

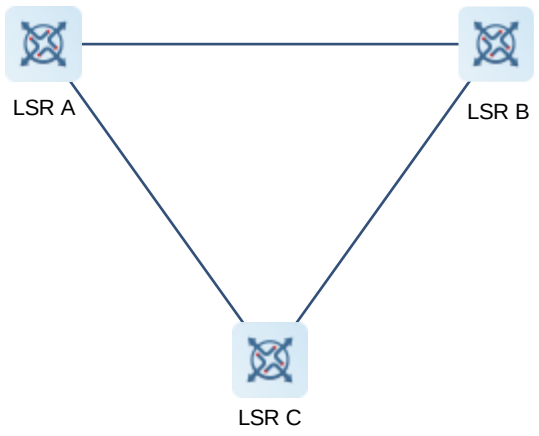
To improve the security of LDP sessions, you can configure GTSM for LDP sessions.

Basic principles of GTSM: In common public networks, LDP sessions are usually established between directly connected neighbors. In this case, the IP TTL value of received LDP packets remains unchanged (the packet is not forwarded, so the value does not decrease by 1). That is, if the TTL value is set to 255 when a packet is sent, the device receiving the packet can determine whether the packet is sent by a directly connected neighbor by checking whether the TTL value is still 255. In addition to LDP, you can apply GTSM to most network protocols that are established between directly connected neighbors, effectively defending against denial of service (DoS) attacks from remote devices.

Because GTSM is simple and robust (the TTL value cannot be forged), LDP IPv4 can support GTSM through a simple add-on. Considering compatibility, if you want to enable GTSM for LDP IPv4 sessions, both session parties need to support GTSM (see the negotiation mechanism in RFC 6720). In addition, the TTL value is set to 1 when an IPv4 link Hello packet is sent, so IPv4 link Hello packets do not support GTSM.

Considering the robustness of GTSM, if GTSM is performed based on the rule of directly connected neighbors (that is, the TTL value must be 255 when a packet is received), the LDP-IGP synchronization mechanism may fail, as shown in the following topology.

Figure 1-9 GTSM



In LDP-IGP synchronization, if the link between LSRA and LSRB recovers, IGP suppresses traffic transmission through the direct link before the session between LSRA and LSRB is established. As a result, the TCP unicast packets between LSRA and LSRB are transmitted along the LSRA-LSRC-LSRB link. When the packets arrive, the TTL value is 254 and the packets are filtered out by GTSM. As a result, the session cannot be established, and IGP continues to suppress traffic on the link. (Note that link Hello packets are multicast packets and are not affected by IGP routes. They are still transmitted over direct links.)

To address the preceding issue, disable GTSM during device running or relax the protection conditions (for example, you can set the hop count of the preceding topology to two so that packets with a TTL value of 255 or 254 are not filtered out).

In summary, LDP requires GTSM in the following scenario:

- You can enable or disable GTSM for IPv4 sessions separately. After GTSM is enabled, the TTL value is set to 255 when a packet is sent, and GTSM check is performed on the received packet. The destination port number is 646, the source address is the IPv4 address of the session peer, the destination address is the IPv4 address of the local device of the session, and the packet is an IPv4 TCP packet. The packet is discarded if the TTL value of the matched packet is smaller than the specified value (255 by default).

1.1.8 Protocols and Standards

- RFC 3032: MPLS Label Stack Encoding
- RFC 3036: LDP Specification
- RFC 4182: Removing a Restriction on the use of MPLS Explicit NULL
- RFC 5283: LDP Extension for Inter-Area Label Switched Paths (LSPs)

1.2 Restrictions and Guidelines

- MPLS interface-related commands can be configured on Layer 3 interfaces only. Non-Layer 3 interfaces can configure MPLS related commands only after they are converted to Layer 3 interfaces.
- On some platforms, if an MPLS signaling protocol, such as LDP is enabled when MPLS forwarding is disabled globally, IP packet forwarding may be invalid. If MPLS forwarding is not required, you are advised to disable the related MPLS signaling protocol at the same time.

1.3 Configuration Task Summary

MPLS configuration includes the following tasks:

(1) Configuring a Static LSP

(2) Configuring Basic LDP Functions

(3) (Optional) Configuring an LDP LSP

(4) Iterating IP Routes to LDP LSPs

(5) (Optional) Configuring LSP Connectivity Detection

(6) Configuring LSP Connectivity Detection

(7) Configuring GTSM

1.4 Configuring MPLS Public Functions

1.4.1 Configuration Tasks

MPLS public function configuration includes the following tasks:

(1) Configuring MPLS Forwarding

(2) (Optional) Configuring the MPLS MTU for an Interface

(3) (Optional) Configuring the Processing Method for ICMP Error Messages

(4) (Optional) Configuring an MPLS TTL Processing Mode

(5) (Optional) Configuring DiffServ Mode for MPLS Penultimate Hop

1.4.2 Configuring MPLS Forwarding

1. Overview

After MPLS forwarding is enabled, a device preferentially forwards packets according to their labels. If packet forwarding based on labels fails, the device then attempts to forward the packets according to their IP addresses.

2. Restrictions and Guidelines

- Unless otherwise specified, enable MPLS forwarding globally on each LSR that an LSP passes through.
- Unless otherwise specified, enable MPLS forwarding on each interface that an LSP passes through.
- When labeled MPLS packet forwarding is enabled on an interface, adjust the maximum transmission unit (MTU) on the interface based on the service type. Otherwise, transmission of large packets may be affected.
- This feature controls MPLS incoming label map (ILM) entry forwarding on an inbound interface but not an outbound interface.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enable MPLS forwarding globally.

mpls enable

MPLS forwarding is disabled globally by default.

To implement MPLS forwarding on a device, enable MPLS forwarding globally first.

(4) Enter the interface configuration mode.

- Enter the Layer 3 Ethernet interface configuration mode.

  interface *ethernet-type interface-number*

- Enter the Layer 3 link aggregation configuration mode.

  interface aggregateport *interface-number*

- Enter the Layer 3 Ethernet subinterface configuration mode.

  interface ethernet-type *interface-number.subnumber*

- Enter the Layer 3 aggregated subinterface configuration mode.

  interface aggregateport i*nterface-number.subnumber*

(5) Enable an interface to forward labeled MPLS packets.

label-switching

Labeled MPLS packet forwarding is disabled on an interface by default.

1.4.3 Configuring the MPLS MTU for an Interface

1. Overview

The MPLS MTU determines whether MPLS packets need be fragmented when being forwarded. The MPLS MTU indicates the overall length of the MPLS encapsulation and encapsulated (such as IP) layers. Devices that support MPLS packet fragmentation will fragment MPLS packets based on the MPLS MTU of an interface when the packet length is longer than the MPLS MTU of the interface after MPLS label encapsulation. Devices that do not support MPLS packet fragmentation will discard packets whose length is longer than the MTU of an interface after MPLS label encapsulation.

2. Restrictions and Guidelines

- The **mpls mtu** command is used to configure an interface MTU for MPLS packets. When you run the **mtu-check-mode ip slot** *slot-id* command, the MPLS MTU contains the length of the encapsulated layer (such as IP) but not the MPLS encapsulation layer. When you run the **mtu-check-mode label-contained-length slot** *slot-id* command, the MPLS MTU is the sum of the MPLS encapsulation layer length and the encapsulated layer (such as IP) length.
- The **mpls mtu** command is valid to outgoing traffic but not incoming traffic.
- You can run the **mpls path-mtu independent** command to determine whether the MPLS MTU takes effect independently. (The smaller one between the IP MTU and MPLS MTU is used by default.)
- When you run the **interface range** command to configure an MPLS MTU for interfaces in a batch, the maximum value of *mpls-mtu* is the largest MTU of all the interfaces.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) (Optional) Enable the MPLS MTU to take effect independently.

mpls path-mtu independent

The MPLS MTU does not take effect independently by default.

(4) (Optional) Configure an interface MTU check method.

mtu-check-mode { **ip** | **label-contained-length** } **slot** *slot-id*

The device checks the interface MTU based on the IP packet length by default.

(5) Enter the interface configuration mode.

- Enter the Layer 3 Ethernet interface configuration mode.

interface *ethernet-type interface-number*

- Enter the Layer 3 link aggregation configuration mode.

  interface aggregateport interface-number

- Enter the Layer 3 Ethernet subinterface configuration mode.

  interface ethernet-type interface-number.subnumber

- Enter the Layer 3 aggregated subinterface configuration mode.

  interface aggregateport interface-number.subnumber

- Enter the loopback interface configuration mode.

  interface loopback

(6) Configure the MPLS MTU for an interface.

mpls mtu *mpls-mtu*

The MTU of MPLS packets that can be transmitted by an interface is the same as the MTU of the interface by default.

1.4.4 Configuring the Processing Method for ICMP Error Messages

1. Overview

Configure the processing method for Internet Control Message Protocol (ICMP) error messages (such as typical MPLS TTL timeout messages) generated during the forwarding of MPLS packets. ICMP error messages are encapsulated with the original label stack and forwarded along the original LSP to the egress LER by default. The egress LER pops the label stack off and selects a route based on the IP addresses to forward the messages. However, you can specify the number of labels carried in packets to be forwarded to process ICMP error messages in different ways.

- When the number of labels carried in packets to be forwarded is greater than the configured label quantity, ICMP error messages are forwarded along the LSP of the original label stack.
- When the number of labels carried in packets to be forwarded is less than or equal to the configured label quantity, ICMP error messages are forwarded according to the IP routing table where the FEC corresponding to the top label resides.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure the processing method for ICMP error messages generated during the forwarding of MPLS packets.

mpls icmp-error pop *labels*

ICMP error messages are encapsulated with the original label stack and forwarded along the original LSP by default.

1.4.5 Configuring an MPLS TTL Processing Mode

1. Overview

You can configure an MPLS TTL processing mode to control transmission of the TTL value between the IP packet header and the label stack. MPLS provides two modes for TTL processing: Uniform and Pipe.

2. Configuring a TTL Processing Mode for MPLS LDP

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure a TTL processing mode for MPLS LDP.

mpls ttl-mode ldp { **pipe** | **uniform** }

The TTL processing mode for MPLS LDP is Uniform by default.

3. Configuring a TTL Processing Mode for Explicit Null Labels

(2) Enter the privileged EXEC mode.

enable

(1) Enter the global configuration mode.

configure terminal

(2) Configure a TTL processing mode for explicit null labels.

mpls ttl-mode explict-null-label { **pipe** | **uniform** }

The TTL processing mode for explicit null labels is Uniform by default.

4. Configuring a TTL Copy Mode for the BGP LSP Egress Node

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure a TTL copy mode for the BGP LSP egress node.

mpls ttl-mode bgp-egress { **pipe** | **uniform** }

The TTL copy mode for the BGP LSP egress node is Uniform by default.

1.4.6 Configuring DiffServ Mode for MPLS Penultimate Hop

1. Overview

Configure the DiffServ mode for MPLS penultimate hop:

- When the MPLS DiffServ mode is set to Pipe, the EXP field in outer labels is not copied to inner labels.
- When the MPLS DiffServ mode is set to Uniform, the EXP field in outer labels is copied to inner labels.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure the Uniform/Pipe mode for the MPLS penultimate hop.

mpls lsp exp-type { **pipe** | **uniform** }

The MPLS DiffServ mode on the MPLS penultimate hop is Uniform by default.

1.5 Configuring a Static LSP

1.5.1 Overview

To implement basic MPLS forwarding functions, you can configure static LSPs. Static LSP configuration is independent of the LDP and does not rely on IPv4 routes. Even if no IPv4 routes exist on the network, a static LSP takes effect as long as the physical network is reachable.

On the ingress LER, set up an FTN entry for an FEC, that is, bind the FEC to a label. On the transit LSRs, configure ILM entries to map incoming labels to outgoing ones to forward labeled packets based on labels. On the penultimate LSR, enable PHP. In this case, the ILM entry of the penultimate LSR is different from other transit LSRs. The outgoing label of the penultimate LSR must be implicit null label 3.

1.5.2 Restrictions and Guidelines

- For two adjacent LSRs, the outgoing label of the upstream LSR must be the same as the incoming label of the downstream LSR.
- LSP is a unidirectional path. Therefore, you need to configure static LSPs in both data transmission directions.
- The static FTN entry with the outgoing label set to 3 takes effect only after an IP route with the same prefix as the FTN entry is configured.
- An FTN entry with the destination address and mask set to 0 takes effect when the corresponding default route exists in the IP routing forwarding table.
- It is recommended that the outgoing label of the penultimate LSR be set to 3. In this case, the egress LER can directly receive IP packets. Otherwise, the egress LER needs to configure the corresponding static ILM entry.

1.5.3 Prerequisites

- MPLS forwarding has been configured on all LSRs.
- MPLS forwarding has been enabled globally and on an interface.

1.5.4 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure a static FTN entry on the ingress LER.

mpls static ftn *ipv4-address*/*mask-length* **out-label** *label* **nexthop** *interface-type interface-number nexthop-ipv4-address*

No static FTN entry is configured by default.

To import IP traffic to an LSP, an ingress LER must be configured with an FTN entry.

(4) Configure static ILM entries on transit LSRs. Configure one of the following tasks.

- Configure static ILM entries applied to L3VPN.

  (IPv4 network)

  mpls static ilm in-label *in-label* **forward-action pop-l3vpn-nexthop** *vrf-name* **nexthop** *interface-type interface-number nexthop-ipv4-address* **fec** *ipv4-address*/*mask-length*

- Configure static ILM entries applied to the public network.

  (IPv4 network)

  mpls static ilm in-label *in-label* **forward-action swap-label** *swap-label* **nexthop** *interface-type interface-number nexthop-ipv4-address* **fec** *ipv4-address*/*mask-length*

A transit LSR can forward MPLS packets only after an ILM entry is configured on it.

1.6 Configuring Basic LDP Functions

1.6.1 Overview

An LDP session can be established between adjacent LSRs to switch label bindings.

1.6.2 Configuration Tasks

The configuration of LDP basic functions includes the following tasks:

(1) Enabling LDP Globally

(2) (Optional) Configuring the LDP Router ID

(3) Enabling LDP on an Interface

(4) (Optional) Configuring the Transport Address

(5) Configuring an LDP Remote Peer

(6) Configuring Targeted Hello Packet Receiving on an LDP Instance

(7) Configuring the Time Interval for Hello Packets

(8) (Optional) Configuring the Hold Time of Hello Packets

(9) (Optional) Configuring the Hold Time of Keepalive Packets

(10) (Optional) Configuring the Maximum PDU

(11) (Optional) Configuring LDP MD5 Authentication

1.6.3 Enabling LDP Globally

1. Restrictions and Guidelines

- LDP needs to be enabled globally on the LSRs at both ends of an LDP session.
- The number of LDP instances supported on a device is limited by the number of VPN Routing and Forwarding (VRF) tables on the device. Each VRF instance can start an LDP instance.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enable LDP globally and enter the LDP configuration mode.

mpls router ldp [*vrf-name*]

LDP is disabled by default.

If no VRF instance is specified, LDP is enabled or disabled for the global VRF instance by default.

1.6.4 Configuring the LDP Router ID

1. Restrictions and Guidelines

- In actual applications, the LDP router ID needs to be configured. If the LDP router ID is not configured, LDP may use the router ID elected by the current device as the LSR ID for communication by default. If the remote device does not have a route to this LSR ID, the LDP session cannot be established and the router ID may be changed after the LDP is restarted, resulting in invalidity of some functions, for example, LDP MD5 authentication configured using the original router ID.
- It is recommended that the router ID be configured on LSRs at both ends of a session to ensure stable and reliable LDP functions.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the LDP configuration mode.

mpls router ldp [*vrf-name*]

(4) Configure the LDP router ID.

ldp router-id { *ipv4-address* | **interface** *interface-type interface-number* [**force**] }

The system router ID is used as the LDP router ID by default.

If **force** is specified, the new router ID is forced to take effect immediately. Otherwise, the system prompts that the current operation may cause LDP session re-establishment and asks whether you want to modify the router ID.

1.6.5 Enabling LDP on an Interface

1. Restrictions and Guidelines

If a local LDP session is established, enable LDP on an interface in interface configuration mode.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

- Enter the Layer 3 Ethernet interface configuration mode.

  interface *ethernet-type interface-number*

- Enter the Layer 3 link aggregation configuration mode.

  interface aggregateport *interface-number*

- Enter the Layer 3 Ethernet subinterface configuration mode.

  interface ethernet-type *interface-number.subnumber*

- Enter the Layer 3 aggregated subinterface configuration mode.

  interface aggregateport *interface-number.subnumber*

(4) Enable LDP on an interface.

mpls ldp enable

LDP is disabled on an interface by default.

1.6.6 Configuring the Transport Address

1. Restrictions and Guidelines

- If a local LDP session is established, you can configure the global transport address in LDP configuration mode. If a neighbor requires a specified transport address, configure the specified transport address on the interface connected to the neighbor.
- If a remote LDP session is established, no transport address needs to be configured.
- You can use the primary address of an interface or specify an IP address as the transport address to set up an LDP session on the interface. There are two configuration methods. Use the transport address configuration command in interface configuration mode or use the command in LDP configuration mode to globally configure a transport address for all LDP sessions.
- The global transport address configuration command for local LDP sessions takes effect only to local LDP sessions established using the LDP basic discovery mechanism. It is invalid to remote LDP sessions established using the LDP extended discovery mechanism. Remote LDP sessions always use the LDP router ID as the transport address.
- The transport address configuration command for local LDP sessions on an interface takes effect only to local LDP sessions established using the LDP basic discovery mechanism. It is invalid to remote LDP sessions established using the LDP extended discovery mechanism. The transport address configuration command on an interface takes effect only to local LDP sessions established after this command is configured. It is invalid to previously established local LDP sessions. If a transport address is configured on an interface and globally, the transport address configured on the interface takes effect preferentially.

2. Prerequisites

For the configuration of a transport address for LDP peers, a reachable IP route is required. You can configure a static route in global configuration mode or establish a route using an IGP, such as OSPF.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the LDP configuration mode.

mpls router ldp [*vrf-name*]

(4) Configure a global transport address for local LDP sessions.

transport-address { **interface** | *ipv4-address* | *interface-type interface-number* }

The LDP router ID is used as the LDP session transport address by default.

(5) Exit the LDP configuration mode.

exit

(6) Enter the interface configuration mode.

- Enter the Layer 3 Ethernet interface configuration mode.

  interface *ethernet-type interface-number*

- Enter the Layer 3 link aggregation configuration mode.

  interface aggregateport interface-number

- Enter the Layer 3 Ethernet subinterface configuration mode.

  interface ethernet-type interface-number.subnumber

- Enter the Layer 3 aggregated subinterface configuration mode.

  interface aggregateport interface-number.subnumber

(7) Configure the transport address for local LDP sessions on an interface.

mpls ldp transport-address { **interface** | *ipv4-address* }

The LDP router ID is used as the LDP session transport address by default.

1.6.7 Configuring an LDP Remote Peer

1. Overview

Create an LDP remote peer.

2. Restrictions and Guidelines

To establish a remote LDP session, you must configure remote peers in LDP configuration mode.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the LDP configuration mode.

mpls router ldp [*vrf-name*]

(4) Configure an LDP remote peer.

neighbor *ipv4-address*

No LDP remote peer is configured by default.

1.6.8 Configuring Targeted Hello Packet Receiving on an LDP Instance

1. Restrictions and Guidelines

When you configure two devices as remote peers, you can configure **neighbor** on one end and enable targeted Hello packet receiving on the other end. To delete remote peers, you only need to delete the **neighbor** configuration.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the LDP configuration mode.

mpls router ldp [*vrf-name*]

(4) Configure targeted Hello packet receiving on an LDP instance.

discovery targeted-hello accept [**from** *acl-name*]

An LDP instance receives targeted Hello packets only from remote peers by default.

Only targeted Hello packets from neighbors that meet access control list (ACL) rules will be received.

1.6.9 Configuring the Time Interval for Hello Packets

1. Restrictions and Guidelines

- If a local LDP session is established, configure the time interval for Hello packets in interface configuration mode.
- If a remote LDP session is established, configure the time interval for Hello packets in LDP configuration mode.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

- Enter the Layer 3 Ethernet interface configuration mode.

  interface *ethernet-type interface-number*

- Enter the Layer 3 link aggregation configuration mode.

interface aggregateport interface-number

(4) Configure the interval for sending link Hello packets.

mpls ldp hello-interval *hello-interval*

The default interval for sending link Hello packets is 5s.

(5) Enter the LDP configuration mode.

mpls router ldp [*vrf-name*]

(6) Configure the interval for sending targeted Hello packets.

discovery targeted-hello interval *targeted-hello-interval*

The default interval for sending targeted Hello packets in the extended LDP discovery mechanism is 1/9 of the hold time of the packets, that is, 5s.

1.6.10 Configuring the Hold Time of Hello Packets

1. Restrictions and Guidelines

- If a local LDP session is established, configure the hold time of Hello packets in interface configuration mode.
- If a remote LDP session is established, configure the hold time of Hello packets in LDP configuration mode.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

- Enter the Layer 3 Ethernet interface configuration mode.

  interface *ethernet-type interface-number*

- Enter the Layer 3 link aggregation configuration mode.

  interface aggregateport interface-number

- Enter the Layer 3 Ethernet sub-interface configuration mode.
  interface *ethernet-type interface-number.subnumber*

- Enter the Layer 3 aggregate sub-interface configuration mode.
  interface aggregateport *interface-number.subnumber*

(4) Configure the hold time of link Hello packets.

mpls ldp hello-holdtime *hello-holdtime*

The default hold time of link Hello packets is 15s.

(5) Enter the LDP configuration mode.

mpls router ldp [*vrf-name*]

(6) Configure the hold time of targeted Hello packets.

discovery targeted-hello holdtime *targeted-hello-holdtime*

The default hold time of targeted Hello packets is 45s.

1.6.11 Configuring the Hold Time of Keepalive Packets

1. Restrictions and Guidelines

- If a local LDP session is established, configure the hold time of keepalive packets in interface configuration mode.
- If a remote LDP session is established, configure the hold time of keepalive packets in LDP configuration mode.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

- Enter the Layer 3 Ethernet interface configuration mode.

  interface *ethernet-type interface-number*

- Enter the Layer 3 link aggregation configuration mode.

  interface aggregateport interface-number

- Enter the Layer 3 Ethernet sub-interface configuration mode.
  interface *ethernet-type interface-number.subnumber*

- Enter the Layer 3 aggregate sub-interface configuration mode.
  interface aggregateport *interface-number.subnumber*

(4) Configure the hold time of keepalive packets in local LDP sessions on an interface.

mpls ldp keepalive-holdtime *keepalive-holdtime*

The default hold time of keepalive packets on an interface is 45s. The default interval for sending keepalive packets is one third of the hold time.

(5) Enter the LDP configuration mode.

mpls router ldp [*vrf-name*]

(6) Configure the hold time of keepalive packets in remote LDP sessions.

targeted-session holdtime*hold-time*

The default hold time of keepalive packets in remote LDP session established using the LDP extended discovery mechanism is 180s, and the interval for sending keepalive packets is one third of the hold time.

1.6.12 Configuring the Maximum PDU

1. Overview

The messages exchanged between LDP devices are all contained in protocol data units (PDUs). This function allows you to specify the maximum PDU length allowed for each LDP message.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

- Enter the Layer 3 Ethernet interface configuration mode.

  interface *ethernet-type interface-number*

- Enter the Layer 3 link aggregation configuration mode.

  interface aggregateport interface-number

- Enter the Layer 3 Ethernet sub-interface configuration mode.
  interface *ethernet-type interface-number.subnumber*

- Enter the Layer 3 aggregate sub-interface configuration mode.
  interface aggregateport *interface-number.subnumber*

(4) Configure the maximum PDU length.

mpls ldp max-pdu *max-pdu*

The maximum PDU length allowed for each LDP message is 4096 bytes by default.

1.6.13 Configuring LDP MD5 Authentication

1. Overview

To enhance the security of LDP sessions, you can configure LDP-MD5 authentication on LSRs at both ends of an LDP session.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the LDP configuration mode.

mpls router ldp [*vrf-name*]

(4) Configure a device to adopt MD5 authentication for the TCP connections with its peer.

neighbor *ipv4-address* **password** [**0** | **7**] *password-string*

The LDP MD5 authentication function is disabled by default.

1.6.14 Enabling LDP to Delay Label Mapping

1. Overview

Enabling LDP to delay label mapping can improve the LDP entry processing capability. This capability prevents repeated addition and deletion of downstream-related entries during route update through delayed processing of label mapping information.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the LDP configuration mode.

mpls router ldp [*vrf-name*]

(4) Enable LDP to delay label mapping.

route wait label-mapping *wait-time*

LDP does not delay label mapping by default.

1.7 Configuring an LDP LSP

1.7.1 Overview

Set up an LSP for an IPv4 unicast route by using LDP.

1.7.2 Restrictions and Guidelines

The LDP needs to use existing unicast routes on the network. Therefore, IP unicast routes must be configured on the network.

1.7.3 Configuration Tasks

All the configuration tasks below are optional. Select them based on your requirement. LDP LSP configuration includes the following tasks:

(1) Configuring LDP Loop Detection

(2) Configuring a Label Distribution Policy for an LDP Instance

(3) Configuring a Label Reception Policy for an LDP Instance

1.7.4 Configuring LDP Loop Detection

1. Overview

Loop detection will affect the parameters in the interaction packets during Session Init.

2. Restrictions and Guidelines

If an IP route is statically configured instead of being dynamically generated by using IGP, you are advised to enable the loop detection function on all LSRs that an LSP passes through to prevent loops caused by incorrect configuration.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the LDP configuration mode.

mpls router ldp [*vrf-name*]

(4) Enable loop detection.

loop-detection

Loop detection is disabled by default.

(5) Exit the LDP configuration mode and return to the global configuration mode.

exit

(6) Enter the interface configuration mode.

- Enter the Layer 3 Ethernet interface configuration mode.

  interface *ethernet-type interface-number*

- Enter the Layer 3 link aggregation configuration mode.

  interface aggregateport interface-number

- Enter the Layer 3 Ethernet sub-interface configuration mode.
  interface *ethernet-type interface-number.subnumber*

- Enter the Layer 3 aggregate sub-interface configuration mode.
  interface aggregateport *interface-number.subnumber*

(7) Configure the maximum number of hops allowed for loop detection.

mpls ldp max-hop-count *max-hop-count*

The maximum number of hops allowed for loop detection on an interface is 254 by default.

(8) Configure the maximum path vector value allowed for loop detection on an interface.

mpls ldp max-path-vector *number*

The maximum path vector value allowed for loop detection on an interface is 254 by default.

1.7.5 Configuring a Label Distribution Policy for an LDP Instance

1. Overview

Configure a policy for distributing labels to IP route FECs.

2. Restrictions and Guidelines

- You can run the **advertise-labels for bgp-routes** command to enable the function of distributing labels to BGP routes.
- You can run the **advertise-labels for host-routes** command to configure the device to process only the FECs of host IP routes.
- LDP processes FECs of host IP routes and distributes all the labels to all LDP peers by default.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the LDP configuration mode.

mpls router ldp [*vrf-name*]

(4) Configure a label distribution policy.

advertise-labels for { **acl** *acl-name* [**to** *peer-acl-name*] | **bgp-routes** [**acl** *bgp-routes-acl-name*] | **host-routes** }

By default, LDP distributes labels to host IP routes but not IGP routes, distributes all the labels to all LDP peers, but does not add FTN entries to BGP routes.

1.7.6 Configuring a Label Reception Policy for an LDP Instance

1. Restrictions and Guidelines

- The **neighbor** command takes effect only to label mapping messages with IP route FECs. It is invalid to other types of FECs, such as pseudo wire (PW) FECs.
- After an ACL rule for incoming label mapping messages is configured by running the **neighbor** command, an LDP instance receives FEC-label mapping messages that come from specified neighbors and meet the ACL rule, and discards FEC-label messages not meeting the ACL rule. However, the LDP instance can receive label mapping messages from other neighbors.
- If the **neighbor** command is configured for a neighbor but no ACL rule is specified, the LDP instance discards all FEC-label mapping messages sent from the neighbor. After an ACL rule is canceled by running the **no** form of the **neighbor** command, FEC-label mapping messages that have been discarded based on the ACL rule cannot be re-obtained, and only newly received FEC-label mapping messages are affected. You need to run the **clear mpls ldp neighbor** command to reset the LDP session to restore it to the normal status.
- Only one rule can be configured for each neighbor, and the newly configured rule will overwrite the existing one.
- Each LDP instance can configure ACL rules for a maximum of 64 neighbors.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the LDP configuration mode.

mpls router ldp [*vrf-name*]

(4) Configure a label reception policy.

neighbor *ipv4-address* **labels accept** *acl-name*

No ACL rule is configured by default.

The configured policy applies only to standard and extended IP ACLs.

1.7.7 Configuring a Label Distribution Policy for the Penultimate Hop

1. Restrictions and Guidelines

A policy for distributing explicit null labels can be configured only for global LDP instances. This function is not supported on VRF instances.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the LDP configuration mode.

mpls router ldp [*vrf-name*]

(4) Distribute labels to IP route prefixes on the penultimate hop.

php-mode { **explicit** | **implicit** }

Implicit null labels are distributed to IP route prefixes on the penultimate hop by default.

1.8 Iterating IP Routes to LDP LSPs

1.8.1 Overview

Iterate non-direct IP routes to LDP LSPs to forward traffic to the remote ends through the LSPs.

1.8.2 Restrictions and Guidelines

- The FEC of an LDP LSP to which an IP route is iterated must be a host route.
- The function of iterating IP routes to LDP LSPs needs to be enabled only on the LERs and does not need to be enabled on the LSRs.
- All IP routes can be iterated, including but not limited to static routes and BGP routes.

1.8.3 Prerequisites

- LDP is configured in global configuration mode.
- LDP is enabled on each LSR that an LSP passes through.
- MPLS forwarding is enabled on each interface that an LSP passes through.
- (Optional) A remote peer is configured to establish an extended LDP session.

1.8.4 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Iterate IP routes to LDP LSPs.

recursive-route to mpls

The function of recurring and iterating IP routes to LDP LSPs is disabled by default.

1.9 Configuring LSP Connectivity Detection

1.9.1 Overview

In an MPLS network, common LSP connectivity detection tools include MPLS ping and MPLS traceroute. MPLS ping is used to manually detect the connectivity of an LSP. MPLS traceroute is used to trace LSRs between the ingress LER and egress LER. In addition to detecting LSP connectivity, MPLS traceroute can locate the network fault.

1.9.2 Restrictions and Guidelines

Both **ping mpls** and **traceroute mpls** support the following two parameter specification methods:

- Enter a command with specified parameters.
- Enter **ping mpls** or **traceroute mpls** and press **Enter** to enter the interactive input mode and then specify parameters.

1.9.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Detect the connectivity of an MPLS LSP.

ping mpls ipv4 *ipv4-address/mask-length* [**destination** *destination-ipv4-address* | **exp** *exp-value* | **flags fec** | **force-explicit-null** | **interval** *interval* | **nexthop** *nexthop-ipv4-address* | **nil-fec** | **pad** *pattern* | **repeat** *repeat-count* | **reply mode** { **no-reply** | **router-alert** | **udp** } | **size** *size* | **source** *source-ipv4-address* | **timeout** *timeout* | **ttl** *time-to-live* | **verbose**] *

(3) Trace the MPLS nodes that an LSP passes through.

traceroute mpls ipv4 *ipv4-address/mask-length* [**ddmap** | **destination** *destination-ipv4-address* | **exp** *exp-value* | **flags fec** | **force-explicit-null** | **nexthop** *nexthop-ipv4-address* | **nil-fec** | **pad** *pattern* | **reply mode** { **no-reply** | **router-alert** | **udp** } | **size** *size* | **source** *source-ipv4-address* | **timeout** *timeout* | **ttl** *time-to-live*] *

1.10 Configuring an MPLS Tunnel Policy

1.10.1 Overview

Set up public network tunnels.

1.10.2 Restrictions and Guidelines

- The MPLS forwarding capability must be enabled globally and on interfaces of the ingress and egress devices of a tunnel.
- When the TE tunnel binding method is used, you must specify the TE tunnel for VPN binding.

1.10.3 Configuration Tasks

The LDP basic feature configuration includes the following tasks:

- Configuring a Tunnel Policy

- Configuring and Applying a Tunnel Policy Method
- Configuring a Tunnel Selection Policy

1.10.4 Configuring a Tunnel Policy

1. Restrictions and Guidelines

- Generally, tunnel policies are configured on PEs.
- A tunnel policy name uniquely identifies a tunnel policy.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Create a tunnel policy.

tunnel-policy *policy-name*

No tunnel policy is created by default. The value of *policy-name* is a string of 1 to 31 case-sensitive characters, including letters, digits, or symbols (excluding spaces).

1.10.5 Configuring and Applying a Tunnel Policy Method

1. Restrictions and Guidelines

- Generally, a tunnel policy method is configured and applied to a PE.

1.10.6 Configuring a Tunnel Selection Policy

1. Overview

The tunnel selection method is used on the MPLS core network.

2. Restrictions and Guidelines

- If a VPN service does not need bandwidth assurance, select a common LSP tunnel preferentially when you deploy this VPN service to reduce the cost.
- If a VPN service requires certain control on the traffic (such as the path for the traffic) but does not need bandwidth assurance, select a TE tunnel preferentially when you deploy this VPN service.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the tunnel policy configuration mode.

tunnel-policy *policy-name*

(4) Configure a tunnel selection policy.

tunnel select { **ipv6** { **srv6-policy** | **srv6-policy-group** }* | **lsp** [**loadbalance** *loadbalance-number*] }

No tunnel selection policy is configured by default.

1.11 Configuring GTSM

1.11.1 Configuration Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the LDP configuration mode.

mpls router ldp [*vrf-name*]

(4) Configure the GTSM hop count for a specified LDP session.

neighbor ipv4-address **valid-hops** hops

By default, no hop count is configured for an LDP session. That is, GTSM does not take effect on LDP sessions.

1.12 Enabling MPLS-related Trap Switches

1.12.1 Overview

Simple Network Management Protocol (SNMP) is used for network monitoring and management. Network administrators can use SNMP to perform information query, network configuration, fault locating, and capacity planning for network nodes. SNMP exchanges information between a network management system (NMS) and an agent and defines six operation types, one of which is trap. The trap operation means that the agent actively sends a packet to inform the NMS of the situation occurs on the agent.

To use the trap function, you need to enable MPLS-related trap switches.

1.12.2 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enable MPLS-related trap switches.

snmp-server enable traps mpls l3vpn [**max-thresh-cleared** | **max-threshold** | **mid-threshold** | **vrf-down** | **vrf-up**] *

snmp-server enable traps mpls ldp [**pv-limit** | **session-down** | **session-up**] *

No MPLS trap is sent by default.

1.13 Monitoring

Run the **show** commands to check the running status of a configured function to verify the configuration effect.

Run the **clear** commands to clear information.

Caution

Running the **clear** commands may lose vital information and thus interrupt services.

Run the **debug** command to output debugging information.

Caution

The output debugging information occupies system resources. Therefore, disable the debugging function immediately after use.

Table 1-2 Monitoring

Command	Purpose
show mpls forwarding-table [**frr**] [**detail**] **show mpls forwarding-table** { *ipv4-address/mask- length* | *ipv6-address/prefix-length* } [**frr**] [**detail**] **show mpls forwarding-table** { **ftn** | **ilm** } [**ip** | **ipv6**] [**frr**] [**detail**] **show mpls forwarding-table** { **global** | **vrf** *vrf-name* } [**ftn** | **ilm**] [**frr**] [**detail**] **show mpls forwarding-table interface** *interface-type interface-number* [**frr**] [**detail**] **show mpls forwarding-table label** *label* [**frr**] [**detail**] **show mpls forwarding-table next-hop** { *ipv4-address* | *ipv6-address* } [**frr**] [**detail**] **show mpls forwarding-table summary**	Displays MPLS forwarding table information.
show mpls interface [*interface-type interface-number*] **show mpls interface** [*interface-type interface-number*] [**detail**]	Displays information about an interface that is enabled to forward labeled MPLS packets.
show mpls label-pool [*label-space*]	Displays label pool usage of a specified label space.
show mpls ldp backup-frr [**all** | **vrf** *vrf-name*] [*ipv4-address/mask-length* | **ipv4**]	Displays information about master and backup LDP FRR entries.
show mpls ldp bindings [**all** | **vrf** *vrf-name*] [**ipv4** | **label** *label*] [**local** | **remote**]	Displays LDP label binding information.
show mpls ldp discovery [**all** | **vrf** *vrf-name*] [**detail**]	Displays LDP neighbor discovery information of all or specified VRF instances.

Command	Purpose
show mpls ldp interface [**all** | **vrf** *vrf-name* | *interface-type interface-number*]	Displays interfaces enabled with LDP.
show mpls ldp neighbor [**all** | **vrf** *vrf-name*] [*ipv4-address*] [**detail**]	Displays LDP neighbors of all or specified VRF instances.
show mpls ldp parameters [**all** | **vrf** *vrf-name*]	Displays LDP parameters of all or specified VRF instances.
show mpls psn notify-entry [**all** | **l3vpn** { **global** | **vrf** *vrf-name* }]	Displays the L3VPN instances that register public network reachability information to the MPLS platform.
show mpls ref ftn-ipv4 [**global** | **vrf** *vrf-name*] [*ipv4-address/mask-length* [**detail**]] **show mpls ref ftn-ipv6** [**global** | **vrf** *vrf-name*] [*ipv6-address/prefix-length* [**detail**]] **show mpls ref ilm** [**in-label** *in-label* [**detail**] | **summary**] **show mpls ref nhlfe** [*nhlfe-id* [**detail**] | **summary**] **show mpls ref summary**	Displays MPLS quick forward information.
show mpls rib [**all** | **vrf** *vrf-name*] [**ipv6**]	Displays MPLS RIB routing table information.
show mpls statistics [**lsp** [**bgp** | **isis** | **l3vpn** | **ldp** | **ospf**]]	Displays statistics on MPLS routing entries, MPLS forwarding entries, and MPLS LSPs.
show mpls summary	Displays MPLS global configurations.
show mpls tunnel-info { *tunnel-id* | **all | dest** *ipv4-address*/*mask-length* }	Displays the public network tunnel information.
show mpls vrf [**name** *vrf-name*] [**detail**]	Displays MPLS VRF information.
show mpls vrf-table-i [**vrf** *vrf-name*] [**fec** *ipv4-address/mask-length* | **owner** *protocol-name*] **show mpls vrf-table-i ipv6** [**vrf** *vrf-name*] [**fec** *ipv6-address/mask-length* | **owner** *protocol-name*]	Displays MPLS VRF entries.
show tunnel-policy { **all** | **name** *policy-name* }	Displays tunnel policy information.
clear mpls ldp neighbor [**all** | **vrf** *vrf-name*] [*ipv4-address*]	Clears established LDP sessions.
debug mpls	Debugs MPLS entry internal processing.
debug mpls ldp binding	Debugs LDP label binding.

Command	Purpose
debug mpls ldp internal-log prefix-whitelist [*ipv4-address/mask* | *****]	Debugs the LDP prefix whitelist.
debug mpls ldp message [**hello** | **keepalive**] [**received** | **sent**]	Debugs LDP session messages.
debug mpls lspv { **all** | **error** | **event** | **packet** | **tlv** }	Debugs the **ping mpls** and **traceroute mpls** execution processes.
debug mpls msg [**send** | **recv**]	Debugs MPLS messages.
debug mpls ref [**control** | **packet**]	Debugs MPLS quick forwarding (control plane or forwarding plane).

1.14 Configuration Examples

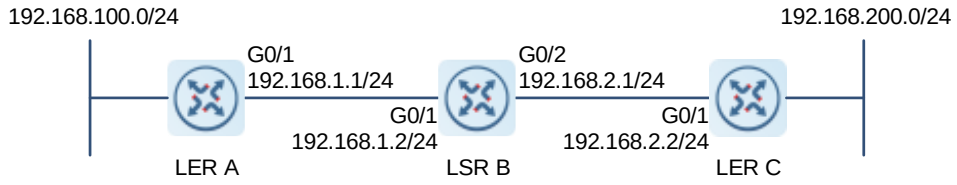
1.14.1 Configuring a Static LSP

1. Requirements

Configure static MPLS entries on LER A, LSR B, and LER C to set up an LSP and ensure that VPN sites can interconnect with each other through the MPLS network. LER A, LSR B, and LER C need to support the MPLS function.

2. Topology

Figure 1-10 Configuring a Static LSP



3. Notes

- Configure interface IP addresses and an IPv4 unicast routing protocol (for example, OSPF) on the devices to ensure that the routes between the devices are reachable.
- Enable MPLS forwarding globally and label forwarding on an interface.
- Configure static FTN entries on LER A and LER C, configure static ILM entries on LSR B, and set up static LSPs from LER A to LER C and from LER C to LER A. The outgoing label of the ILM entries on LSR B is implicit null label 3.

4. Procedure

(1) Configure interface IP addresses and OSPF on the devices to ensure that the routes between the devices are reachable.

Configure LER A.

```
LERA> enable
LERA# configure terminal
LERA(config)# interface gigabitethernet 0/1
LERA(config-if-GigabitEthernet 0/1)# ip address 192.168.1.1 255.255.255.0
LERA(config-if-GigabitEthernet 0/1)# exit
LERA(config)# router ospf 10
LERA(config-router)# network 192.168.1.0 0.0.0.255 area 0
LERA(config-router)# network 192.168.100.0 0.0.0.255 area 0
LERA(config-router)# exit
```

Configure LSR B.

```
LSRB> enable
LSRB# configure terminal
LSRB(config)# interface gigabitethernet 0/1
LSRB(config-if-GigabitEthernet 0/1)# ip address 192.168.1.2 255.255.255.0
LSRB(config-if-GigabitEthernet 0/1)# exit
LSRB(config)# interface gigabitethernet 0/2
LSRB(config-if-GigabitEthernet 0/2)# ip address 192.168.2.1 255.255.255.0
LSRB(config-if-GigabitEthernet 0/2)# exit
LSRB(config)# router ospf 10
LSRB(config-router)# network 192.168.1.0 0.0.0.255 area 0
LSRB(config-router)# network 192.168.2.0 0.0.0.255 area 0
LSRB(config-router)# exit
```

Configure LER C.

```
LERC> enable
LERC# configure terminal
LERC(config)# interface gigabitethernet 0/1
LERC(config-if-GigabitEthernet 0/1)# ip address 192.168.2.2 255.255.255.0
LERC(config-if-GigabitEthernet 0/1)# exit
LERC(config)# router ospf 10
LERC(config-router)# network 192.168.2.0 0.0.0.255 area 0
LERC(config-router)# network 192.168.200.0 0.0.0.255 area 0
LERC(config-router)# exit
```

(2) Enable MPLS forwarding globally and label forwarding on an interface.

Configure LER A.

```
LERA(config)# mpls enable
LERA(config)# interface gigabitethernet 0/1
LERA(config-if-GigabitEthernet 0/1)# label-switching
LERA(config-if-GigabitEthernet 0/1)# exit
```

Configure LSR B.

```
LSRB(config)# mpls enable
LSRB(config)# interface gigabitethernet 0/1
LSRB(config-if-GigabitEthernet 0/1)# label-switching
LSRB(config-if-GigabitEthernet 0/1)# exit
```

```
LSRB(config)# interface gigabitethernet 0/2
LSRB(config-if-GigabitEthernet 0/2)# label-switching
LSRB(config-if-GigabitEthernet 0/2)# exit
```

Configure LER C.

```
LERC(config)# mpls enable
LERC(config)# interface gigabitethernet 0/1
LERC(config-if-GigabitEthernet 0/1)# label-switching
LERC(config-if-GigabitEthernet 0/1)# exit
```

(3) Configure static FTN entries on LER A and LER C, configure static ILM entries on LSR B, and set up static LSPs from LER A to LER C and from LER C to LER A.

Configure LER A.

```
LERA(config)# mpls static ftn 192.168.200.0/24 out-label 16 nexthop gigabitethernet 0/1 192.168.1.2
LERA(config)# exit
```

Configure LSR B.

```
LSRB(config)# mpls static ilm in-label 16 forward-action swap-label 3 nexthop gigabitethernet 0/2
192.168.2.2 fec 192.168.200.0/24
LSRB(config)# mpls static ilm in-label 17 forward-action swap-label 3 nexthop gigabitethernet 0/1
192.168.1.1 fec 192.168.100.0/24
LSRB(config)# exit
```

Configure LER C.

```
LERC(config)# mpls static ftn 192.168.100.0/24 out-label 17 nexthop gigabitethernet 0/1 192.168.2.1
LERC(config)# exit
```

5. Verification

After the configuration is completed, run the **show mpls forwarding-table** command on devices to display MPLS entries.

Display MPLS entries on LER A.

```
LERA# show mpls forwarding-table
Label Operation Code:
PH--PUSH label
PP--POP label
SW--SWAP label
SP--SWAP topmost label and push new label
DP--DROP packet
PC--POP label and continue lookup by IP or Label
PI--POP label and do ip lookup forward
PN--POP label and forward to nexthop
PM--POP label and do MAC lookup forward
PV--POP label and output to VC attach interface
IP--IP lookup forward
 s--stale
  Local     Outgoing OP FEC                                Outgoing              Nexthop     Uptime
  label     label                                          interface
```

```
--      16      PH 192.168.200.0/24      Gi0/1      192.168.1.2    00:01:32
```

Display MPLS entries on LSR B.

```
LSRB# show mpls forwarding-table
Label Operation Code:
PH--PUSH label
PP--POP label
SW--SWAP label
SP--SWAP topmost label and push new label
DP--DROP packet
PC--POP label and continue lookup by IP or Label
PI--POP label and do ip lookup forward
PN--POP label and forward to nexthop
PM--POP label and do MAC lookup forward
PV--POP label and output to VC attach interface
IP--IP lookup forward
 s--stale
  Local    Outgoing OP FEC                Outgoing        Nexthop         Uptime
  label    label                          interface
  16        imp-null PP 192.168.200.0/24  Gi0/2           192.168.2.2     00:01:39
  17        imp-null PP 192.168.100.0/24  Gi0/1           192.168.1.1     00:01:39
```

Display MPLS entries on LER C.

```
LERC# show mpls forwarding-table
Label Operation Code:
PH--PUSH label
PP--POP label
SW--SWAP label
SP--SWAP topmost label and push new label
DP--DROP packet
PC--POP label and continue lookup by IP or Label
PI--POP label and do ip lookup forward
PN--POP label and forward to nexthop
PM--POP label and do MAC lookup forward
PV--POP label and output to VC attach interface
IP--IP lookup forward
 s--stale
  Local    Outgoing OP FEC                Outgoing        Nexthop      Uptime
  label    label                          interface
  --       17       PH 192.168.100.0/24   Gi0/1           192.168.2.1  00:02:04
```

6. Configuration Files

- LER A configuration file

```
hostname LERA
!
mpls enable
!
```

```
interface gigabitethernet 0/1
 mpls ldp enable
 ip address 192.168.1.1 255.255.255.0
 label-switching
!
router ospf 10
 network 192.168.1.0 0.0.0.255 area 0
 network 192.168.100.0 0.0.0.255 area 0
!
mpls static ftn 192.168.200.0/24 out-label 16 nexthop GigabitEthernet 0/1 192.168.1.2
!
```

- LSR B configuration file

```
hostname LSRB
!
mpls enable
!
interface gigabitethernet 0/1
 mpls ldp enable
 ip address 192.168.1.2 255.255.255.0
 label-switching
!
interface gigabitethernet 0/2
 mpls ldp enable
 ip address 192.168.2.1 255.255.255.0
 label-switching
!
router ospf 10
 network 192.168.1.0 0.0.0.255 area 0
 network 192.168.2.0 0.0.0.255 area 0
!
mpls static ilm in-label 16 forward-action swap-label 3 nexthop GigabitEthernet 0/2 192.168.2.2 fec
192.168.200.0/24
mpls static ilm in-label 17 forward-action swap-label 3 nexthop GigabitEthernet 0/1 192.168.1.1 fec
192.168.100.0/24
!
```

- LER C configuration file

```
hostname LERC
!
mpls enable
!
interface gigabitethernet 0/1
 mpls ldp enable
 ip address 192.168.2.2 255.255.255.0
 label-switching
!
```

```
router ospf 10
 network 192.168.2.0 0.0.0.255 area 0
 network 192.168.200.0 0.0.0.255 area 0
!
mpls static ftn 192.168.100.0/24 out-label 17 nexthop GigabitEthernet 0/1 192.168.2.1
!
```

7. Common Errors

- MPLS forwarding is not enabled globally.
- MPLS forwarding is not enabled on an interface.

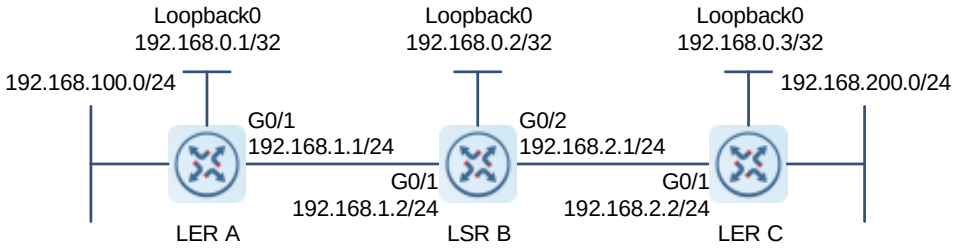
1.14.2 Configuring an LDP LSP

1. Requirements

Configure local LDP sessions among LER A, LSR B, and LER C to set up an LDP LSP and ensure that VPN sites can interconnect with each other through the MPLS network. LER A, LSR B, and LER C need to support the MPLS function.

2. Topology

Figure 1-11 Configuring an LDP LSP



3. Notes

- Configure interface IP addresses and an IPv4 unicast routing protocol (for example, OSPF) on the devices to ensure that the routes between the devices are reachable.
- Enable MPLS forwarding globally.
- Configure the LDP and LDP router ID.
- Enable the LDP function and label forwarding capability on an interface.

4. Procedure

(1) Configure interface IP addresses and OSPF on the devices to ensure that the routes between the devices are reachable.

Configure LER A.

```
LERA> enable
LERA# configure terminal
LERA(config)# interface gigabitethernet 0/1
LERA(config-if-GigabitEthernet 0/1)# mpls ldp enable
```

```
LERA(config-if-GigabitEthernet 0/1)# ip address 192.168.1.1 255.255.255.0
LERA(config-if-GigabitEthernet 0/1)# exit
LERA(config)# interface loopback 0
LERA(config-if-Loopback 0)# ip address 192.168.0.1 255.255.255.255
LERA(config-if-Loopback 0)# exit
LERA(config)# router ospf 10
LERA(config-router)# network 192.168.1.0 0.0.0.255 area 0
LERA(config-router)# network 192.168.0.1 0.0.0.0 area 0
LERA(config-router)# network 192.168.100.0 0.0.0.255 area 0
LERA(config-router)# exit
```

Configure LSR B.

```
LSRB> enable
LSRB# configure terminal
LSRB(config)# interface gigabitethernet 0/1
LSRB(config-if-GigabitEthernet 0/1)# mpls ldp enable
LSRB(config-if-GigabitEthernet 0/1)# ip address 192.168.1.2 255.255.255.0
LSRB(config-if-GigabitEthernet 0/1)# exit
LSRB(config)# interface gigabitethernet 0/2
LSRB(config-if-GigabitEthernet 0/2)# mpls ldp enable
LSRB(config-if-GigabitEthernet 0/2)# ip address 192.168.2.1 255.255.255.0
LSRB(config-if-GigabitEthernet 0/2)# exit
LSRB(config)# interface loopback 0
LSRB(config-if-Loopback 0)# ip address 192.168.0.2 255.255.255.255
LSRB(config-if-Loopback 0)# exit
LSRB(config)# router ospf 10
LSRB(config-router)# network 192.168.1.0 0.0.0.255 area 0
LSRB(config-router)# network 192.168.2.0 0.0.0.255 area 0
LSRB(config-router)# network 192.168.0.2 0.0.0.0 area 0
LSRB(config-router)# exit
```

Configure LER C.

```
LERC> enable
LERC# configure terminal
LERC(config)# interface gigabitethernet 0/1
LERC(config-if-GigabitEthernet 0/1)# mpls ldp enable
LERC(config-if-GigabitEthernet 0/1)# ip address 192.168.2.2 255.255.255.0
LERC(config-if-GigabitEthernet 0/1)# exit
LERC(config)# interface loopback 0
LERC(config-if-Loopback 0)# ip address 192.168.0.3 255.255.255.255
LERC(config-if-Loopback 0)# exit
LERC(config)# router ospf 10
LERC(config-router)# network 192.168.2.0 0.0.0.255 area 0
LERC(config-router)# network 192.168.0.3 0.0.0.0 area 0
LERC(config-router)# network 192.168.200.0 0.0.0.255 area 0
LERC(config-router)# exit
```

(2) Enable MPLS forwarding globally. LER A is used as an example. Configurations on LSR B and LER C are similar to those on LER A.

```
LERA(config)# mpls enable
```

(3) Configure the LDP and LDP router ID. LER A is used as an example. Configurations on LSR B and LER C are similar to those on LER A.

```
LERA(config)# mpls router ldp
LERA(config-mpls-router)# ldp router-id interface loopback 0 force
LERA(config-mpls-router)# exit
```

(4) Enable the LDP function and label forwarding capability on an interface.

Configure LER A.

```
LERA(config)# interface gigabitethernet 0/1
LERA(config-if-GigabitEthernet 0/1)# mpls enable
LERA(config-if-GigabitEthernet 0/1)# label-switching
LERA(config-if-GigabitEthernet 0/1)# end
```

Configure LSR B.

```
LSRB(config)# interface gigabitethernet 0/1
LSRB(config-if-GigabitEthernet 0/1)# mpls enable
LSRB(config-if-GigabitEthernet 0/1)# label-switching
LSRB(config-if-GigabitEthernet 0/1)# exit
LSRB(config)# interface gigabitethernet 0/2
LSRB(config-if-GigabitEthernet 0/2)# mpls enable
LSRB(config-if-GigabitEthernet 0/2)# label-switching
LSRB(config-if-GigabitEthernet 0/2)# end
```

Configure LER C.

```
LERC (config)# interface gigabitethernet 0/1
LERC(config-if-GigabitEthernet 0/1)# mpls enable
LERC(config-if-GigabitEthernet 0/1)# label-switching
LERC(config-if-GigabitEthernet 0/1)# end
```

5. Verification

(1) After the configuration is completed, run the **show mpls ldp neighbor** command to check whether the status of LDP sessions among LER A, LSR B, and LER C is "OPERATIONAL."

Display LDP session information on LER A.

```
LERA# show mpls ldp neighbor
global-vrf:
    Peer LDP Ident: 192.168.0.2:0; Local LDP Ident: 192.168.0.1:0
        TCP connection: 192.168.0.2.45063 - 192.168.0.1.646
        State: OPERATIONAL; Msgs sent/recv: 606/606; UNSOLICITED
        Up time: 02:28:09
        Graceful Restart enabled; Peer reconnect time (msecs): 300000
        LDP discovery sources:
          Link Peer on GigabitEthernet 0/1, Src IP addr: 192.168.1.2
        Addresses bound to peer LDP Ident: ( Count: 3 )
```

```
    192.168.1.2        192.168.2.1        192.168.0.2
```

Display LDP session information on LSR B.

```
LSRB# show mpls ldp neighbor
global-vrf:
    Peer LDP Ident: 192.168.0.1:0; Local LDP Ident: 192.168.0.2:0
        TCP connection: 192.168.0.1.646 - 192.168.0.2.45063
        State: OPERATIONAL; Msgs sent/recv: 650/653; UNSOLICITED
        Up time: 02:39:26
        Graceful Restart enabled; Peer reconnect time (msecs): 300000
        LDP discovery sources:
          Link Peer on GigabitEthernet 0/1, Src IP addr: 192.168.1.1
        Addresses bound to peer LDP Ident: ( Count: 2 )
          192.168.0.1        192.168.1.1
    Peer LDP Ident: 192.168.0.3:0; Local LDP Ident: 192.168.0.2:0
        TCP connection: 192.168.0.3.41299 - 192.168.0.2.646
        State: OPERATIONAL; Msgs sent/recv: 335/336; UNSOLICITED
        Up time: 01:21:20
        Graceful Restart enabled; Peer reconnect time (msecs): 300000
        LDP discovery sources:
          Link Peer on GigabitEthernet 0/2, Src IP addr: 192.168.2.2
        Addresses bound to peer LDP Ident: ( Count: 3 )
          192.168.2.2        192.168.0.3        192.168.200.1
```

Display LDP session information on LER C.

```
LERC# show mpls ldp neighbor
global-vrf:
    Peer LDP Ident: 192.168.0.2:0; Local LDP Ident: 192.168.0.3:0
        TCP connection: 192.168.0.2.646 - 192.168.0.3.41299
        State: OPERATIONAL; Msgs sent/recv: 344/345; UNSOLICITED
        Up time: 01:23:33
        Graceful Restart enabled; Peer reconnect time (msecs): 300000
        LDP discovery sources:
          Link Peer on GigabitEthernet 0/1, Src IP addr: 192.168.2.1
        Addresses bound to peer LDP Ident: ( Count: 3 )
          192.168.1.2        192.168.2.1        192.168.0.2
```

(2) Run the **show mpls forwarding-table** command to display MPLS forwarding entries on LER A, LSR B, and LER C and verify that the LDP LSP is set up.

Display MPLS forwarding entries on LER A.

```
LERA# show mpls forwarding-table
Label Operation Code:
PH--PUSH label
PP--POP label
SW--SWAP label
SP--SWAP topmost label and push new label
DP--DROP packet
```

```
PC--POP label and continue lookup by IP or Label
PI--POP label and do ip lookup forward
PN--POP label and forward to nexthop
PM--POP label and do MAC lookup forward
PV--POP label and output to VC attach interface
IP--IP lookup forward
 s--stale
   Local     Outgoing OP FEC                  Outgoing          Nexthop          Uptime
   label     label                            interface
   --        imp-null PH 192.168.0.2/32       Gi0/1             192.168.1.2      00:06:29
   --        11265      PH 192.168.0.3/32     Gi0/1             192.168.1.2      00:06:29
   --        imp-null PH 192.168.2.0/24       Gi0/1             192.168.1.2      00:06:29
   11265     imp-null PP 192.168.0.2/32       Gi0/1             192.168.1.2      00:06:29
   11266     11265      SW 192.168.0.3/32     Gi0/1             192.168.1.2      00:06:29
   11267     imp-null PP 192.168.2.0/24       Gi0/1             192.168.1.2      00:06:29
```

Display MPLS forwarding entries on LSR B.

```
LSRB# show mpls forwarding-table
Label Operation Code:
PH--PUSH label
PP--POP label
SW--SWAP label
SP--SWAP topmost label and push new label
DP--DROP packet
PC--POP label and continue lookup by IP or Label
PI--POP label and do ip lookup forward
PN--POP label and forward to nexthop
PM--POP label and do MAC lookup forward
PV--POP label and output to VC attach interface
IP--IP lookup forward
 s--stale
   Local     Outgoing OP FEC                  Outgoing          Nexthop          Uptime
   label     label                            interface
   --        imp-null PH 192.168.0.1/32       Gi0/1             192.168.1.1      00:03:08
   --        imp-null PH 192.168.0.3/32       Gi0/2             192.168.2.2      00:03:08
   11265     imp-null PP 192.168.0.3/32       Gi0/2             192.168.2.2      00:03:08
   11267     imp-null PP 192.168.0.1/32       Gi0/1             192.168.1.1      00:03:08
```

Display MPLS forwarding entries on LER C.

```
LERC# show mpls forwarding-table
Label Operation Code:
PH--PUSH label
PP--POP label
SW--SWAP label
SP--SWAP topmost label and push new label
DP--DROP packet
PC--POP label and continue lookup by IP or Label
```

```
PI--POP label and do ip lookup forward
PN--POP label and forward to nexthop
PM--POP label and do MAC lookup forward
PV--POP label and output to VC attach interface
IP--IP lookup forward
 s--stale
   Local     Outgoing OP FEC                Outgoing          Nexthop          Uptime
   label     label                          interface
   --        11267       PH 192.168.0.1/32      Gi0/1              192.168.2.1      00:09:16
   --        imp-null PH 192.168.0.2/32     Gi0/1              192.168.2.1      00:09:16
   --        imp-null PH 192.168.1.0/24     Gi0/1              192.168.2.1      00:09:16
   11265     11267       SW 192.168.0.1/32      Gi0/1              192.168.2.1      00:09:16
   11266     imp-null PP 192.168.0.2/32     Gi0/1              192.168.2.1      00:09:16
   11267     imp-null PP 192.168.1.0/24     Gi0/1              192.168.2.1      00:09:16
```

6. Configuration Files

- LER A configuration file

```
hostname LERA
!
mpls enable
!
interface gigabitethernet 0/1
 mpls ldp enable
 ip address 192.168.1.1 255.255.255.0
 mpls ldp enable
 label-switching
!
interface loopback 0
 ip address 192.168.0.1 255.255.255.255
!
router ospf 10
 network 192.168.0.1 0.0.0.0 area 0
 network 192.168.1.0 0.0.0.255 area 0
 network 192.168.100.0 0.0.0.255 area 0
!
mpls router ldp
 ldp router-id interface loopback 0 force
!
```

- LSR B configuration file

```
hostname LSRB
!
mpls enable
!
interface gigabitethernet 0/1
 mpls ldp enable
```

```
 ip address 192.168.1.2 255.255.255.0
 mpls enable
 label-switching
!
interface gigabitethernet 0/2
 mpls ldp enable
 ip address 192.168.2.1 255.255.255.0
 mpls enable
 label-switching
!
interface loopback 0
 ip address 192.168.0.2 255.255.255.255
!
router ospf 10
 network 192.168.0.2 0.0.0.0 area 0
 network 192.168.1.0 0.0.0.255 area 0
 network 192.168.2.0 0.0.0.255 area 0
!
mpls router ldp
 ldp router-id interface loopback 0 force
!
```

- LER C configuration file

```
hostname LERC
!
mpls enable
!
interface gigabitethernet 0/1
 mpls ldp enable
 ip address 192.168.2.2 255.255.255.0
 mpls ldp enable
 label-switching
!
interface loopback 0
 ip address 192.168.0.3 255.255.255.255
!
router ospf 10
 network 192.168.0.3 0.0.0.0 area 0
 network 192.168.2.0 0.0.0.255 area 0
 network 192.168.200.0 0.0.0.255 area 0
!
mpls router ldp
 ldp router-id interface loopback 0 force
!
```

7. Common Errors

- An IPv4 unicast route is incorrectly configured.

- MPLS forwarding is not enabled globally.
- LDP is not configured.
- LDP is not enabled on an interface.
- The label forwarding capability is not enabled on an interface.

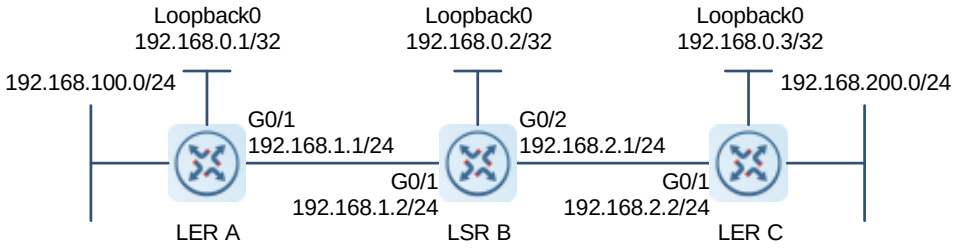
1.14.3 Configuring a Remote LDP Session

1. Requirements

Establish a remote LDP session.

2. Topology

Figure 1-12 Establishing a Remote LDP Session



3. Notes

- Configure an IPv4 unicast routing protocol (such as OSPF) on the devices and ensure that the loopback interfaces are accessible via unicast routes.
- Enable MPLS forwarding and LDP globally and configure the LDP router ID.
- Configure remote peers.

4. Procedure

(1) Configure interface IP addresses and OSPF on the devices to ensure communication between them.

Configure LER A.

```
LERA> enable
LERA# configure terminal
LERA(config)# interface gigabitethernet 0/1
LERA(config-if-GigabitEthernet 0/1)# mpls ldp enable
LERA(config-if-GigabitEthernet 0/1)# ip address 192.168.1.1 255.255.255.0
LERA(config-if-GigabitEthernet 0/1)# exit
LERA(config)# interface loopback 0
LERA(config-if-Loopback 0)# ip address 192.168.0.1 255.255.255.255
LERA(config-if-Loopback 0)# exit
LERA(config)# router ospf 10
LERA(config-router)# network 192.168.1.0 0.0.0.255 area 0
LERA(config-router)# network 192.168.0.1 0.0.0.0 area 0
LERA(config-router)# network 192.168.100.0 0.0.0.255 area 0
LERA(config-router)# exit
```

Configure LSR B.

```
LSRB> enable
LSRB# configure terminal
LSRB(config)# interface gigabitethernet 0/1
LSRB(config-if-GigabitEthernet 0/1)# mpls ldp enable
LSRB(config-if-GigabitEthernet 0/1)# ip address 192.168.1.2 255.255.255.0
LSRB(config-if-GigabitEthernet 0/1)# exit
LSRB(config)# interface gigabitethernet 0/2
LSRB(config-if-GigabitEthernet 0/2)# mpls ldp enable
LSRB(config-if-GigabitEthernet 0/2)# ip address 192.168.2.1 255.255.255.0
LSRB(config-if-GigabitEthernet 0/2)# exit
LSRB(config)# interface loopback 0
LSRB(config-if-Loopback 0)# ip address 192.168.0.2 255.255.255.255
LSRB(config-if-Loopback 0)# exit
LSRB(config)# router ospf 10
LSRB(config-router)# network 192.168.1.0 0.0.0.255 area 0
LSRB(config-router)# network 192.168.0.2 0.0.0.0 area 0
LSRB(config-router)# network 192.168.2.0 0.0.0.255 area 0
LSRB(config-router)# exit#
```

Configure LER C.

```
LERC> enable
LERC# configure terminal
LERC(config)# interface gigabitethernet 0/1
LERC(config-if-GigabitEthernet 0/1)# mpls ldp enable
LERC(config-if-GigabitEthernet 0/1)# ip address 192.168.2.2 255.255.255.0
LERC(config-if-GigabitEthernet 0/1)# exit
LERC(config)# interface loopback 0
LERC(config-if-Loopback 0)# ip address 192.168.0.3 255.255.255.255
LERC(config-if-Loopback 0)# exit
LERC(config)# router ospf 10
LERC(config-router)# network 192.168.2.0 0.0.0.255 area 0
LERC(config-router)# network 192.168.0.3 0.0.0.0 area 0
LERC(config-router)# network 192.168.200.0 0.0.0.255 area 0
LERC(config-router)# exit
```

(2) Enable MPLS forwarding and LDP globally and configure the LDP router ID. LER A is used as an example. Configurations on LER C are similar to those on LER A.

Configure LER A.

```
LERA(config)# mpls enable
LERA(config)# mpls router ldp
LERA(config-mpls-router)# ldp router-id interface loopback 0 force
```

(3) Configure remote peers.

Configure LER A.

```
LERA(config-mpls-router)# neighbor 192.168.0.3
LERA(config-mpls-router)# end
```

Configure LER C.

```
LERC(config-mpls-router)# neighbor 192.168.0.1
LERC(config-mpls-router)# end
```

5. Verification

Run the **show mpls ldp neighbor** command to check whether an LDP session is established between LER A and LER C.

Check whether an LDP session to LER C is established on LER A.

```
LERA# show mpls ldp neighbor
global-vrf:
    Peer LDP Ident: 192.168.0.3:0; Local LDP Ident: 192.168.0.1:0
        TCP connection: 192.168.0.3.36809 - 192.168.0.1.646
        State: OPERATIONAL; Msgs sent/recv: 15/16; UNSOLICITED
        Up time: 00:10:52
        Graceful Restart enabled; Peer reconnect time (msecs): 300000
        LDP discovery sources:
          Targeted Hello 192.168.0.1 -> 192.168.0.3, active, passive;
        Addresses bound to peer LDP Ident: ( Count: 2 )
          192.168.2.2        192.168.0.3
```

Check whether an LDP session to LER A is established on LER C.

```
LERC# show mpls ldp neighbor
global-vrf:
    Peer LDP Ident: 192.168.0.1:0; Local LDP Ident: 192.168.0.3:0
        TCP connection: 192.168.0.1.646 - 192.168.0.3.36809
        State: OPERATIONAL; Msgs sent/recv: 17/18; UNSOLICITED
        Up time: 00:12:02
        Graceful Restart enabled; Peer reconnect time (msecs): 300000
        LDP discovery sources:
          Targeted Hello 192.168.0.3 -> 192.168.0.1, active, passive;
        Addresses bound to peer LDP Ident: ( Count: 2 )
          192.168.1.1        192.168.0.1
```

6. Configuration Files

- LER A configuration file

```
hostname LERA
!
mpls enable
!
interface GigabitEthernet 0/1
 mpls ldp enable
 ip address 192.168.1.1 255.255.255.0
!
interface Loopback 0
 ip address 192.168.0.1 255.255.255.255
!
```

```
router ospf 10
 network 192.168.0.1 0.0.0.0 area 0
 network 192.168.1.0 0.0.0.255 area 0
 network 192.168.100.0 0.0.0.255 area 0
!
mpls router ldp
 ldp router-id interface Loopback 0 force
 neighbor 192.168.0.3
!
```

- LSR B configuration file

```
hostname LSRB
!
interface GigabitEthernet 0/1
 mpls ldp enable
 ip address 192.168.1.2 255.255.255.0
!
interface GigabitEthernet 0/2
 mpls ldp enable
 ip address 192.168.2.1 255.255.255.0
!
interface Loopback 0
 ip address 192.168.0.2 255.255.255.255
!
router ospf 10
 network 192.168.0.2 0.0.0.0 area 0
 network 192.168.1.0 0.0.0.255 area 0
 network 192.168.2.0 0.0.0.255 area 0
!
```

- LER C configuration file

```
hostname LERC
!
mpls enable
!
interface GigabitEthernet 0/1
 mpls ldp enable
 ip address 192.168.2.2 255.255.255.0
!
interface Loopback 0
 ip address 192.168.0.3 255.255.255.255
!
router ospf 10
 network 192.168.0.3 0.0.0.0 area 0
 network 192.168.2.0 0.0.0.255 area 0
 network 192.168.200.0 0.0.0.255 area 0
!
```

```
mpls router ldp
 ldp router-id interface Loopback 0 force
 neighbor 192.168.0.1
!
```

7. Common Errors

- An IPv4 unicast route is incorrectly configured.
- MPLS forwarding is not enabled globally.
- LDP is not configured.
- Remote peers are not configured.

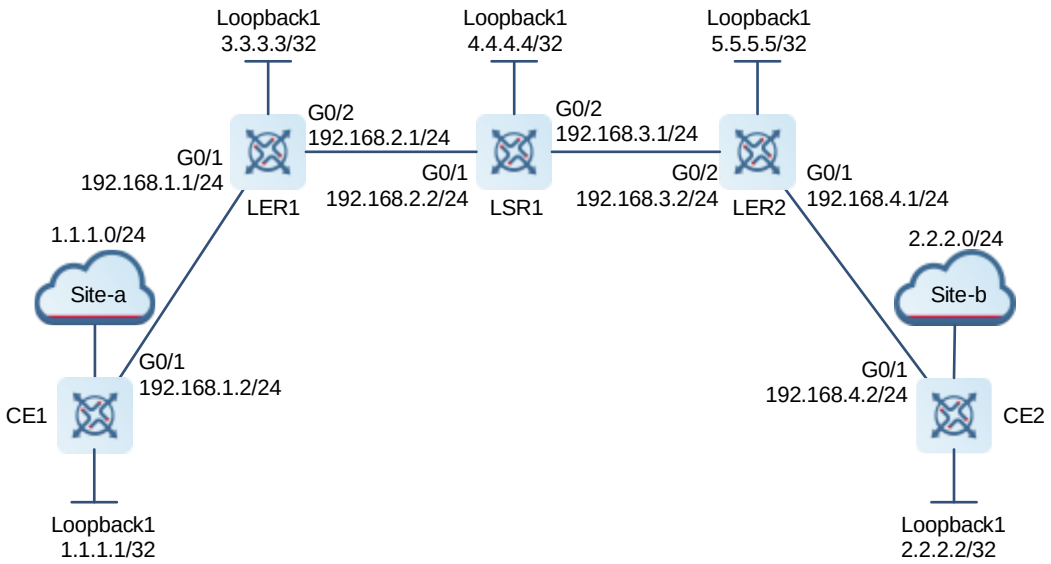
1.14.4 Iterating IP Routes to LDP LSPs

1. Requirements

Iterate IP routes to LDP LSPs.

2. Topology

Figure 1-13 Iterating IP Routes to LDP LSPs



3. Notes

- Configure IP addresses and IS-IS on LER1, LSR1, and LER2 and establish IS-IS unicast neighbors.
- Configure the LDP on LER1, LSR1, and LER2 and establish LDP neighbors.
- Configure IP addresses and OSPF and establish OSPF neighbors between CE1 and LER1, and between CE2 and LER2, respectively.
- Configure a static route from LER1 to CE2, configure a static route from LER2 to CE1, and re-distribute the static routes to OSPF.
- Enable the function of iterating IP routes to LDP LSPs on LER1 and LER2.

4. Procedure

(1) Configure IP addresses and IS-IS on LER1, LSR1, and LER2 and establish IS-IS unicast neighbors.

Configure LER1.

```
LER1> enable
LER1# configure terminal
LER1(config)# router isis
LER1(config-router)# net 49.0001.0000.0000.0001.00
LER1(config-router)# exit
LER1(config)# interface loopback 1
LER1(config-if-Loopback 1)# ip address 3.3.3.3 255.255.255.255
LER1(config-if-Loopback 1)# ip router isis
LER1(config-if-Loopback 1)# exit
LER1(config)# interface gigabitethernet 0/2
LER1(config-if-GigabitEthernet 0/2)# mpls ldp enable
LER1(config-if-GigabitEthernet 0/2)# ip address 192.168.2.1 255.255.255.0
LER1(config-if-GigabitEthernet 0/2)# ip router isis
LER1(config-if-GigabitEthernet 0/2)# exit
```

Configure LSR1.

```
LSR1> enable
LSR1# configure terminal
LSR1(config)# router isis
LSR1(config-router)# net 49.0001.0000.0000.0002.00
LSR1(config-router)# exit
LSR1(config)# interface loopback 1
LSR1(config-if-Loopback 1)# ip address 4.4.4.4 255.255.255.255
LSR1(config-if-Loopback 1)# ip router isis
LSR1(config-if-Loopback 1)# exit
LSR1(config)# interface gigabitethernet 0/1
LSR1(config-if-GigabitEthernet 0/1)# mpls ldp enable
LSR1(config-if-GigabitEthernet 0/1)# ip address 192.168.2.2 255.255.255.0
LSR1(config-if-GigabitEthernet 0/1)# ip router isis
LSR1(config-if-GigabitEthernet 0/1)# exit
LSR1(config)# interface gigabitethernet 0/2
LSR1(config-if-GigabitEthernet 0/2)# mpls ldp enable
LSR1(config-if-GigabitEthernet 0/2)# ip address 192.168.3.1 255.255.255.0
LSR1(config-if-GigabitEthernet 0/2)# ip router isis
LSR1(config-if-GigabitEthernet 0/2)# exit
```

Configure LER2.

```
LER2> enable
LER2# configure terminal
LER2(config)# router isis
LER2(config-router)# net 49.0001.0000.0000.0003.00
LER2(config-router)# exit
LER2(config)# interface loopback 1
```

```
LER2(config-if-Loopback 1)# ip address 5.5.5.5 255.255.255.255
LER2(config-if-Loopback 1)# ip router isis
LER2(config-if-Loopback 1)# exit
LER2(config)# interface gigabitethernet 0/2
LER2(config-if-GigabitEthernet 0/2)# mpls ldp enable
LER2(config-if-GigabitEthernet 0/2)# ip address 192.168.3.2 255.255.255.0
LER2(config-if-GigabitEthernet 0/2)# ip router isis
LER2(config-if-GigabitEthernet 0/2)# exit
```

(2) Configure the LDP on LER1, LSR1, and LER2 and establish LDP neighbors.

Configure LER1.

```
LER1(config)# mpls router ldp
LER1(config-mpls-router)# ldp router-id interface loopback 1 force
LER1(config-mpls-router)# exit
LER1(config)# interface gigabitethernet 0/2
LER1(config-if-GigabitEthernet 0/2)# mpls ldp enable
LER1(config-if-GigabitEthernet 0/2)# label-switching
LER1(config-if-GigabitEthernet 0/2)# exit
```

Configure LSR1.

```
LSR1(config)# mpls router ldp
LSR1(config-mpls-router)# ldp router-id interface loopback 1 force
LSR1(config-mpls-router)# exit
LSR1(config)# interface gigabitethernet 0/1
LSR1(config-if-GigabitEthernet 0/1)# mpls ldp enable
LSR1(config-if-GigabitEthernet 0/1)# label-switching
LSR1(config-if-GigabitEthernet 0/1)# exit
LSR1(config)# interface gigabitethernet 0/2
LSR1(config-if-GigabitEthernet 0/2)# mpls ldp enable
LSR1(config-if-GigabitEthernet 0/2)# label-switching
LSR1(config-if-GigabitEthernet 0/2)# exit
```

Configure LER2.

```
LER2(config)# mpls router ldp
LER2(config-mpls-router)# ldp router-id interface loopback 1 force
LER2(config-mpls-router)# exit
LER2(config)# interface gigabitethernet 0/2
LER2(config-if-GigabitEthernet 0/2)# mpls ldp enable
LER2(config-if-GigabitEthernet 0/2)# label-switching
LER2(config-if-GigabitEthernet 0/2)# exit
```

(3) Configure IP addresses and OSPF and establish OSPF neighbors between CE1 and LER1, and between CE2 and LER2, respectively.

Configure CE1.

```
CE1> enable
CE1# configure terminal
CE1(config)# interface gigabitethernet 0/1
CE1(config-if-GigabitEthernet 0/1)# mpls ldp enable
```

```
CE1(config-if-GigabitEthernet 0/1)# ip address 192.168.1.2 255.255.255.0
CE1(config-if-GigabitEthernet 0/1# exit
CE1(config)# interface loopback 1
CE1(config-if-Loopback 1)# ip address 1.1.1.1 255.255.255.255
CE1(config-if-Loopback 1)# exit
CE1(config)# router ospf 1
CE1(config-router)# network 192.168.1.0 0.0.0.255 area 0
CE1(config-router)# network 1.1.1.0 0.0.0.255 area 0
CE1(config-router)# end
```

Configure LER1.

```
LER1(config)# interface gigabitethernet 0/1
LER1(config-if-GigabitEthernet 0/1)# mpls ldp enable
LER1(config-if-GigabitEthernet 0/1)# ip address 192.168.1.1 255.255.255.0
LER1(config-if-GigabitEthernet 0/1)# exit
LER1(config)# router ospf 1
LER1(config-router)# network 192.168.1.0 0.0.0.255 area 0
LER1(config-router)# exit
```

Configure LER2.

```
LER2(config)# interface gigabitethernet 0/1
LER2(config-if-GigabitEthernet 0/1)# mpls ldp enable
LER2(config-if-GigabitEthernet 0/1)# ip address 192.168.4.1 255.255.255.0
LER2(config-if-GigabitEthernet 0/1)# exit
LER2(config)# router ospf 1
LER2(config-router)# network 192.168.4.0 0.0.0.255 area 0
LER2(config-router)# exit
```

Configure CE2.

```
CE2> enable
CE2# configure terminal
CE2(config)# interface gigabitethernet 0/1
CE2(config-if-GigabitEthernet 0/1)# mpls ldp enable
CE2(config-if-GigabitEthernet 0/1)# ip address 192.168.4.2 255.255.255.0
CE2(config-if-GigabitEthernet 0/1# exit
CE2(config)# interface loopback 1
CE2(config-if-Loopback 1)# ip address 2.2.2.2 255.255.255.255
CE2(config-if-Loopback 1)# exit
CE2(config)# router ospf 1
CE2(config-router)# network 192.168.4.0 0.0.0.255 area 0
CE2(config-router)# network 2.2.2.0 0.0.0.255 area 0
```

(4) Configure a static route from LER1 to CE2, configure a static route from LER2 to CE1, and re-distribute the static routes to OSPF.

Configure LER1.

```
LER1(config)# ip route 2.2.2.0 255.255.255.0 5.5.5.5
LER1(config)# router ospf 1
LER1(config-router)# redistribute static subnets
```

```
LER1(config-router)# exit
```

Configure LER2.

```
LER2(config)# ip route 1.1.1.0 255.255.255.0 3.3.3.3
LER2(config)# router ospf 1
LER2(config-router)# redistribute static subnets
LER2(config-router)# exit
```

(5) Enable the function of iterating IP routes to LDP LSPs on LER1 and LER2. LER1 is used as an example. Configurations on LER2 are similar to those on LER1.

Configure LER1.

```
LER1(config)# recursive-route to mpls
LER1(config)# end
```

5. Verification

Run the **show mpls forwarding-table** command to check that LER1 and LER2 have public FTN entries to the peer and traffic forwarding between CE1 and CE2 is normal.

Display LER1 entries.

```
LER1# show mpls forwarding-table
Label Operation Code:
PH--PUSH label
PP--POP label
SW--SWAP label
SP--SWAP topmost label and push new label
DP--DROP packet
PC--POP label and continue lookup by IP or Label
PI--POP label and do ip lookup forward
PN--POP label and forward to nexthop
PM--POP label and do MAC lookup forward
PV--POP label and output to VC attach interface
IP--IP lookup forward
 s--stale
  Local     Outgoing OP FEC                Outgoing          Nexthop          Uptime
  label     label                          interface
  --        imp-null PH 4.4.4.4/32         Gi0/2             192.168.2.2      01:28:43
  --        11266    PH 5.5.5.5/32         Gi0/2             192.168.2.2      01:28:43
  --        imp-null PH 192.168.3.0/24     Gi0/2             192.168.2.2      01:28:43
  11265     --       PI 1.1.1.1/32         Gi0/1             192.168.1.2      01:28:43
  11266     imp-null PP 4.4.4.4/32         Gi0/2             192.168.2.2      01:28:43
  11267     imp-null PP 192.168.3.0/24     Gi0/2             192.168.2.2      01:28:43
  11268     11266    SW 5.5.5.5/32         Gi0/2             192.168.2.2      01:28:43
  11269     --       PI 2.2.2.0/24         Gi0/2             5.5.5.5          01:28:43
```

Display LER2 entries.

```
LER2# show mpls forwarding-table
Label Operation Code:
PH--PUSH label
```

```
PP--POP label
SW--SWAP label
SP--SWAP topmost label and push new label
DP--DROP packet
PC--POP label and continue lookup by IP or Label
PI--POP label and do ip lookup forward
PN--POP label and forward to nexthop
PM--POP label and do MAC lookup forward
PV--POP label and output to VC attach interface
IP--IP lookup forward
 s--stale
   Local     Outgoing OP FEC                  Outgoing          Nexthop          Uptime
   label     label                            interface
   --        11265       PH 3.3.3.3/32        Gi0/2             192.168.3.1      01:29:05
   --        imp-null PH 4.4.4.4/32           Gi0/2             192.168.3.1      01:29:05
   --        imp-null PH 192.168.2.0/24       Gi0/2             192.168.3.1      01:29:05
   92162     --          PI 2.2.2.2/32        Gi0/1             192.168.4.2      01:29:05
   92163     11265       SW 3.3.3.3/32        Gi0/2             192.168.3.1      01:29:05
   92164     imp-null PP 4.4.4.4/32           Gi0/2             192.168.3.1      01:29:05
   92168     imp-null PP 192.168.2.0/24       Gi0/2             192.168.3.1      01:29:05
   92169     --          PI 1.1.1.0/24        Gi0/2             3.3.3.3          01:29:05
```

Check that CE1 can access CE2.

```
CE1# ping 2.2.2.2 source 1.1.1.1
Sending 5, 100-byte ICMP Echoes to 2.2.2.2, timeout is 2 seconds:
   < press Ctrl+C to break >
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/6 ms.
```

6. Configuration Files

- CE1 configuration file

```
hostname CE1
!
interface gigabitethernet 0/1
 mpls ldp enable
 ip address 192.168.1.2 255.255.255.0
!
interface Loopback 1
 ip address 1.1.1.1 255.255.255.255
!
router ospf 1
 network 1.1.1.0 0.0.0.255 area 0
 network 192.168.1.0 0.0.0.255 area 0
!
```

- LER1 configuration file

```
hostname LER1
```

```
!
mpls enable
!
interface gigabitethernet 0/1
 mpls ldp enable
 ip address 192.168.1.1 255.255.255.0
!
interface gigabitethernet 0/2
 mpls ldp enable
 ip address 192.168.2.1 255.255.255.0
 ip router isis
 mpls ldp enable
 label-switching
!
interface Loopback 1
 ip address 3.3.3.3 255.255.255.255
 ip router isis
!
router isis
 net 49.0001.0000.0000.0001.00
!
router ospf 1
 redistribute static subnets
 network 192.168.1.0 0.0.0.255 area 0
!
mpls router ldp
 ldp router-id interface Loopback 1 force
!
recursive-route to mpls
!
ip route 2.2.2.0 255.255.255.0 5.5.5.5
```

- LSR1 configuration file

```
hostname LSR1
!
mpls enable
!
interface gigabitethernet 0/1
 ip address 192.168.2.2 255.255.255.0
 ip router isis
 mpls ldp enable
 label-switching
!
interface gigabitethernet 0/2
 ip address 192.168.3.1 255.255.255.0
 ip router isis
 mpls ldp enable
```

```
 label-switching
!
interface Loopback 1
 ip address 4.4.4.4 255.255.255.255
 ip router isis
!
mpls router ldp
 ldp router-id interface Loopback 1 force
!
router isis
 net 49.0001.0000.0000.0002.00
!
mpls router ldp
 ldp router-id interface Loopback 1 force
!
```

- LER2 configuration file

```
hostname LER2
!
mpls enable
!
interface gigabitethernet 0/1
 mpls ldp enable
 ip address 192.168.4.1 255.255.255.0
!
interface gigabitethernet 0/2
 mpls ldp enable
 ip address 192.168.3.2 255.255.255.0
 ip router isis
 mpls ldp enable
 label-switching
!
interface Loopback 1
 ip address 5.5.5.5 255.255.255.255
 ip router isis
!
router isis
 net 49.0001.0000.0000.0003.00
!
router ospf 1
 redistribute static subnets
 network 192.168.4.0 0.0.0.255 area 0
!
mpls router ldp
 ldp router-id interface Loopback 1 force
!
recursive-route to mpls
```

```
!
ip route 1.1.1.0 255.255.255.0 3.3.3.3
```

- CE2 configuration file

```
hostname CE2
!
interface gigabitethernet 0/1
 mpls ldp enable
 ip address 192.168.4.2 255.255.255.0
!
interface Loopback 1
 ip address 2.2.2.2 255.255.255.255
!
router ospf 1
 network 2.2.2.0 0.0.0.255 area 0
 network 192.168.4.0 0.0.0.255 area 0
!
```

7. Common Errors

- MPLS forwarding is not enabled globally.
- LDP is not enabled on an interface.

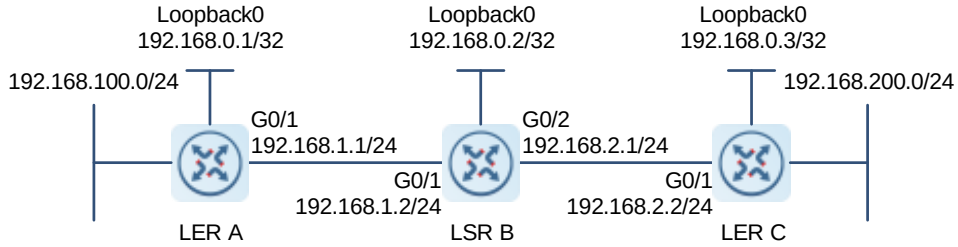
1.14.5 Configuring an MPLS Tunnel Policy

1. Requirements

Configure an MPLS tunnel policy.

2. Topology

Figure 1-2 Configuring an MPLS Tunnel Policy



3. Notes

- Configure interface IP addresses and an IPv4 unicast routing protocol (such as OSPF) on each device to implement route reachability between the devices.
- Enable the MPLS forwarding capability globally and configure LDP and an LDP router ID.
- Enable LDP and the ability to forward labeled packets on interfaces.
- Create a tunnel policy and configure a tunnel selection policy.

4. Procedure

(1) Configure interface IP addresses and OSPF on each device to implement route reachability between the devices.

Configure LER A.

```
LERA> enable
LERA# configure terminal
LERA(config)# interface gigabitethernet 0/1
LERA(config-if-GigabitEthernet 0/1)# ip address 192.168.1.1 255.255.255.0
LERA(config-if-GigabitEthernet 0/1)# exit
LERA(config)# interface loopback 0
LERA(config-if-Loopback 0)# ip address 192.168.0.1 255.255.255.255
LERA(config-if-Loopback 0)# exit
LERA(config)# router ospf 10
LERA(config-router)# network 192.168.1.0 0.0.0.255 area 0
LERA(config-router)# network 192.168.0.1 0.0.0.0 area 0
LERA(config-router)# network 192.168.100.0 0.0.0.255 area 0
LERA(config-router)# exit
```

Configure LSR B.

```
LSRB> enable
LSRB# configure terminal
LSRB(config)# interface gigabitethernet 0/1
LSRB(config-if-GigabitEthernet 0/1)# ip address 192.168.1.2 255.255.255.0
LSRB(config-if-GigabitEthernet 0/1)# exit
LSRB(config)# interface gigabitethernet 0/2
LSRB(config-if-GigabitEthernet 0/2)# ip address 192.168.2.1 255.255.255.0
LSRB(config-if-GigabitEthernet 0/2)# exit
LSRB(config)# interface loopback 0
LSRB(config-if-Loopback 0)# ip address 192.168.0.2 255.255.255.255
LSRB(config-if-Loopback 0)# exit
LSRB(config)# router ospf 10
LSRB(config-router)# network 192.168.1.0 0.0.0.255 area 0
LSRB(config-router)# network 192.168.2.0 0.0.0.255 area 0
LSRB(config-router)# network 192.168.0.2 0.0.0.0 area 0
LSRB(config-router)# exit
```

Configure LER C.

```
LERC> enable
LERC# configure terminal
LERC(config)# interface gigabitethernet 0/1
LERC(config-if-GigabitEthernet 0/1)# ip address 192.168.2.2 255.255.255.0
LERC(config-if-GigabitEthernet 0/1)# exit
LERC(config)# interface loopback 0
LERC(config-if-Loopback 0)# ip address 192.168.0.3 255.255.255.255
LERC(config-if-Loopback 0)# exit
LERC(config)# router ospf 10
LERC(config-router)# network 192.168.2.0 0.0.0.255 area 0
LERC(config-router)# network 192.168.0.3 0.0.0.0 area 0
LERC(config-router)# network 192.168.200.0 0.0.0.255 area 0
LERC(config-router)# exit
```

(2) Enable the MPLS forwarding capability globally and configure LDP and an LDP router ID. LER A is used as an example. Configurations on LER B and LER C are similar to those on LER A, and are omitted here.

```
LERA(config)# mpls enable
LERA(config)# mpls router ldp
LERA(config-mpls-router)# ldp router-id interface loopback 0 force
LERA(config-mpls-router)# exit
```

(3) Enable LDP and the ability to forward labeled packets on interfaces.

Configure LER A.

```
LERA(config)# interface gigabitethernet 0/1
LERA(config-if-GigabitEthernet 0/1)# mpls ldp enable
LERA(config-if-GigabitEthernet 0/1)# label-switching
LERA(config-if-GigabitEthernet 0/1)# exit
```

Configure LER B.

```
LSRB(config)# interface gigabitethernet 0/1
LSRB(config-if-GigabitEthernet 0/1)# mpls ldp enable
LSRB(config-if-GigabitEthernet 0/1)# label-switching
LSRB(config-if-GigabitEthernet 0/1)# exit
LSRB(config)# interface gigabitethernet 0/2
LSRB(config-if-GigabitEthernet 0/2)# mpls ldp enable
LSRB(config-if-GigabitEthernet 0/2)# label-switching
LSRB(config-if-GigabitEthernet 0/2)# end
```

Configure LER C.

```
LERC (config)# interface gigabitethernet 0/1
LERC(config-if-GigabitEthernet 0/1)# mpls ldp enable
LERC(config-if-GigabitEthernet 0/1)# label-switching
```

(4) Create a tunnel policy and configure a tunnel selection policy.

Configure LER A.

```
LERA(config)# tunnel-policy tun-pol
LERA(config-tunnel-policy)# tunnel select lsp
LERA(config-tunnel-policy)# end
```

5. Verification

Run the **show mpls tunnel-info all** command to check the public network tunnel information on LER A.

```
LERA# show mpls tunnel-info all
Total   tunnel-info num:    3
SRP      tunnel-info num:    0
LSP      tunnel-info num:    3
TE       tunnel-info num:    0
BE       tunnel-info num:    0
GRE      tunnel-info num:    0
TP       tunnel-info num:    0
 Tunnel-ID          Type          Destination
 0x00000001         LSP           192.168.0.2/32
```

```
0x00000003      LSP         192.168.0.3/32
0x00000002      LSP         192.168.2.0/24
```

Run the **show mpls forwarding-table** command to check MPLS forwarding entries on LER A.

```
LERA# show mpls forwarding-table
Label Operation Code:
PH--PUSH label
PP--POP label
SW--SWAP label
SP--SWAP topmost label and push new label
DP--DROP packet
PC--POP label and continue lookup by IP or Label
PI--POP label and do ip lookup forward
PN--POP label and forward to nexthop
PM--POP label and do MAC lookup forward
PV--POP label and output to VC attach interface
IP--IP lookup forward
 s--stale
  Local    Outgoing OP FEC                  Outgoing          Nexthop          Uptime
  label    label                            interface
  --       imp-null PH 192.168.0.2/32       Gi0/1             192.168.1.2      00:06:32
  --       92163      PH 192.168.0.3/32     Gi0/1               192.168.1.2      00:06:32
  --       imp-null PH 192.168.2.0/24       Gi0/1             192.168.1.2      00:06:32
  92162    imp-null PP 192.168.0.2/32       Gi0/1               192.168.1.2      00:06:32
  92163    imp-null PP 192.168.2.0/24       Gi0/1               192.168.1.2      00:06:32
  92164    92163      SW 192.168.0.3/32     Gi0/1               192.168.1.2      00:06:32
```

6. Configuration Files

- LER A configuration file

```
hostname LERA
!
mpls enable
!
interface gigabitethernet 0/1
 ip address 192.168.1.1 255.255.255.0
 mpls ldp enable
 label-switching
!
interface loopback 0
 ip address 192.168.0.1 255.255.255.255
!
router ospf 10
 network 192.168.0.1 0.0.0.0 area 0
 network 192.168.1.0 0.0.0.255 area 0
 network 192.168.100.0 0.0.0.255 area 0
!
mpls router ldp
```

```
 ldp router-id interface loopback 0 force
!
tunnel-policy tun-pol
 tunnel select lsp
!
```

- LSR B configuration file

```
hostname LSRB
!
mpls enable
!
interface gigabitethernet 0/1
 ip address 192.168.1.2 255.255.255.0
 mpls ldp enable
 label-switching
!
interface gigabitethernet 0/2
 ip address 192.168.2.1 255.255.255.0
 mpls ldp enable
 label-switching
!
interface loopback 0
 ip address 192.168.0.2 255.255.255.255
!
router ospf 10
 network 192.168.0.2 0.0.0.0 area 0
 network 192.168.1.0 0.0.0.255 area 0
 network 192.168.2.0 0.0.0.255 area 0
!
mpls router ldp
 ldp router-id interface loopback 0 force
!
```

- LER C configuration file

```
hostname LERC
!
mpls enable
!
interface gigabitethernet 0/1
 ip address 192.168.2.2 255.255.255.0
 mpls ldp enable
 label-switching
!
interface loopback 0
 ip address 192.168.0.3 255.255.255.255
!
router ospf 10
 network 192.168.0.3 0.0.0.0 area 0
```

```
 network 192.168.2.0 0.0.0.255 area 0
 network 192.168.200.0 0.0.0.255 area 0
!
mpls router ldp
 ldp router-id interface loopback 0 force
!
```

Contents

1 Configuring MPLS GR

1.1 Introduction

1.1.1 Overview

Multiprotocol Label Switching (MPLS) Graceful Restart (GR) indicates that the packet forwarding path remains unchanged and system data forwarding is not interrupted during Label Distribution Protocol (LDP) restart, ensuring high reliability for MPLS application services. MPLS GR functions include LDP GR and layer 3 VPN (L3VPN) GR.

LDP GR indicates uninterruptable data forwarding of a device upon an active/standby switchover or LDP restart with the help of a neighboring device.

1.1.2 GR Devices

1. GR Devices Classified by Capability

GR devices are classified by capability into GR-capable devices, GR-aware devices, and GR-unaware devices.

- GR-capable devices

  A GR-capable router has the GR capability and is equipped with two Supervisor Engines working in 1+1 master/slave mode generally. During a switchover between the master and slave Supervisor Engines, the GR-capable router sends an advertisement packet to its neighboring devices and inform them to keep its forwarding entries. After the switchover between the master and slave Supervisor Engines, routing tables are re-established without causing route flapping or changing the packet forwarding path, thus guaranteeing uninterrupted data forwarding in the system.

- GR-aware devices

  A GR-aware router has the GR detection capability. It may not be equipped with two Supervisor Engines but can detect GR of its neighbors and assist its neighbors completing GR.

- GR-unaware devices

  A GR-unaware router does not have the GR detection capability. It cannot detect GR of its neighbors or assist its neighbors completing GR. Generally, the system software of a GR-unaware device does not support the GR function or the GR function is disabled.

2. GR Devices Classified by Role

GR devices are classified by role during router restart into GR restarters and GR helpers.

- GR restarters
- A GR restarter has the GR capability, such as a GR-capable device, and its restart is triggered by administrators or faults.
- GR helpers

  A GR helper is a neighbor of a GR restarter. It must have at least the GR detection capability, for example, a GR-capable device or GR-aware device.

1.1.3 MPLS GR

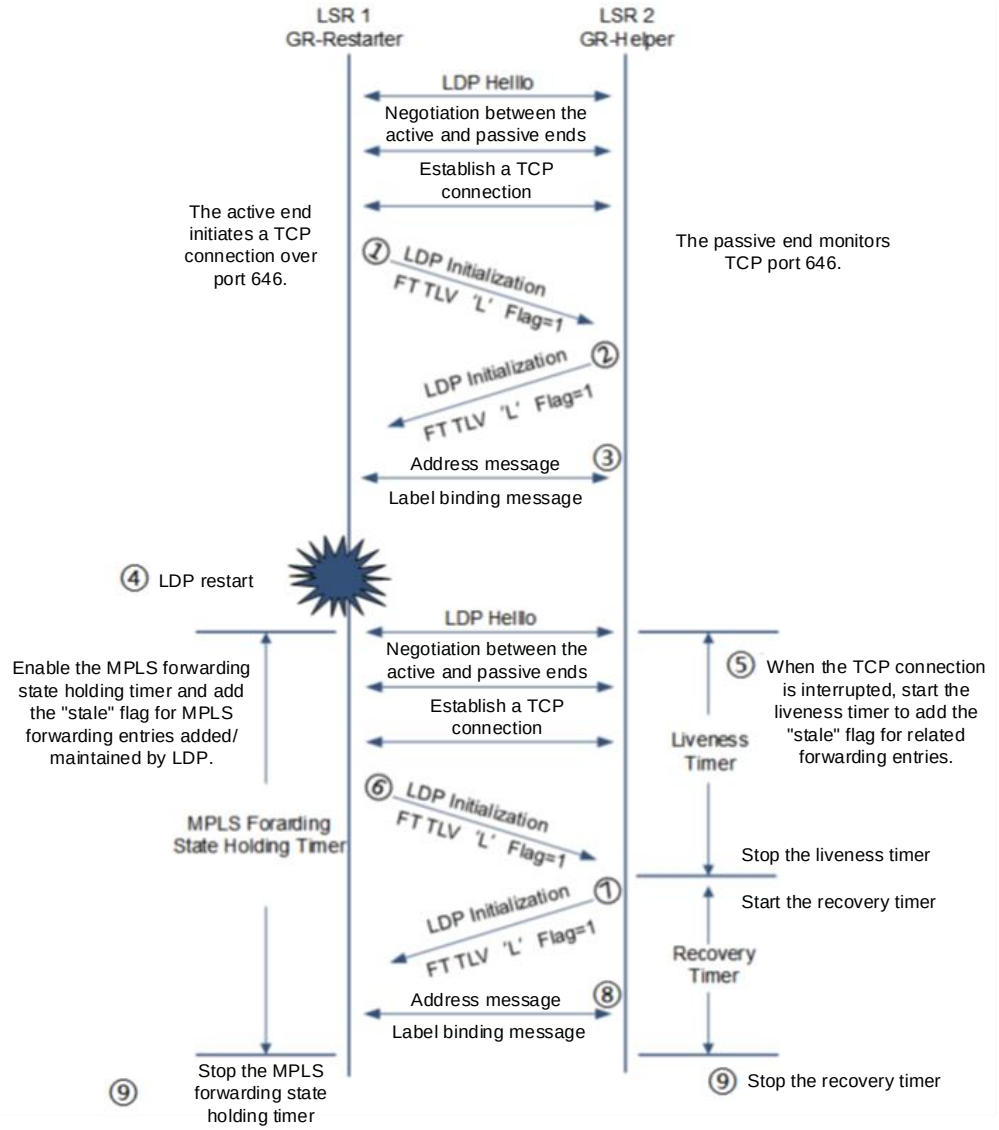
LDP GR can be used together with Interior Gateway Protocol (IGP) GR to ensure uninterruptable data forwarding in a common MPLS network, and be used together with Border Gateway Protocol (BGP) GR to ensure uninterruptable data forwarding in an L3VPN. The extended LDP GR function has the same implementation principles as the basic LDP GR function. The only difference is the backup MPLS forwarding entries. This section mainly describes the working principles of LDP GR.

To establish a GR-capable LDP session, devices at both ends of the session need to support and enable LDP GR. If LDP GR is not supported by any end during LDP session establishment, a common LDP session is established. If the session initiator supports and enables LDP GR, it includes **FT Session TLV** in the Initialization message.

After receiving an Initialization message carrying **FT Session TLV** during LDP session establishment, the receiver determines whether to carry **FT Session TLV** in the Initialization message according to its own situation. If the receiver supports and enables LDP GR, it carries **FT Session TLV** in the Initialization message to establish a GR-capable LDP session. If the receiver does not carry **FT Session TLV** in the Initialization message, a common LDP session without GR capability is established. If the Initialization message received by the receiver does not carry **FT Session TLV**, a common LDP session without GR capability is established no matter whether the receiver carries **FT Session TLV** in the Initialization message.

Figure 1-1 shows the process of establishing an LDP session between two label switching devices (LSRs) that support LDP GR.

Figure 1-1 LDP GR Process



(1) LSR 1 carries the optional parameter **FT Session TLV** in the Initialization message sent to LSR 2 to indicate its support to LDP GR.

(2) After receiving the Initialization message, LSR 2 also carries the optional parameter **FT Session TLV** in the Initialization message to LSR 1 since it supports LDP GR.

(3) After LSR 1 receives the Initialization message from LSR 2, a GR-capable LDP session is established.

(4) LSR 1 and LSR 2 exchange address information and label mapping information.

(5) For some reasons, the LDP process of LSR 1 is restarted. LSR 1 retains all MPLS forwarding entries added/maintained by LDP, marks them as "stale", and enables the MPLS forwarding state holding timer.

(6) LSR 2 detects that its GR-capable LDP session with LSR 1 is disconnected. It retains the MPLS forwarding entries related to this session and marks them as "stale". Meanwhile, it uses the smaller value between **Liveness Timer** configured and **FT Reconnect Timeout** in **FT Session TLV** received to start the liveness timer and retains these "stale" forwarding entries before the timer expires.

(7) When LSR 1 reestablishes a session with LSR 2, it sets **Recovery Time** in **FT Session TLV** carried by the Initialization message to the residual value of the MPLS forwarding state holding timer.

(8) After receiving the Initialization message carrying **FT Session TLV** sent by LSR 1, LSR 2 detects that **Recovery Time** is not **0**. It continues to retain the "stale" forwarding entries and stop the liveness timer at the same time. Meanwhile, it uses the smaller value between **Recovery Time** configured and **Recovery Time** in **FT Session TLV** received to start the recovery timer, and retains these "stale" forwarding entries before the timer expires.

(9) LSR 1 and LSR 2 re-exchange address information and label mapping information, and remove or retain MPLS forwarding entries marked as "stale" according to the information exchanged.

(10) The GR process ends. LSR 1 and LSR 2 delete their own MPLS forwarding entries marked as "stale".

1.1.4 Protocols and Standards

- RFC 3036: LDP Specification
- RFC 3037: LDP Applicability
- RFC 3215: LDP State Machine
- RFC 3478: Graceful Restart Mechanism for Label Distribution Protocol
- RFC 3479: Fault Tolerance for the Label Distribution Protocol (LDP)
- RFC 4724: Graceful Restart Mechanism for BGP
- RFC 4781: Graceful Restart Mechanism for BGP with MPLS

1.2 Configuration Task Summary

MPLS GR configuration includes the following tasks:

- Configuring LDP GR

1.3 Configuring LDP GR

1.3.1 Overview

When an LDP restart or manual master/slave switchover occurs, a device with LDP GR enabled can retain original MPLS forwarding entries and forward packets based on the original entries, ensuring uninterruptable traffic forwarding.

- LDP neighbor liveness time
  - Only GR helpers use the LDP neighbor liveness time.
  - A GR helper uses the smaller value between configured *neighbor-liveness-time* and received LDP session reconnection time to start the liveness timer and retains these "stale" forwarding entries before the timer expires.
- LDP session reconnection time
  - During the GR process, both the GR restarter and GR helper use the LDP session reconnection time.
  - For the GR restarter, the LDP session reconnection time is the time for retaining "stale" forwarding entries.
- LDP session recovery time
  - Only GR helpers use the LDP session recovery time.
  - A GR helper uses the smaller value between configured *recovery-time* and received LDP session recovery time to start the recovery timer and retains these "stale" forwarding entries before the timer

expires.

1.3.2 Restrictions and Guidelines

- The LDP neighbor liveness time is the time when the GR helper waits for the GR restarter to restart and reestablish a session. If it takes a long time for the GR restarter to restart, increase the LDP neighbor liveness time.
- The LDP session reconnection time is the time when the GR restarter retains "stale" forwarding entries. If many services and MPLS entries are configured on a device, it takes a long time to reconnect to a neighbor when a fault occurs. To ensure that the neighbor can wait for the local device to complete a restart, adjust *reconnection-time* of the local device and LDP neighbor liveness time of the neighboring device. In typical layer 3 virtual private network (L3VPN) scenarios, the time is increased by one minute for every 100 VPN services.
- The LDP session recovery time is the time when the helper assists the restarter in recovering entries after a session is reestablished between the helper and restarter. When many MPLS entries exist, it takes a long time to recover entries and therefore the LDP session recovery time needs to be prolonged.
- Enabling LDP GR does not affect the LDP session, namely it does not cause an LDP session restart or other exceptions.
- New LDP GR changes take effect after the LDP session is restarted and do not affect previously established LDP sessions.
- The new LDP neighbor liveness time takes effect after the LDP session is restarted.
- The new LDP session reconnection time takes effect after the LDP session is restarted.
- The new LDP session recovery time takes effect after the LDP session is restarted.
- If the topology is changed during GR (for example, the IP address corresponding to the LSR ID used before GR is deleted or the link is changed), GR may be invalid and causes traffic interruption.

1.3.3 Prerequisites

- Before configuring MPLS LDP GR, complete the following tasks:
  - Configure IGP GR.
  - Configure an MPLS LDP session.
- Before configuring MPLS LDP GR, prepare the following data:
  - LDP neighbor liveness time
  - LDP session reconnection time
  - LDP session recovery time

1.3.4 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enable LDP and enter the LDP configuration mode.

mpls router ldp [*vrf-name*]

(4) Enable LDP GR.

graceful-restart

LDP GR is enabled automatically for devices enabled with LDP by default.

The GR function is enabled by default to support process restart. Unless otherwise specified, do not disable the LDP GR function.

(5) (Optional) Configure the LDP neighbor liveness time.

graceful-restart timer neighbor-liveness *neighbor-liveness-time*

The default LDP neighbor liveness time is 600s.

(6) (Optional) Configure the LDP session reconnection time.

graceful-restart timer reconnect *reconnect-time*

The default LDP session reconnection time is 300s.

(7) (Optional) Configure the LDP session recovery time.

graceful-restart timer recovery *recovery-time*

The default LDP session recovery time is 300s.

1.4 Monitoring

Run the **show** command to check the configuration.

Run the **debug** command to output debugging information.

⚠ Caution

Debugging occupies system resources, so disable it immediately if not required.

Table 1-1 Monitoring

Command	Purpose
show mpls ldp graceful-restart [**all** | **vrf** *vrf-name*]	Displays LDP GR sessions and session parameters.
show mpls ldp neighbor [**all** | **vrf** *vrf-name*] [*ipv4-address*] [**detail**]	Displays whether GR is enabled for LDP sessions.
debug mpls ldp graceful-restart	Debugs LDP GR.

1.5 Configuration Examples

1.5.1 Configuring LDP GR

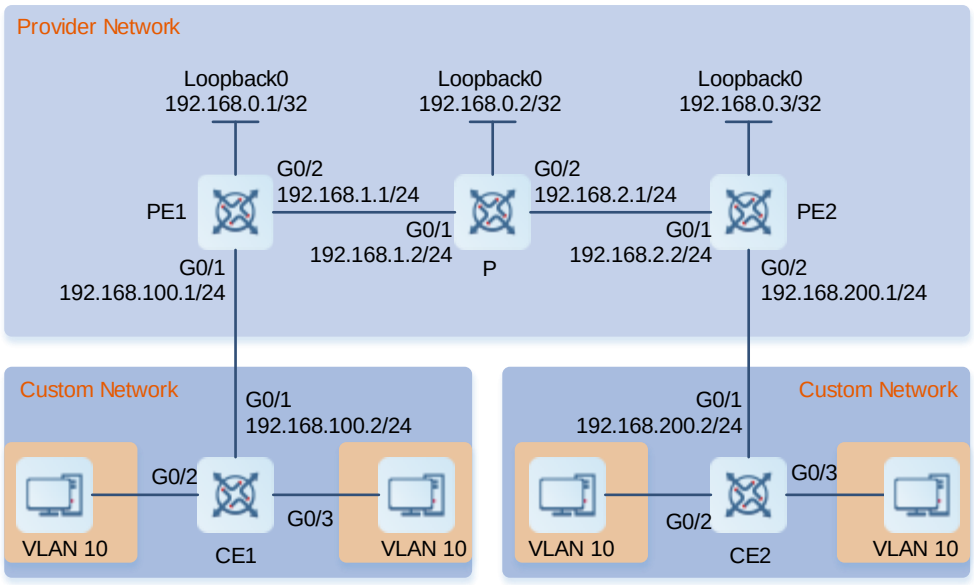
1. Requirements

Data forwarding is not interrupted upon a master/slave switchover or an LDP restart.

- Provider edges (PEs) and provider (P) form an MPLS network.
- PEs and P support LDP and have the GR capability.
- Use PE1 and P as examples to configure the LDP GR function. PE1 is a GR-capable device and serves as the GR restarter, and P is a GR-aware device and serves as the GR helper.

2. Topology

Figure 1-2 Configuring LDP GR



3. Notes

- Configure interface IP addresses and Open Shortest Path First (OSPF) on devices to ensure communication between them.
- Enable MPLS forwarding globally and on interfaces and configure LDP to ensure MPLS traffic forwarding in the network.
- Enable OSPF GR and LDP GR, and configure LDP GR parameters.
- Restart the LDP session for the configurations to take effect.

4. Procedure

(1) Configure interface IP addresses and OSPF on devices to ensure communication between them.

Configure PE1.

```
PE1> enable
PE1# configure terminal
PE1(config)# interface gigabitethernet 0/1
PE1(config-if-Gigabitethernet 0/1)# ip address 192.168.100.1 255.255.255.0
PE1(config-if-Gigabitethernet 0/1)# exit
PE1(config)# interface gigabitethernet 0/2
PE1(config-if-Gigabitethernet 0/2)# ip address 192.168.1.1 255.255.255.0
PE1(config-if-Gigabitethernet 0/2)# exit
```

```
PE1(config)# interface loopback 0
PE1(config-Loopback 0)# ip address 192.168.0.1 255.255.255.255
PE1(config-Loopback 0)# exit
PE1(config)# router ospf 1
PE1(config-router)# network 192.168.100.0 0.0.0.255 area 0
PE1(config-router)# network 192.168.1.0 0.0.0.255 area 0
PE1(config-router)# network 192.168.0.1 0.0.0.0 area 0
PE1(config-router)# exit
```

Configure P.

```
P> enable
P# configure terminal
P(config)# interface gigabitethernet 0/1
P(config-if-Gigabitethernet 0/1)# ip address 192.168.1.2 255.255.255.0
P(config-if-Gigabitethernet 0/1)# exit
P(config)# interface gigabitethernet 0/2
P(config-if-Gigabitethernet 0/2)# ip address 192.168.2.1 255.255.255.0
P(config-if-Gigabitethernet 0/2)# exit
P(config)# interface loopback 0
P(config-Loopback 0)# ip address 192.168.0.2 255.255.255.255
P(config-Loopback 0)# exit
P(config)# router ospf 1
P(config-router)# network 192.168.1.0 0.0.0.255 area 0
P(config-router)# network 192.168.2.0 0.0.0.255 area 0
P(config-router)# network 192.168.0.2 255.255.255.255 area 0
P(config-router)# exit
```

(2) Configure MPLS forwarding and LDP.

Configure PE1.

```
PE1(config)# mpls enable
PE1(config)# interface gigabitethernet 0/2
PE1(config-if-Gigabitethernet 0/2)# label-switching
PE1(config-if-Gigabitethernet 0/2)# mpls ldp enable
PE1(config-if-Gigabitethernet 0/2)# exit
PE1(config)# mpls router ldp
PE1(config-mpls-router)# ldp router-id interface loopback 0 force
PE1(config-mpls-router)# exit
```

Configure P.

```
P(config)# mpls enable
P(config)# interface gigabitethernet 0/1
P(config-if-Gigabitethernet 0/1)# label-switching
P(config-if-Gigabitethernet 0/1)# mpls ldp enable
P(config-if-Gigabitethernet 0/1)# exit
P(config)# interface gigabitethernet 0/2
P(config-if-Gigabitethernet 0/2)# label-switching
P(config-if-Gigabitethernet 0/2)# mpls ldp enable
```

```
P(config-if-Gigabitethernet 0/2)# exit
P(config)# mpls router ldp
P(config-mpls-router)# ldp router-id interface loopback 0 force
P(config-mpls-router)# exit
```

(3) Enable OSPF GR and LDP GR, and configure LDP GR parameters.

Configure PE1.

```
PE1(config)# router ospf 1
PE1(config-router)# graceful-restart
PE1(config-router)# exit
PE1(config)# mpls router ldp
PE1(config-mpls-router)# graceful-restart
PE1(config-mpls-router)# graceful-restart timer reconnect 300
PE1(config-mpls-router)# graceful-restart timer neighbor-liveness 120
PE1(config-mpls-router)# graceful-restart timer recovery 120
PE1(config-mpls-router)# end
```

Configure P.

```
P(config)# router ospf 1
P(config-router)# graceful-restart
P(config-router)# exit
P(config)# mpls router ldp
P(config-mpls-router)# graceful-restart
P(config-mpls-router)# graceful-restart timer reconnect 300
P(config-mpls-router)# graceful-restart timer neighbor-liveness 120
P(config-mpls-router)# graceful-restart timer recovery 120
P(config-mpls-router)# end
```

(4) Restart the LDP session for the configurations to take effect. PE1 is used as an example. Configurations on P are similar to those on PE1.

Configure PE1.

```
PE1# clear mpls ldp neighbor all
```

5. Verification

On PE1 and P, run the **show mpls ldp graceful-restart** command to display GR-capable LDP sessions and run the **show mpls ldp neighbors** command to check whether a session has the GR capability.

PE1 verification result

```
PE1# show mpls ldp graceful-restart
Default VRF:
  LDP Graceful Restart is enabled
  Neighbor Liveness Timer: 120 seconds
  Max Recovery Time: 120 seconds
  Forwarding State Holding Time: 300 seconds
  Down Neighbor Database (0 records):
  Graceful Restart-enabled Sessions:
    Peer LDP Ident: 192.168.0.2:0, State: estab
PE1# show mpls ldp neighbor
```

```
Default VRF:
   Peer LDP Ident: 192.168.0.2:0; Local LDP Ident: 192.168.0.1:0
      TCP connection: 192.168.0.2.36659 - 192.168.0.1.646
      State: OPERATIONAL; Msgs sent/recv: 103/107; UNSOLICITED
      Up time: 00:20:59
      Graceful Restart enabled; Peer reconnect time (msecs): 300000
      LDP discovery sources:
        Link Peer on GigabitEthernet 0/2, Src IP addr: 192.168.1.2
      Addresses bound to peer LDP Ident:
        192.168.0.2    192.168.1.2
```

P verification result

```
P# show mpls ldp graceful-restart
Default VRF:
  LDP Graceful Restart is enabled
  Neighbor Liveness Timer: 120 seconds
  Max Recovery Time: 120 seconds
  Forwarding State Holding Time: 300 seconds
  Down Neighbor Database (0 records):
  Graceful Restart-enabled Sessions:
    Peer LDP Ident: 192.168.0.1:0, State: estab
P# show mpls ldp neighbor
Default VRF:
   Peer LDP Ident: 192.168.0.1:0; Local LDP Ident: 192.168.0.2:0
      TCP connection: 192.168.0.1.646 - 192.168.0.2.36659
      State: OPERATIONAL; Msgs sent/recv: 106/105; UNSOLICITED
      Up time: 00:21:02
      Graceful Restart enabled; Peer reconnect time (msecs): 300000
      LDP discovery sources:
        Link Peer on GigabitEthernet 0/1, Src IP addr: 192.168.1.1
      Addresses bound to peer LDP Ident:
        192.168.0.1    192.168.1.1
```

6. Configuration Files

PE1 configuration file

```
hostname PE1
!
mpls enable
!
interface GigabitEthernet 0/1
 ip address 192.168.100.1 255.255.255.0
!
interface GigabitEthernet 0/2
 ip address 192.168.1.1 255.255.255.0
 mpls ldp enable
 label-switching
```

```
!
interface Loopback 0
 ip address 192.168.0.1 255.255.255.255
!
router ospf 1
 graceful-restart
 network 192.168.0.1 0.0.0.0 area 0
 network 192.168.1.0 0.0.0.255 area 0
 network 192.168.100.0 0.0.0.255 area 0
!
mpls router ldp
 ldp router-id interface Loopback 0 force
 graceful-restart
!
```

- P configuration file

```
hostname P
!
mpls enable
!
interface GigabitEthernet 0/1
 ip address 192.168.1.2 255.255.255.0
 mpls ldp enable
 label-switching
!
interface GigabitEthernet 0/2
 ip address 192.168.2.1 255.255.255.0
 mpls ldp enable
 label-switching
!
interface Loopback 0
 ip address 192.168.0.2 255.255.255.255
!
router ospf 1
 graceful-restart
 network 192.168.0.2 0.0.0.0 area 0
 network 192.168.1.0 0.0.0.255 area 0
 network 192.168.2.0 0.0.0.255 area 0
!
mpls router ldp
 ldp router-id interface Loopback 0 force
 graceful-restart
!
```

1.5.2 Configuring L3VPN GR

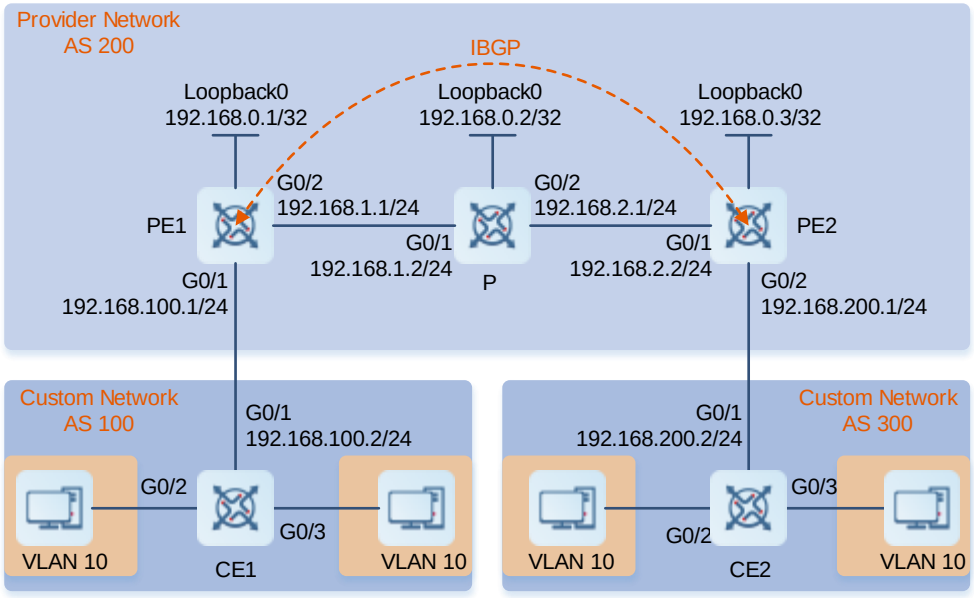
1. Requirements

Data forwarding of L3VPN services is not interrupted. When the control plane of a device is faulty, the forwarding plane can still forward VPN data normally. This ensures that VPN services in the network are not affected.

- CEs represent the customer network and run IGP or External BGP (EBGP).
- PEs and P form an ISP network and run IGP.
- A label switched path (LSP) is established among PE1, P, and PE2 using LDP.
- A private network tunnel is established between PE1 and PE2 using Internal BGP (IBGP).
- IGP, GBP, and LDP have the GR capability.
- PEs are GR-capable devices, and P is a GR-aware device.

2. Topology

Figure 1-3 Configuring L3VPN GR



3. Notes

- Configure interface IP addresses and OSPF on MPLS backbone network nodes to ensure communication between them.
- Enable MPLS forwarding globally and on interfaces and configure LDP to ensure MPLS traffic forwarding in the network.
- Configure VPN route instances on PE1 and PE2 and connect CE1 to PE1 and CE2 to PE2.
- Configure MP-IBGP neighbor relationship between PE1 and PE2 and between PE1 and PE3 to transmit VPN routing information.
- Enable OSPF GR, LDP GR, and BGP GR and configure LDP GR parameters. Restart the LDP session for the configurations to take effect.

4. Procedure

(1) Configure interface IP addresses and OSPF on MPLS backbone network nodes to ensure communication between them.

Configure PE1.

```
PE1> enable
PE1# configure terminal
PE1(config)# interface gigabitethernet 0/2
PE1(config-if-Gigabitethernet 0/2)# ip address 192.168.1.1 255.255.255.0
PE1(config-if-Gigabitethernet 0/2)# exit
PE1(config)# interface loopback 0
PE1(config-Loopback 0)# ip address 192.168.0.1 255.255.255.255
PE1(config-Loopback 0)# exit
PE1(config)# router ospf 10
PE1(config-router)# network 192.168.0.1 0.0.0.0 area 0
PE1(config-router)# network 192.168.1.0 0.0.0.255 area 0
PE1(config-router)# exit
```

Configure P.

```
P> enable
P# configure terminal
P(config)# interface gigabitethernet 0/1
P(config-if-Gigabitethernet 0/1)# ip address 192.168.1.2 255.255.255.0
P(config-if-Gigabitethernet 0/1)# exit
P(config)# interface gigabitethernet 0/2
P(config-if-Gigabitethernet 0/2)# ip address 192.168.2.1 255.255.255.0
P(config-if-Gigabitethernet 0/2)# exit
P(config)# interface loopback 0
P(config-Loopback 0)# ip address 192.168.0.2 255.255.255.255
P(config-Loopback 0)# exit
P(config)# router ospf 10
P(config-router)# network 192.168.1.0 0.0.0.255 area 0
P(config-router)# network 192.168.2.0 0.0.0.255 area 0
P(config-router)# network 192.168.0.2 0.0.0.0 area 0
P(config-router)# exit
```

Configure PE2.

```
PE2> enable
PE2# configure terminal
PE2(config)# interface gigabitethernet 0/1
PE2(config-if-Gigabitethernet 0/1)# ip address 192.168.2.2 255.255.255.0
PE2(config-if-Gigabitethernet 0/1)# exit
PE2(config)# interface loopback 0
PE2(config-Loopback 0)# ip address 192.168.0.3 255.255.255.255
PE2(config-Loopback 0)# exit
PE2(config)# router ospf 10
PE2(config-router)# network 192.168.0.3 0.0.0.0 area 0
```

```
PE2(config-router)# network 192.168.2.0 0.0.0.255 area 0
PE2(config-router)# exit
```

(2) Enable MPLS forwarding globally and on interfaces and configure LDP to ensure MPLS traffic forwarding in the network.

Configure PE1.

```
PE1(config)# mpls enable
PE1(config)# interface gigabitethernet 0/2
PE1(config-if-Gigabitethernet 0/2)# label-switching
PE1(config-if-Gigabitethernet 0/2)# mpls ldp enable
PE1(config-if-Gigabitethernet 0/2)# exit
PE1(config)# mpls router ldp
PE1(config-mpls-router)# ldp router-id interface loopback 0 force
PE1(config-mpls-router)# exit
```

Configure P.

```
P(config)# mpls enable
P(config)# interface gigabitethernet 0/1
P(config-if-Gigabitethernet 0/1)# label-switching
P(config-if-Gigabitethernet 0/1)# mpls ldp enable
P(config-if-Gigabitethernet 0/1)# exit
P(config)# interface gigabitethernet 0/2
P(config-if-Gigabitethernet 0/2)# label-switching
P(config-if-Gigabitethernet 0/2)# mpls ldp enable
P(config-if-Gigabitethernet 0/2)# exit
P(config)# mpls router ldp
P(config-mpls-router)# ldp router-id interface loopback 0 force
P(config-mpls-router)# exit
```

Configure PE2.

```
PE2(config)#mpls enablep
PE2(config)# interface gigabitethernet 0/1
PE2(config-if-Gigabitethernet 0/1)# label-switching
PE2(config-if-Gigabitethernet 0/1)# mpls ldp enable
Router(config-if-Gigabitethernet 0/1)# exit
PE2(config)# mpls router ldp
PE2(config-mpls-router)# ldp router-id interface loopback 0 force
PE2(config-mpls-router)# exit
```

(3) Configure VPN route instances on PE1 and PE2 and connect CE1 to PE1 and CE2 to PE2.

Configure PE1.

```
PE1(config)# ip vrf 10
PE1(config-vrf)# rd 1:100
PE1(config-vrf)# route-target both 1:100
PE1(config-vrf)# exit
PE1(config)# interface gigabitethernet 0/1
PE1(config-if-Gigabitethernet 0/1)# ip vrf forwarding 10
PE1(config-if-Gigabitethernet 0/1)# ip address 192.168.100.1 255.255.255.0
```

```
PE1(config-if-Gigabitethernet 0/1)# exit
```

Configure PE2.

```
PE2> enable
PE2# configure terminal
PE2(config)# ip vrf 10
PE2(config-vrf)# rd 1:100
PE2(config-vrf)# route-target both 1:100
PE2(config-vrf)# exit
PE2(config)# interface gigabitethernet 0/2
PE2(config-if-Gigabitethernet 0/2)# ip vrf forwarding 10
PE2(config-if-Gigabitethernet 0/2)# ip address 192.168.200.1 255.255.255.0
PE2(config-if-Gigabitethernet 0/2)# exit
```

(4) Configure MP-IBGP neighbor relationship between PE1 and PE2 to transmit VPN routing information.

Configure PE1.

```
PE1(config)# router bgp 200
PE1(config-router)# address-family ipv4 vrf 10
PE1(config-router-af)# neighbor 192.168.100.2 remote-as 100
PE1(config-router-af)# neighbor 192.168.100.2 update-source Gigabitethernet 0/1
PE1(config-router-af)# neighbor 192.168.200.2 activate
PE1(config-router-af)# exit-address-family
PE1(config-router)# address-family ipv4
PE1(config-router-af)# neighbor 192.168.0.3 remote-as 200
PE1(config-router-af)# neighbor 192.168.0.3 update-source loopback 0
PE1(config-router-af)# neighbor 192.168.0.3 activate
PE1(config-router-af)# exit-address-family
PE1(config-router)# address-family vpnv4 unicast
PE1(config-router-af)# neighbor 192.168.0.3 activate
PE1(config-router-af)# exit-address-family
PE1(config-router-af)# exit
```

Configure PE2.

```
PE2(config)# router bgp 200
PE2(config-router)# address-family ipv4 vrf 10
PE2(config-router-af)# neighbor 192.168.200.2 remote-as 300
PE2(config-router-af)# neighbor 192.168.200.2 update-source Gigabitethernet 0/2
PE2(config-router-af)# neighbor 192.168.100.2 activate
PE2(config-router-af)# exit-address-family
PE2(config-router)# address-family ipv4
PE2(config-router-af)# neighbor 192.168.0.1 remote-as 200
PE2(config-router-af)# neighbor 192.168.0.1 update-source loopback 0
PE2(config-router-af)# neighbor 192.168.0.1 activate
PE2(config-router-af)# exit-address-family
PE2(config-router)# address-family vpnv4 unicast
PE2(config-router-af)# neighbor 192.168.0.1 activate
PE2(config-router-af)# exit-address-family
```

```
PE2(config-router-af)# exit
```

(5) Enable OSPF GR, LDP GR, and BGP GR and configure LDP GR parameters.

Configure PE1.

```
PE1(config)# router ospf 10
PE1(config-router)# graceful-restart
PE1(config-router)# exit
PE1(config)# mpls router ldp
PE1(config-mpls-router)# graceful-restart
PE1(config-mpls-router)# graceful-restart timer reconnect 300
PE1(config-mpls-router)# graceful-restart timer neighbor-liveness 120
PE1(config-mpls-router)# graceful-restart timer recovery 120
PE1(config-mpls-router)# exit
PE1(config)# router bgp 200
PE1(config-router)# bgp graceful-restart
PE1(config-router)# end
```

Configure P.

```
P(config)# router ospf 10
P(config-router)# graceful-restart
P(config-router)# exit
P(config)# mpls router ldp
P(config-mpls-router)# graceful-restart
P(config-mpls-router)# graceful-restart timer reconnect 300
P(config-mpls-router)# graceful-restart timer neighbor-liveness 120
P(config-mpls-router)# graceful-restart timer recovery 120
P(config-mpls-router)# end
```

Configure PE2.

```
PE2(config)# router ospf 10
PE2(config-router)# graceful-restart
PE2(config-router)# exit
PE2(config)# mpls router ldp
PE2(config-mpls-router)# graceful-restart
PE2(config-mpls-router)# graceful-restart timer reconnect 300
PE2(config-mpls-router)# graceful-restart timer neighbor-liveness 120
PE2(config-mpls-router)# graceful-restart timer recovery 120
PE2(config-mpls-router)# exit
PE2(config)# router bgp 200
PE2(config-router)# bgp graceful-restart
PE2(config-router)# end
```

(6) Restart the LDP session for the configurations to take effect. PE1 is used as an example. Configurations on P and PE2 are similar to those on PE1.

Configure PE1.

```
PE1# clear mpls ldp neighbor all
```

5. Verification

On PE1, P, and PE2, run the **show mpls ldp graceful-restart** command to display GR-capable LDP sessions and run the **show bgp vpnv4 unicast all neighbor** command to display the BGP neighbor status.

PE1 verification result

```
PE1# show mpls ldp graceful-restart
Default VRF:
  LDP Graceful Restart is enabled
  Neighbor Liveness Timer: 120 seconds
  Max Recovery Time: 120 seconds
  Forwarding State Holding Time: 300 seconds
  Down Neighbor Database (0 records):
  Graceful Restart-enabled Sessions:
    Peer LDP Ident: 192.168.0.2:0, State: estab
PE1# show bgp vpnv4 unicast all neighbor
BGP neighbor is 192.168.0.3, remote AS 200, internal link
BGP version 4, remote router ID 192.168.0.3
BGP state = Established, up for 02:49:47
Last read 00:00:47, hold time is 180, keepalive interval is 60 seconds
Neighbor capabilities:
Route refresh: advertised and received(new)
Address family VPNv4 Unicast: advertised and received
Graceful Restart Capabilty: advertised and received
Remote Restart timer is 120 seconds
Address families preserved by peer:
VPNv4 Unicast
```

P verification result

```
P# show mpls ldp graceful-restart
Default VRF:
  LDP Graceful Restart is enabled
  Neighbor Liveness Timer: 120 seconds
  Max Recovery Time: 120 seconds
  Forwarding State Holding Time: 300 seconds
  Down Neighbor Database (0 records):
  Graceful Restart-enabled Sessions:
Peer LDP Ident: 192.168.0.1:0, State: estab
Peer LDP Ident: 192.168.0.3:0, State: estab
```

PE2 verification result

```
PE2# show mpls ldp graceful-restart
Default VRF:
  LDP Graceful Restart is enabled
  Neighbor Liveness Timer: 120 seconds
  Max Recovery Time: 120 seconds
  Forwarding State Holding Time: 300 seconds
  Down Neighbor Database (0 records):
```

```
  Graceful Restart-enabled Sessions:
    Peer LDP Ident: 192.168.0.2:0, State: estab
PE2# show bgp vpnv4 unicast all neighbor
BGP neighbor is 192.168.0.1, remote AS 200, internal link
BGP version 4, remote router ID 192.168.0.1
BGP state = Established, up for 02:49:47
Last read 00:00:47, hold time is 180, keepalive interval is 60 seconds
Neighbor capabilities:
Route refresh: advertised and received(new)
Address family VPNv4 Unicast: advertised and received
Graceful Restart Capabilty: advertised and received
Remote Restart timer is 120 seconds
Address families preserved by peer:
VPNv4 Unicast
```

6. Configuration Files

PE1 configuration file

```
hostname PE1
!
ip vrf 10
 rd 1:100
 route-target both 1:100
!
mpls enable
!
interface GigabitEthernet 0/1
ip vrf forwarding 10
 ip address 192.168.100.1 255.255.255.0
!
interface GigabitEthernet 0/2
 ip address 192.168.1.1 255.255.255.0
 mpls ldp enable
 label-switching
!
interface Loopback 0
 ip address 192.168.0.1 255.255.255.255
!
router bgp 200
 bgp log-neighbor-changes
 bgp graceful-restart
 neighbor 192.168.0.3 remote-as 200
 neighbor 192.168.0.3 update-source Loopback 0
 address-family ipv4
  neighbor 192.168.0.3 activate
  exit-address-family
 address-family vpnv4 unicast
```

```
  neighbor 192.168.0.3 activate
  neighbor 192.168.0.3 send-community extended
  exit-address-family
  !
 address-family ipv4 vrf 10
  neighbor 192.168.100.2 remote-as 100
  neighbor 192.168.100.2 update-source GigabitEthernet 0/1
  neighbor 192.168.100.2 activate
  exit-address-family
!
router ospf 10
 graceful-restart
 network 192.168.0.1 0.0.0.0 area 0
 network 192.168.1.0 0.0.0.255 area 0
!
mpls router ldp
 ldp router-id interface Loopback 0 force
 graceful-restart timer reconnect 300
 graceful-restart timer recovery 120
 graceful-restart timer neighbor-liveness 120
 graceful-restart
!
```

P configuration file

```
hostname P
!
mpls enable
!
interface GigabitEthernet 0/1
 ip address 192.168.1.2 255.255.255.0
 mpls ldp enable
 label-switching
!
interface GigabitEthernet 0/2
 ip address 192.168.2.1 255.255.255.0
 mpls ldp enable
 label-switching
!
interface Loopback 0
 ip address 192.168.0.2 255.255.255.255
!
router ospf 10
 graceful-restart
 network 192.168.0.2 0.0.0.0 area 0
 network 192.168.1.0 0.0.0.255 area 0
 network 192.168.2.0 0.0.0.255 area 0
!
```

```
mpls router ldp
 ldp router-id interface Loopback 0 force
 graceful-restart timer reconnect 300
 graceful-restart timer recovery 120
 graceful-restart timer neighbor-liveness 120
 graceful-restart
!
```

PE2 configuration file

```
hostname PE2
!
ip vrf 10
 rd 1:100
 route-target both 1:100
!
mpls enable
!
interface GigabitEthernet 0/1
ip address 192.168.2.2 255.255.255.0
 mpls ldp enable
 label-switching
!
interface GigabitEthernet 0/2
ip vrf forwarding 10
 ip address 192.168.200.1 255.255.255.0
!
interface Loopback 0
 ip address 192.168.0.3 255.255.255.255
!
router bgp 200
 bgp log-neighbor-changes
 bgp graceful-restart
 neighbor 192.168.0.1 remote-as 200
 neighbor 192.168.0.1 update-source Loopback 0
 address-family ipv4
  neighbor 192.168.0.1 activate
  exit-address-family
 address-family vpnv4 unicast
  neighbor 192.168.0.1 activate
  neighbor 192.168.0.1 send-community extended
  exit-address-family
  !
 address-family ipv4 vrf 10
  neighbor 192.168.200.2 remote-as 300
  neighbor 192.168.200.2 update-source GigabitEthernet 0/2
  neighbor 192.168.200.2 activate
  exit-address-family
```

```
!
router ospf 10
 graceful-restart
 network 192.168.0.3 0.0.0.0 area 0
 network 192.168.2.0 0.0.0.255 area 0
!
mpls router ldp
 ldp router-id interface Loopback 0 force
 graceful-restart timer reconnect 300
 graceful-restart timer recovery 120
 graceful-restart timer neighbor-liveness 120
 graceful-restart
!
```

CE1 configuration file

```
hostname CE1
!
interface GigabitEthernet 0/1
 ip address 192.168.100.2 255.255.255.0
!
interface Loopback 0
ip address 1.1.1.1 255.255.255.255
!
router bgp 100
 neighbor 192.168.100.1 remote-as 1
 address-family ipv4
  network 1.1.1.1 mask 255.255.255.255
  neighbor 192.168.100.1 activate
  exit-address-family
!
```

CE2 configuration file

```
hostname CE2
!
interface GigabitEthernet 0/1
 ip address 192.168.200.2 255.255.255.0
!
interface Loopback 0
 ip address 2.2.2.2 255.255.255.255
!
router bgp 100
 neighbor 192.168.200.1 remote-as 1
 address-family ipv4
  network 2.2.2.2 mask 255.255.255.255
  neighbor 192.168.100.1 activate
  exit-address-family
!
```

1.6 Common Errors

- Basic MPLS or L3VPN environment setup is not complete. As a result, data forwarding fails.
- The GR function is configured on the restarter but not configured on the adjacent helper.
- The IGP or BGP GR function is not configured.
- Many routing entries exist, but the configured LDP GR timer time is short. As a result, some entries are not restored when GR is complete.
- The topology or configuration is changed during GR, resulting in traffic interruption.

2 MPLS BFD

Note

Routers and router icons involved in this section refer to routing devices and Layer 3 switches running a routing protocol. Router series products and switch series products are used to distinguish the specific device type.

2.1 Overview

2.1.1 MPLS BFD

MPLS BFD is implemented based on the BFD For MPLS LSPs standards defined in IETF. MPLS BFD provides methods to detect MPLS LSPs, and is an important application of BFD.

Note

For details about BFD, see "BFD" in *Reliability Configuration*.

Generally, the MPLS network uses the following methods to detect LSP faults:

- MPLS Operation, Administration and Maintenance (OAM): This mechanism can effectively detect, confirm, and locate internal defects or faults of the MPLS network. However, standardization of MPLS OAM mechanisms is still ongoing and various OAM mechanisms are just applying to actual networks. It cannot be guaranteed that network-wide devices support the OAM features.
- Hello packet mechanism using the MPLS signaling protocol: Fault detection using this mechanism takes a long time, usually several seconds. Therefore, it will lead to a large amount of traffic loss.

MPLS BFD can solve the above problems. It provides the following features:

- Interoperability: Provides detection mechanisms that are uniform on the entire network.
- Quick detection: It supports quick detection with light load to speed up backup forwarding path selection and improve the MPLS network reliability.

BFD can be used to detect data plane faults on the MPLS LSP forwarding path. In addition, BFD packets have fixed format, which are easily implemented on hardware and can traverse firewalls.

2.1.2 Basic Concepts

1. BFD Session

BFD uses the local discriminator and remote discriminator to distinguish multiple BFD sessions between the same pair of systems. The discriminators can be configured manually or automatically.

- In manual configuration mode, the BFD local discriminator and remote discriminator are configured manually. In this way, LSP Ping Echo packets do not need to carry the discriminator for negotiating and learning the remote discriminator before a BFD session can be created.
- In auto configuration mode, LSP Ping Echo packets need to carry the discriminator for negotiating and learning the remote discriminator before starting the BFD session establishment mechanism.

Currently, the software supports only the manual configuration.

2. BFD Detection Modes

Before two devices can exchange BFD control packets, a BFD session must be created to ensure the same path for the control plane and the data plane. Two modes are available for managing the BFD session.

- Asynchronous mode: The two ends of the session periodically send a control packet to each other. If one end fails to receive a control packet from the peer within the specified period, it considers the peer Down.
- Query mode: The two ends of the session do not send packets immediately after the session is established. They send a control packet to each other when connectivity check is required. If the peer does not reply, the local end considers the session Down.

Apart from the above two modes, BFD defines the Echo feature to send a custom packet to the peer. The peer returns the packet back to the sender without processing it. This feature can be used in both asynchronous mode and query mode.

Caution

Currently, association between BFD and LSP supports the asynchronous mode, but not the query mode or the Echo feature.

2.1.3 BFD Session Establishment

In the initial stage of BFD session establishment, packet sending devices on two ends play active and passive roles. The active or passive role of the ingress LSR and egress LSR is determined by the application. However, at least one end plays the active role. The working process of the initial stage is as follows:

1. Both Ends Are Active

As LSP is unidirectional and both ends play the active role, the working process varies as follows:

- Use BFD to detect one LSP from the ingress LSR to the egress LSR, and use BFD to detect another LSP from the egress LSR to the ingress LSR.

The ingress LSR sends an LSP Ping Echo Request packet carrying the local discriminator to the egress LSR. After the egress LSR receives the Echo Request packet, it obtains the remote discriminator from the Echo Request packet. In this way, the egress LSR owns the local discriminator (generated by itself) and the remote discriminator. After that, the egress LSR starts to send a BFD control packet to the ingress LSR. After the ingress LSR receives the BFD control packet, it obtains the remote discriminator from the received control packet. In this way, the ingress LSR owns the local discriminator (generated by itself) and the remote discriminator. After that, the ingress LSR starts to send a BFD control packet to the egress LSR. Until now, the ingress LSR and the egress LSR enter the initial stage of BFD session establishment.

It should be noted that, after the egress LSR receives an Echo Request packet, it can choose to send or not to send an Echo Reply packet. If the egress LSR sends an Echo Reply packet, the Echo Reply packet must carry the local discriminator (generated by itself). In this way, the ingress LSR can obtain the remote discriminator from the BFD control packet or Echo Reply packet.

Note

The working process of the egress LSR is similar to that of the ingress LSR, and is omitted here.

- Use BFD to detect one LSP from the ingress LSR to the egress LSR, and use BFD to detect IP addresses (multi-hop) from the egress LSR to the ingress LSR.

In this case, discriminators can only be configured manually on the ingress LSR and the egress LSR for creating a BFD session. It means that this working process does not engage automatic discriminator negotiation and the two ends start creating a BFD session immediately after the discriminators are manually configured.

2. One End Is Active and the Other End Is Passive

The active party sends an LSP Ping Echo Request packet carrying the local discriminator to the passive party. After the passive party receives the Echo Request packet, it obtains the remote discriminator from the Echo Request packet. In this way, the passive party owns the local discriminator (generated by itself) and the remote discriminator. After that, the passive party starts to send a BFD control packet to the active party. After the active party receives the BFD control packet, it obtains the remote discriminator from the received BFD control packet. In this way, the active party owns the local discriminator (generated by itself) and the remote discriminator. After that, the active party starts to send a BFD control packet to the passive party. Until now, the active party and the passive party enter the initial stage of BFD session establishment.

It should be noted that, after the passive party receives an Echo Request packet, it can choose to send or not to send an Echo Reply packet. If the passive party sends an Echo Reply packet, the Echo Reply packet must carry the local discriminator (generated by itself). In this way, the active party can obtain the remote discriminator from the BFD control packet or Echo Reply packet.

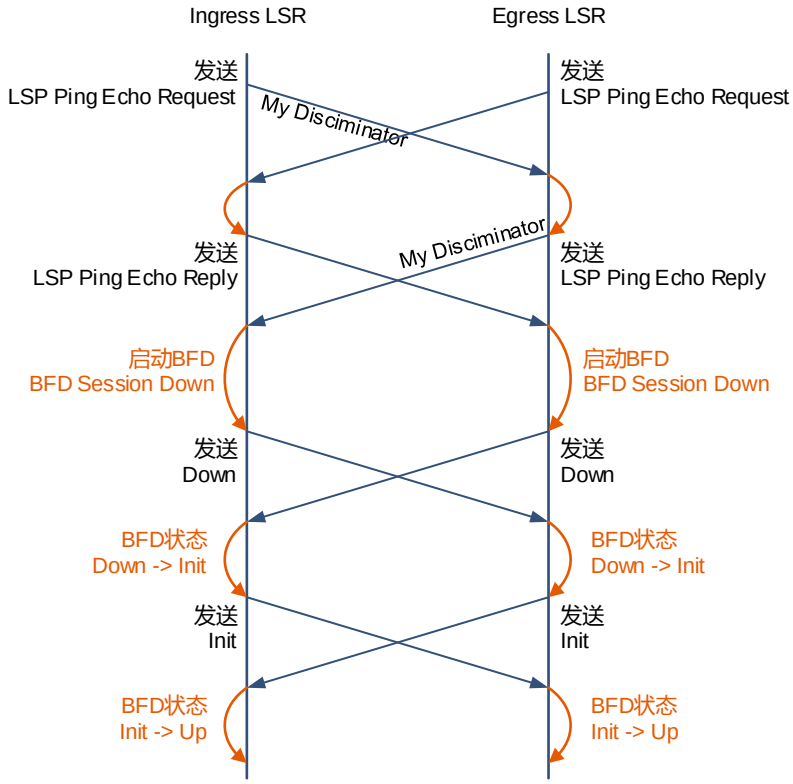
The passive party does not actively send a BFD control packet to the active party before it receives an Echo Request packet from the active party.

Note

Currently, association between BFD and LSP supports the case "Both Ends Are Active" but not the case "One End Is Active and the Other End Is Passive".

The following figure shows the BFD session establishment process when both ends are active and when BFD is used to detect one LSP from the ingress LSR to the egress LSR, and BFD is used to detect another LSP from the egress LSR to the ingress LSR.

Figure 1-1 BFD Session Establishment Process



- Before BFD is enabled on the ingress LSR and the egress LSR, the remote discriminator must be learned and the LSP status must be Up. As shown in the figure, the ingress LSR sends an LSP Ping Echo Request packet carrying the local discriminator to the egress LSR. After the egress LSR receives the Echo Request packet, it sends an Echo Reply packet carrying the local discriminator (generated by itself) to the ingress LSR. The working process on the egress LSR is similar and omitted here. It should be noted that if no discriminator is specified for both ends, the LSP Ping Echo packets must be exchanged to learn the remote discriminator. If the local discriminator and remote discriminator are specified for both ends, the two steps can be skipped in the BFD session establishment process. For details on the discriminator configuration, see the section "Association Between BFD and LSP".
- Start BFD on the ingress LSR and the egress LSR. In this step, the initial state of the ingress LSR and the egress LSR is Down. Send a BFD packet with the state Down.
- After the egress LSR receives the BFD packet with the Down state, it changes the BFD status to Init and sends a BFD packet with the state Init.
- After the local BFD status of the egress LSR changes to Init, it does not process BFD packets with the state Down any longer.
- The BFD status change is similar on the ingress LSR.
- After the egress LSR receives a BFD packet with the state Init, it changes the local BFD status to Up.
- The BFD status change is similar on the ingress LSR.
- The local BFD status Up indicates that a BFD session is created.

2.1.4 Protocols and Standards

- draft-ietf-bfd-base-09: Bidirectional Forwarding Detection
- draft-ietf-bfd-generic-05: Generic Application of BFD
- draft-ietf-bfd-mib-06: Bidirectional Forwarding Detection Management Information Base
- draft-ietf-bfd-v4v6-1hop-09: BFD for IPv4 and IPv6 (Single Hop)
- draft-ietf-bfd-multihop-07: BFD for IPv4 and IPv6 (Multihop)
- draft-ietf-bfd-mpls-07: BFD For MPLS LSPs

2.2 Configuration Task Summary

MPLS BFD for LSP configuration includes the following tasks:

- Configuring BFD for LSP
- Configuring BFD for Static LSP
- Configuring BFD for LDP LSP
- Configuring BFD for LDP Tunnel
- Configuring BFD for BGP LSP
- Configuring BFD for BGP Tunnel
- Configuring BFD for LSP

2.3 Configuring BFD for Static LSP

1. Overview

After you configure BFD to detect the connectivity of static LSPs and associate static LSPs with BFD, private network routes do not select a static LSP as the forwarding path when the associated static LSP fails.

2. Restrictions and Guidelines

- BFD for static LSP is applicable only to static LSPs established by host routes.
- If the ingress LSR uses the manual configuration mode, the egress LSR must also use the manual configuration mode.
- If discriminators are configured in manual configuration mode, the local discriminator and the remote discriminator configured on the ingress LSR must match those configured on the egress LSR.

3. Prerequisites

- Before you configure BFD for static LSP, the MPLS features must be enabled globally.
- Before you configure BFD for static LSP, the OSPF protocol and MPLS static routes must be configured to enable the network to forward MPLS traffic.
- Before you configure BFD for static LSP, the BFD session parameters must be configured, including the interval for sending BFD control packets, the interval for receiving BFD control packets, and the detection multiplier of BFD control packets.

4. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure BFD for static LSP.

bfd bind static-lsp peer-ip *peer-ip*v4-address **source-ip** source-ipv4-address [**local-discriminator** local-discriminator-value **remote-discriminator** remote-discriminator-value]

BFD for static LSP is disabled by default.

2.4 Configuring BFD for LDP LSP

1. Overview

After you configure BFD to detect the connectivity of LDP LSPs and associate LDP LSPs with BFD, traffic can be quickly switched from a faulty link to the secondary link. In addition, when the primary link becomes Down, private network routes do not select this link as the forwarding path.

2. Restrictions and Guidelines

- BFD for LDP LSP is applicable only to LDP LSPs established by host routes.
- Only one BFD session can be bound to an LSP.
- BFD can only be bound to the ingress node of an LDP LSP.
- If discriminators are configured in manual configuration mode, the local discriminator and the remote discriminator configured on the ingress LSR must match those configured on the egress LSR.
- When static BFD is used for LDP LSP detection, one static BFD session has the same effect as multiple BFD sessions. You are advised to configure one static BFD session.

3. Prerequisites

- Before you configure BFD for LDP LSP, the MPLS features must be enabled globally.
- Before you configure BFD for LDP LSP, the OSPF protocol and MPLS static routes must be configured to enable the network to forward MPLS traffic.
- Before you configure BFD for LDP LSP, the BFD session parameters must be configured, including the interval for sending BFD control packets, the interval for receiving BFD control packets, and the detection multiplier of BFD control packets.

4. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure BFD for LDP LSP.

bfd bind ldp-lsp peer-ip peer-ipv4-address [**vrf** *vrf-name*] [**nexthop** *nexthop-ipv4-address*] [**interface** *interface-type interface-number*] **source-ip** source-ipv4-address [**local-discriminator** local-discriminator-value **remote-discriminator** remote-discriminator-value]

BFD for LDP LSP is disabled by default.

2.5 Configuring BFD for LDP Tunnel

1. Overview

You can configure BFD for LDP tunnel and create BFD sessions to detect the primary and secondary LSPs to quickly detect faults and trigger protection switching for LDP upper-layer applications.

2. Restrictions and Guidelines

- BFD for LDP tunnel is applicable only to LDP LSPs established by host routes.
- BFD for LSP and BFD for tunnel must be configured simultaneously to achieve the purpose of quick switchover.
- LDP tunnel must be configured on both the active device and the passive device.

3. Prerequisites

- The basic MPLS capability must be configured.
- MPLS LDP must be configured.
- Before you configure BFD for LDP tunnel, the OSPF protocol and MPLS static routes must be configured to enable the network to forward MPLS traffic.

4. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure BFD for LDP tunnel.

bfd bind ldp-tunnel peer-ip *peer-ipv4-address* [**vrf** *vrf-name*] **source-ip** *source-ipv4-address* [**local-discriminator** *local-discriminator-value* **remote-discriminator** *remote-discriminator-value*]

BFD for LDP tunnel is disabled by default.

2.6 Configuring BFD for BGP LSP

1. Overview

After you configure BFD to detect the connectivity of BGP LSPs and associate BGP LSPs with BFD, private network routes do not select the LSP as the forwarding path when the BGP LSP becomes Down.

2. Restrictions and Guidelines

- BFD for BGP LSP is applicable only to BGP LSPs established by host routes.
- Only one BFD session can be bound to an LSP.

- BFD can only be bound to the ingress node of a BGP LSP.
- If discriminators are configured in manual configuration mode, the local discriminator and the remote discriminator configured on the ingress LSR must match those configured on the egress LSR.
- When static BFD is used for BGP LSP detection, one static BFD session has the same effect as multiple BFD sessions. You are advised to configure one static BFD session.

3. Prerequisites

- Before you configure BFD for BGP LSP, the MPLS features must be enabled globally.
- Before you configure BFD for BGP LSP, an IGP protocol and static routes must be configured to enable the network to forward MPLS traffic.
- Before you configure BFD for BGP LSP, the BFD session parameters must be configured, including the interval for sending BFD control packets, the interval for receiving BFD control packets, and the detection multiplier of BFD control packets.

4. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure BFD for BGP LSP.

bfd bind bgp-lsp peer-ip bgp-lsppeer-ipv4-address [**vrf** *vrf-name*] **source-ip** source-ipv4-address [**local-discriminator** local-discriminator-value **remote-discriminator** remote-discriminator-value]

BFD for BGP LSP is disabled by default.

2.7 Configuring BFD for BGP Tunnel

1. Overview

You can configure BFD for BGP tunnel to implement quick fault detection for E2E BGP tunnels. This mechanism creates a BFD session that is bound to both the primary and the secondary BGP LSPs, so BFD can quickly perceive and trigger VPN fast reroute (FRR) protection switching when the primary and secondary BGP LSPs fail.

2. Restrictions and Guidelines

- BFD for BGP LSP is applicable only to BGP LSPs established by host routes.
- You can run this command only on the ingress node of a BGP tunnel.
- BFD for BGP tunnel is applicable only to BGP tunnels established by host routes. You can configure only one static BFD session for a tunnel.
- BFD for LSP and BFD for tunnel must be configured simultaneously to achieve the purpose of quick switchover.
- BGP for tunnel must be configured bidirectionally on the devices on both ends of a tunnel, and the protected primary link must have the same path in both directions.

3. Prerequisites

- Before you configure BFD for BGP tunnel, the MPLS features must be enabled globally.

4. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure BFD for BGP tunnel.

bfd bind bgp-tunnel peer-ip *peer-ipv4-address* [**vrf** *vrf-name*] **source-ip** *source-ipv4-address* [**local-discriminator** *local-discriminator-value* **remote-discriminator** *remote-discriminator-value*]

BFD for BGP tunnel is disabled by default.

2.8 Configuring BFD for LSP

1. Overview

Enable BFD for LSP. The BFD session does not restrict the peer LSP type detected by BFD, but only performs matching based on source and destination IP addresses.

2. Restrictions and Guidelines

- If manual configuration is performed on the Ingress LSR, the Egress LSR must also use manual configuration.
- The local and remote discriminators manually configured on the Ingress LSR must be consistent with those on the Egress LSR.
- If the source IP address is not specified, and the IP address of the outbound interface is changed after the BFD session is configured, the source IP address in the BFD packet is not updated.
- If the source IP address is specified, and the source IP address is changed after the BFD session is configured, the source IP address in the BFD packet is not updated. After the BFD session is set up, the discriminators cannot be changed.

3. Prerequisites

- The MPLS function must be enabled globally.
- The OSPF protocol and MPLS routes must be configured for forward MPLS traffic on the network.
- The BFD session parameters must be set on the interface, including the interval for sending BFD control packets, interval for receiving BFD control packets, and multiple of BFD detection times.
- BFD needs to be configured for LDP-LSP, BGP-LSP, or static LSP on the peer.

4. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure BFD for LSP. The BFD session does not restrict the peer LSP type detected by BFD, but only performs matching based on source and destination IP addresses.

bfd bind backward-lsp-with-ip peer-ip peer-ipv4-address [**vrf** vrf-name] **interface** interface-type interface-number **source-ip** *source-ipv4-address* **local-discriminator** local-discriminator-value **remote-discriminator** remote-discriminator-value

By default, BFD for LSP is not configured.

2.9 Monitoring

Run the **show** command to check the configuration.

Run the **debug** command to output debugging information.

Caution

Debugging occupies system resources, so disable it immediately if not required.

Table 1-1 MPLS BFD Monitoring

Command	Purpose
show bfd neighbors	Displays the BFD session status.
show mpls sbfd neighbor [{ **sr-be-lsp** | **sr-be-tunnel** } [**peer-ip** *peer-ipv4-address*] [**source-ip** *source-ipv4-address*]] [**detail**]	Displays neighbor status information of registered SBFD sessions of different types.
debug mpls bfd	Enables debugging for MPLS BFD information.

2.10 Configuration Examples

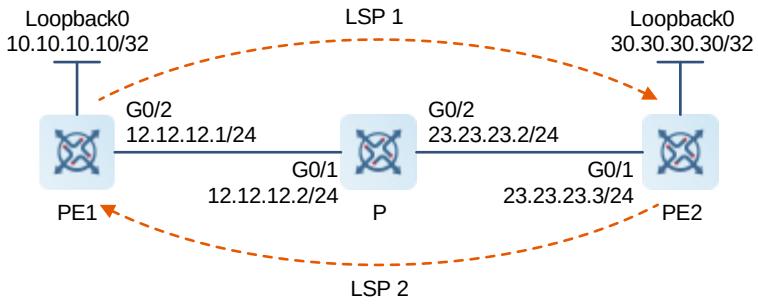
2.10.1 Configuring BFD for LDP LSP

1. Requirements

Configure BFD for LDP LSP.

2. Topology

Figure 1-1 Configuring BFD for LDP LSP



3. Notes

- Configure interface IP addresses and OSPF on each node.
- On each node, enable the global MPLS forwarding capability, enable each interface to forward labeled MPLS packets, and enable LDP on each interface.
- Configure LDP to allow the network to forward MPLS traffic.
- On PE1, configure BFD to detect LDP LSP 1.
- On PE2, configure BFD to detect LDP LSP 2 (reverse LSP).

4. Procedure

(1) Configure interface IP addresses and OSPF to implement interoperability between the nodes.

Configure interface IP addresses and OSPF on PE1. The configuration is similar on all the devices, and the configuration on PE1 is used as an example.

```
PE1> enable
PE1# configure terminal
PE1(config)# interface gigabitethernet 0/2
PE1(config-if-Gigabitethernet 0/2)# ip address 12.12.12.1 255.255.255.0
PE1(config-if-Gigabitethernet 0/2)# exit
PE1(config)# interface loopback 0
PE1(config-Loopback 0)# ip address 10.10.10.10 255.255.255.255
PE1(config-Loopback 0)# exit
PE1(config)# router ospf 1
PE1(config-router)# router-id 10.10.10.10
PE1(config-router)# network 10.10.10.10 0.0.0.0 area 0
PE1(config-router)# network 12.12.12.0 0.0.0.255 area 0
PE1(config-router)# exit
```

(2) Configure the MPLS forwarding capability.

Configure the MPLS forwarding capability on PE1. The configuration is similar on all the devices, and the configuration on PE1 is used as an example.

```
PE1(config)# mpls enable
PE1(config)# interface gigabitethernet 0/2
PE1(config-if-Gigabitethernet 0/2)# mpls ldp enable
```

```
PE1(config-if-Gigabitethernet 0/2)# label-switching
PE1(config-if-Gigabitethernet 0/2)# exit
```

(3) Configure LDP.

Configure LDP on PE1. The configuration is similar on all the devices, and the configuration on PE1 is used as an example.

```
PE1(config)# mpls router ldp
PE1(config-mpls-router)# ldp router-id interface Loopback 0
PE1(config-mpls-router)# exit
```

(4) Configure BFD for LDP LSP.

On PE1, configure BFD to detect LDP LSP 1.

```
PE1(config)# mpls bfd interval 50 min-rx 50 multiplier 3
PE1(config)# bfd bind ldp-lsp peer-ip 30.30.30.30 source-ip 10.10.10.10
local-discriminator 1 remote-discriminator 2
```

On PE2, configure BFD to detect LDP LSP 2.

```
PE2(config)# mpls bfd interval 50 min-rx 50 multiplier 3
PE2(config)# bfd bind ldp-lsp peer-ip 10.10.10.10 source-ip 30.30.30.30
local-discriminator 2 remote-discriminator 1
```

5. Verification

On PE1, check whether the status of the created BFD session is Up.

```
PE1# show bfd neighbors details
OurAddr              NeighAddr          LD/RD   State  Interface
Description
10.10.10.10      30.30.30.30    1/2     Up    -              Bfd for LSP
Session Name:
Session state is Up and not using echo function.
Local Diag: 0             Demand mode: 0        Poll bit: 0
Local MinTxInt(ms): 50     MinRxInt(ms): 50       Multiplier: 3
Actual TxInt(ms): 1000     DetectInt(ms): 3000
Destination Port: 3784     TTL: 255
Up Dampening(sec): 5       Client State: Up
Slot Id: 1               Parm Consult Finish: Yes
FRR: -
Rx Interface: Gi0/2
Registered protocols: LDP-LSP
Uptime: 0:00:49
```

On PE2, check whether the status of the created BFD session is Up.

```
PE2# show bfd neighbors details
OurAddr              NeighAddr          LD/RD   State  Interface
Description
30.30.30.30      10.10.10.10    2/1     Up    -              Bfd for LSP
Session Name:
Session state is Up and not using echo function.
Local Diag: 0             Demand mode: 0        Poll bit: 0
```

```
Local MinTxInt(ms): 50     MinRxInt(ms): 50       Multiplier: 3
Actual TxInt(ms): 1000     DetectInt(ms): 3000
Destination Port: 3784     TTL: 255
Up Dampening(sec): 5       Client State: Up
Slot Id: 1               Parm Consult Finish: Yes
FRR: -
Rx Interface: Gi0/1
Registered protocols: LDP-LSP
Uptime: 0:00:49
```

6. Configuration Files

- PE1 configuration file

```
hostname PE1
!
mpls enable
!
interface GigabitEthernet 0/2
 ip address 12.12.12.1 255.255.255.0
 label-switching
 mpls ldp enable
!
interface Loopback 0
 ip address 10.10.10.10 255.255.255.255
!
router ospf 1
 router-id 10.10.10.10
 network 10.10.10.10 0.0.0.0 area 0
 network 12.12.12.0 0.0.0.255 area 0
!
mpls router ldp
 ldp router-id interface Loopback 0
!
mpls bfd interval 50 min-rx 50 multiplier 3
bfd bind ldp-lsp peer-ip 30.30.30.30 source-ip 10.10.10.10 local-discriminator 1
remote-discriminator 2
!
```

- P configuration file

```
hostname P
!
mpls enable
!
interface GigabitEthernet 0/1
 ip address 12.12.12.2 255.255.255.0
 label-switching
 mpls ldp enable
```

```
!
interface GigabitEthernet 0/2
 ip address 23.23.23.2 255.255.255.0
 label-switching
 mpls ldp enable
!
interface Loopback 0
 ip address 20.20.20.20 255.255.255.255
!
router ospf 1
 router-id 20.20.20.20
 network 12.12.12.0 0.0.0.255 area 0
 network 20.20.20.20 0.0.0.0 area 0
 network 23.23.23.0 0.0.0.255 area 0
!
mpls router ldp
 ldp router-id interface Loopback 0
!
```

- PE2 configuration file

```
hostname PE2
!
mpls enable
!
interface GigabitEthernet 0/1
 ip address 23.23.23.1 255.255.255.0
 label-switching
 mpls ldp enable
!
interface Loopback 0
 ip address 30.30.30.30 255.255.255.255
!
router ospf 1
 router-id 30.30.30.30
 network 23.23.23.0 0.0.0.255 area 0
 network 30.30.30.30 0.0.0.0 area 0
!
mpls router ldp
 ldp router-id interface Loopback 0
!
mpls bfd interval 50 min-rx 50 multiplier 3
bfd bind ldp-lsp peer-ip 10.10.10.10 source-ip 30.30.30.30 local-discriminator 2
remote-discriminator 1
!
```

7. Common Errors

- BFD session parameters are not configured in the global configuration mode, or the configured intervals are

too short.

- No LSP is created.
- The **mpls enable** command is not enabled globally.
- MPLS forwarding is not enabled on an interface (by running the **label-switching** command).
- The source address and destination address on two ends of a BFD session do not match.
- The discriminators configured (in manual configuration mode) on two ends of a BFD session do not match.
- The FEC of the detected LSP is not a host route.

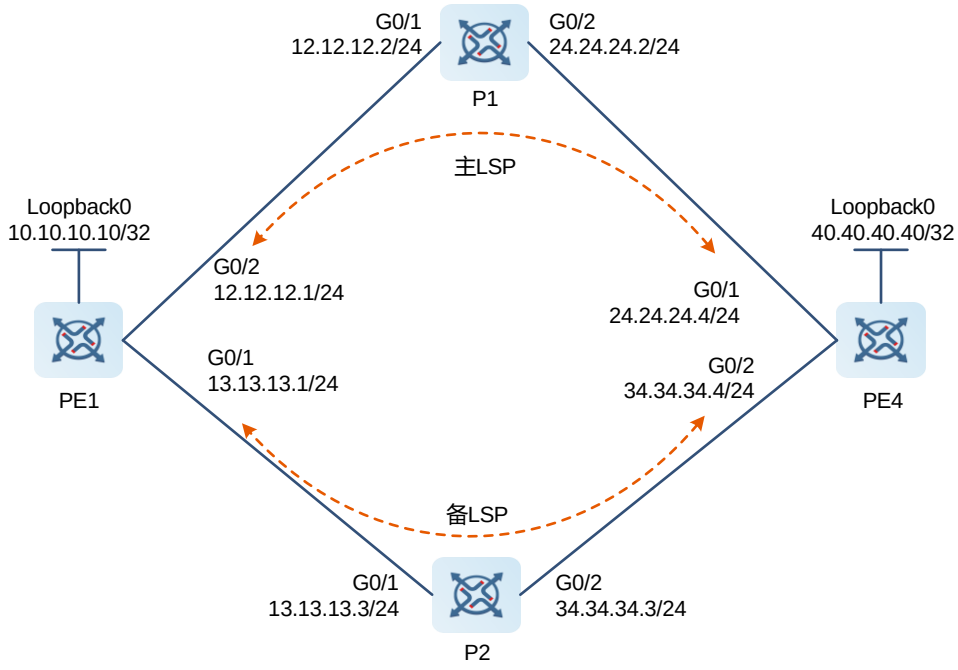
2.10.2 Configuring BFD for LDP FRR

1. Requirements

Configure BFD for LDP FRR.

2. Topology

Figure 1-1 Configuring BFD for LDP LSP



3. Notes

- Configure interface IP addresses and OSPF to implement interoperability between the nodes.
- On each node, enable the global MPLS forwarding capability, enable each interface to forward labeled MPLS packets, and enable LDP on each interface.
- Configure LDP FRR to set up bidirectional primary and secondary LSPs between PE1 and PE4.
- On PE1, configure a static BFD to detect the LDP LSP from PE1 to PE4.
- On PE4, configure a static BFD to detect the LDP LSP from PE4 to PE1.

4. Procedure

(1) Configure interface IP addresses and OSPF to implement interoperability between the nodes.

Configure interface IP addresses and OSPF on PE1. The configuration is similar on all the devices, and the configuration on PE1 is used as an example.

```
PE1> enable
PE1# configure terminal
PE1(config)# interface gigabitethernet 0/2
PE1(config-if-Gigabitethernet 0/2)# ip address 12.12.12.1 255.255.255.0
PE1(config-if-Gigabitethernet 0/2)# exit
PE1(config)# interface loopback 0
PE1(config-Loopback 0)# ip address 10.10.10.10 255.255.255.255
PE1(config-Loopback 0)# exit
PE1(config)# router ospf 1
PE1(config-router)# router-id 10.10.10.10
PE1(config-router)# network 10.10.10.10 0.0.0.0 area 0
PE1(config-router)# network 12.12.12.0 0.0.0.255 area 0
PE1(config-router)# exit
```

(2) Configure the MPLS forwarding capability.

Configure the MPLS forwarding capability on PE1. The configuration is similar on all the devices, and the configuration on PE1 is used as an example.

```
PE1(config)# mpls enable
PE1(config)# interface gigabitethernet 0/2
PE1(config-if-Gigabitethernet 0/2)# mpls ldp enable
PE1(config-if-Gigabitethernet 0/2)# label-switching
PE1(config-if-Gigabitethernet 0/2)# exit
```

(3) Configure LDP.

Configure LDP on PE1. The configuration is similar on all the devices, and the configuration on PE1 is used as an example.

```
PE1(config)# mpls router ldp
PE1(config-mpls-router)# ldp router-id interface Loopback 0
PE1(config-mpls-router)# exit
```

(4) Configure IGP and enable IP FRR.

Configure IGP and enable IP FRR. The configuration is similar on PE1 and PE4, and the configuration on PE1 is used as an example.

```
PE1(config)# router ospf 1
PE1(config-router)# fast-reroute lfa
PE1(config-router)# exit
```

(5) Configure LDP and enable auto FRR.

Configure LDP and enable auto FRR. The configuration is similar on PE1 and PE4, and the configuration on PE1 is used as an example.

```
PE1(config)# mpls router ldp
PE1(config-mpls-router)# auto-frr for all
```

```
PE1(config-router)# exit
```

(6) Configure BFD for LDP LSP.

On PE1, configure BFD to detect an LDP LSP to PE4.

```
PE1(config)# mpls bfd interval 50 min-rx 50 multiplier 3
PE1(config)# bfd bind ldp-lsp peer-ip 40.40.40.40 source-ip 10.10.10.10
local-discriminator 1 remote-discriminator 2
```

On PE4, configure BFD to detect an LDP LSP to PE1.

```
PE4(config)# mpls bfd interval 50 min-rx 50 multiplier 3
PE4(config)# bfd bind ldp-lsp peer-ip 10.10.10.10 source-ip 40.40.40.40
local-discriminator 2 remote-discriminator 1
```

5. Verification

On PE1, check whether the status of the created BFD session is Up.

```
PE1# show bfd neighbors details
OurAddr              NeighAddr           LD/RD   State  Interface
Description
10.10.10.10      40.40.40.40     1/2     Up     -              Bfd for LSP
Session Name:
Session state is Up and not using echo function.
Local Diag: 0             Demand mode: 0         Poll bit: 0
Local MinTxInt(ms): 50     MinRxInt(ms): 50       Multiplier: 3
Actual TxInt(ms): 1000     DetectInt(ms): 3000
Destination Port: 3784     TTL: 255
Up Dampening(sec): 5       Client State: Up
Slot Id: 1               Parm Consult Finish: Yes
FRR: Yes
Rx Interface: Gi0/2
Registered protocols: LDP-LSP
Uptime: 0:00:49
```

On PE4, check whether the status of the created BFD session is Up.

```
PE4# show bfd neighbors details
OurAddr         NeighAddr      LD/RD     State  Interface        Description
40.40.40.40     10.10.10.10    2/1       Up     -              Bfd for LSP
Session Name:
Session state is Up and not using echo function.
Local Diag: 0             Demand mode: 0         Poll bit: 0
Local MinTxInt(ms): 1000   MinRxInt(ms): 1000     Multiplier: 3
Actual TxInt(ms): 1000     DetectInt(ms): 3000
Destination Port: 3784     TTL: 255
Up Dampening(sec): 5       Client State: Up
Slot Id: 1               Parm Consult Finish: Yes
FRR: Yes
Rx Interface: Gi0/1
Registered protocols: LDP-LSP
Uptime: 0:00:52
```

6. Configuration Files

- PE1 configuration file

```
hostname PE1
!
mpls enable
!
interface GigabitEthernet 0/1
 ip address 13.13.13.1 255.255.255.0
 label-switching
 mpls ldp enable
!
interface GigabitEthernet 0/2
 ip address 12.12.12.1 255.255.255.0
 label-switching
 mpls ldp enable
!
interface Loopback 0
 ip address 10.10.10.10 255.255.255.255
!
router ospf 1
 fast-reroute lfa
 router-id 10.10.10.10
 network 10.10.10.10 0.0.0.0 area 0
 network 12.12.12.0 0.0.0.0 area 0
 network 13.13.13.0 0.0.0.255 area 0
!
mpls router ldp
 ldp router-id interface Loopback 0
 auto-frr for all
!
mpls bfd interval 50 min-rx 50 multiplier 3
bfd bind ldp-lsp peer-ip 40.40.40.40 source-ip 10.10.10.10 local-discriminator 1
remote-discriminator 2
!
```

- P1 configuration file

```
hostname P1
!
mpls enable
!
interface GigabitEthernet 0/1
 ip address 12.12.12.2 255.255.255.0
 label-switching
 mpls ldp enable
!
interface GigabitEthernet 0/2
```

```
 ip address 24.24.24.2 255.255.255.0
 label-switching
 mpls ldp enable
!
interface Loopback 0
 ip address 20.20.20.20 255.255.255.255
!
router ospf 1
 router-id 20.20.20.20
 network 12.12.12.0 0.0.0.255 area 0
 network 20.20.20.20 0.0.0.0 area 0
 network 24.24.24.0 0.0.0.255 area 0
!
mpls router ldp
 ldp router-id interface Loopback 0
!
```

- P2 configuration file

```
hostname P2
!
mpls enable
!
interface GigabitEthernet 0/1
 ip address 13.13.13.3 255.255.255.0
 label-switching
 mpls ldp enable
!
interface GigabitEthernet 0/2
 ip address 34.34.34.2 255.255.255.0
 label-switching
 mpls ldp enable
!
interface Loopback 0
 ip address 30.30.30.30 255.255.255.255
!
router ospf 1
 router-id 30.30.30.30
 network 13.13.13.0 0.0.0.255 area 0
 network 30.30.30.30 0.0.0.0 area 0
 network 34.34.34.0 0.0.0.255 area 0
!
mpls router ldp
 ldp router-id interface Loopback 0
!
```

- PE4 configuration file

```
hostname PE4
```

```
!
mpls enable
!
interface GigabitEthernet 0/1
 ip address 24.24.24.4 255.255.255.0
 label-switching
 mpls ldp enable
!
interface GigabitEthernet 0/2
 ip address 34.34.34.4 255.255.255.0
 label-switching
 mpls ldp enable
!

interface Loopback 0
 ip address 40.40.40.40 255.255.255.255
!
router ospf 1
 fast-reroute lfa
 router-id 40.40.40.40
 network 24.24.24.0 0.0.0.255 area 0
 network 34.34.34.0 0.0.0.255 area 0
 network 40.40.40.40 0.0.0.0 area 0
!
mpls router ldp
 ldp router-id interface Loopback 0
 auto-frr for all
!
mpls bfd interval 50 min-rx 50 multiplier 3
bfd bind ldp-lsp peer-ip 10.10.10.10 source-ip 40.40.40.40 local-discriminator 2
remote-discriminator 1
!
```

7. Common Errors

- BFD session parameters are not configured in the global configuration mode, or the configured intervals are too short.
- No LSP is created.
- The **mpls enable** command is not enabled globally.
- MPLS forwarding is not enabled on an interface (by running the **label-switching** command).
- The source address and destination address on two ends of a BFD session do not match.
- The discriminators configured (in manual configuration mode) on two ends of a BFD session do not match.
- The FEC of the detected LSP is not a host route.

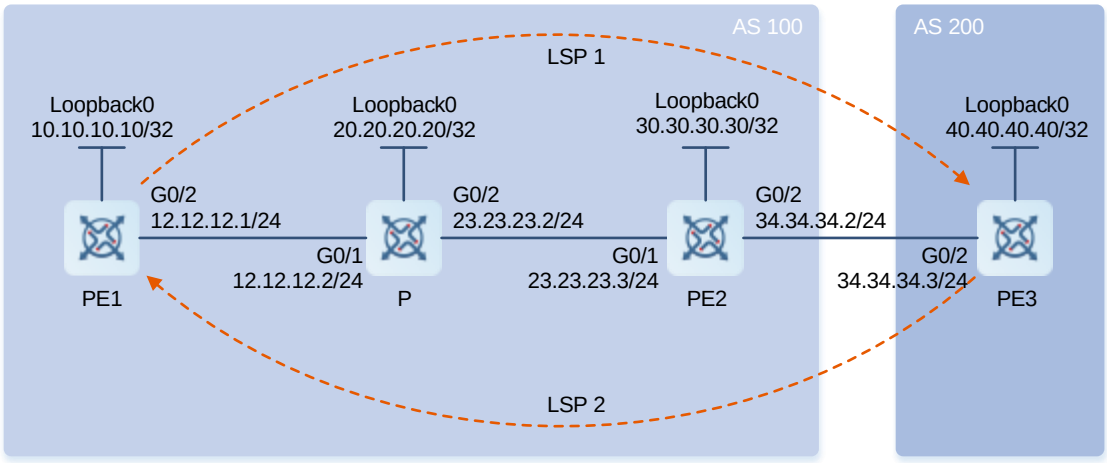
2.10.3 Configuring BFD for BGP LSP

1. Requirements

Configure BFD for BGP LSP.

2. Topology

Figure 1-1 Configuring BFD for BGP LSP



3. Notes

- Configure interface IP addresses and loopback interfaces for each node.
- Configure OSPF and LDP between PE1 and PE2.
- On each node, enable the global MPLS forwarding capability and enable each interface to forward labeled MPLS packets.
- Configure IBGP between PE1 and PE2 and distribute labels to BGP routes. Configure EBGP between PE2 and PE3 and distribute labels to BGP routes.
- On PE1, configure BFD to detect LDP LSP 1. On PE3, configure BFD to detect LDP LSP 2 (reverse LSP).

4. Procedure

(1) Configure interface IP addresses.

Configure interface IP addresses on PE1. The configuration is similar on all the devices, and the configuration on PE1 is used as an example.

```
PE1> enable
PE1# configure terminal
PE1(config)# interface gigabitethernet 0/2
PE1(config-if-Gigabitethernet 0/2)# ip address 12.12.12.1 255.255.255.0
PE1(config-if-Gigabitethernet 0/2)# exit
PE1(config)# interface loopback 0
PE1(config-Loopback 0)# ip address 10.10.10.10 255.255.255.255
PE1(config-Loopback 0)# exit
```

(2) Configure OSPF and LDP between PE1 and PE2.

Configure OSPF and LDP on PE1. The configuration is similar on PE1, P, and PE2, and the configuration on PE1 is used as an example.

```
PE1(config)# router ospf 1
PE1(config-router)# router-id 10.10.10.10
PE1(config-router)# network 10.10.10.10 0.0.0.0 area 0
PE1(config-router)# network 12.12.12.0 0.0.0.255 area 0
PE1(config-router)# exit
PE1(config)# mpls router ldp
PE1(config-mpls-router)# ldp router-id interface Loopback 0
PE1(config-mpls-router)# exit
```

(3) Configure the MPLS forwarding capability.

Configure the MPLS forwarding capability on PE1. The configuration is similar on all the devices, and the configuration on PE1 is used as an example.

```
PE1(config)# mpls enable
PE1(config)# interface gigabitethernet 0/2
PE1(config-if-Gigabitethernet 0/2)# mpls ldp enable
PE1(config-if-Gigabitethernet 0/2)# label-switching
PE1(config-if-Gigabitethernet 0/2)# exit
```

(4) Configure IBGP between PE1 and PE2 and distribute labels to BGP routes.

Configure IBGP on PE1.

```
PE1(config)# router bgp 100
PE1(config-router)# neighbor 30.30.30.30 remote-as 100
PE1(config-router)# neighbor 30.30.30.30 update-source loopback 0
PE1(config-router)# neighbor 30.30.30.30 send-label
PE1(config-router)# network 10.10.10.10 mask 255.255.255.255
PE1(config-router)# exit
```

Configure IBGP on PE2.

```
PE2(config)# router bgp 100
PE2(config-router)# neighbor 10.10.10.10 remote-as 100
PE2(config-router)# neighbor 10.10.10.10 update-source loopback 0
PE2(config-router)# neighbor 10.10.10.10 send-label
```

(5) Configure EBGP between PE2 and PE3 and distribute labels to BGP routes.

Configure EBGP on PE2.

```
PE2(config)# router bgp 100
PE2(config-router)# neighbor 34.34.34.3 remote-as 200
PE2(config-router)# neighbor 34.34.34.3 send-label
```

Configure EBGP on PE3.

```
PE3(config)# router bgp 200
PE3(config-router)# neighbor 34.34.34.2 remote-as 100
PE3(config-router)# neighbor 34.34.34.2 send-label
PE3(config-router)# network 40.40.40.40 mask 255.255.255.255
```

(6) On PE2, set the label distribution mode of the global VRF instance to per-route.

```
PE2(config)# vrf global-vrf
PE2(config-global-vrf)# address-family ipv4
PE2(config-vrf-af)# alloc-label per-route
```

(7) Configure BFD for BGP LSP.

On PE1, configure BFD to detect LDP LSP 1.

```
PE1(config)# mpls bgp bfd interval 50 min-rx 50 multiplier 3
PE1(config)# bfd bind bgp-lsp peer-ip 40.40.40.40 source-ip 10.10.10.10
local-discriminator 1 remote-discriminator 2
```

On PE3, configure BFD to detect LDP LSP 2.

```
PE3(config)# mpls bgp bfd interval 50 min-rx 50 multiplier 3
PE3(config)# bfd bind bgp-lsp peer-ip 10.10.10.10 source-ip 40.40.40.40
local-discriminator 2 remote-discriminator 1
```

5. Verification

On PE1, check whether the status of the created BFD session is Up.

```
PE1# show bfd neighbors details
OurAddr              NeighAddr          LD/RD   State  Interface
Description
10.10.10.10        40.40.40.40      1/2     Up    -              Bfd for LSP
Session Name:
Session state is Up and not using echo function.
Local Diag: 0             Demand mode: 0         Poll bit: 0
Local MinTxInt(ms): 50     MinRxInt(ms): 50       Multiplier: 3
Actual TxInt(ms): 1000     DetectInt(ms): 3000
Destination Port: 3784     TTL: 255
Up Dampening(sec): 5       Client State: Up
Slot Id: 1               Parm Consult Finish: Yes
FRR: -
Rx Interface: Gi0/2
Registered protocols: BGP-LSP
Uptime: 0:00:05
```

On PE3, check whether the status of the created BFD session is Up.

```
PE3# show bfd neighbors details
OurAddr              NeighAddr          LD/RD   State  Interface
Description
40.40.40.40        10.10.10.10      2/1     Up    -              Bfd for LSP
Session Name:
Session state is Up and not using echo function.
Local Diag: 0             Demand mode: 0         Poll bit: 0
Local MinTxInt(ms): 50     MinRxInt(ms): 50       Multiplier: 3
Actual TxInt(ms): 1000     DetectInt(ms): 3000
Destination Port: 3784     TTL: 255
Up Dampening(sec): 5       Client State: Up
Slot Id: 1               Parm Consult Finish: Yes
FRR: -
```

```
Rx Interface: Gi0/1
Registered protocols: BGP-LSP
Uptime: 0:01:02
```

6. Configuration Files

- PE1 configuration file

```
hostname PE1
!
mpls enable
!
interface GigabitEthernet 0/2
 ip address 12.12.12.1 255.255.255.0
 label-switching
 mpls ldp enable
!
interface Loopback 0
 ip address 10.10.10.10 255.255.255.255
!
router bgp 100
 neighbor 30.30.30.30 remote-as 100
 neighbor 30.30.30.30 update-source Loopback 0
 address-family ipv4
  network 10.10.10.10 mask 255.255.255.255
  neighbor 30.30.30.30 send-label
  exit-address-family
!
router ospf 1
 router-id 10.10.10.10
 network 10.10.10.10 0.0.0.0 area 0
 network 12.12.12.0 0.0.0.255 area 0
!
mpls router ldp
 ldp router-id interface Loopback 0
!
mpls bgp bfd interval 50 min-rx 50 multiplier 3
bfd bind bgp-lsp peer-ip 40.40.40.40 source-ip 10.10.10.10 local-discriminator 1
remote-discriminator 2
!
```

- P configuration file

```
hostname P
!
mpls enable
!
interface GigabitEthernet 0/1
 ip address 12.12.12.2 255.255.255.0
```

```
 label-switching
 mpls ldp enable
!
interface GigabitEthernet 0/2
 ip address 23.23.23.2 255.255.255.0
 label-switching
 mpls ldp enable
!
interface Loopback 0
 ip address 20.20.20.20 255.255.255.255
!
router ospf 1
 router-id 20.20.20.20
 network 12.12.12.0 0.0.0.255 area 0
 network 20.20.20.20 0.0.0.0 area 0
 network 23.23.23.0 0.0.0.255 area 0
!
mpls router ldp
 ldp router-id interface Loopback 0
!
```

- PE2 configuration file

```
hostname PE2
!
vrf global-vrf
 address-family ipv4
  alloc-label per-route
  exit-address-family
 address-family ipv6
  exit-address-family
!
mpls enable
!
interface GigabitEthernet 0/1
 ip address 23.23.23.3 255.255.255.0
 label-switching
 mpls ldp enable
!
interface GigabitEthernet 0/2
 ip address 34.34.34.2 255.255.255.0
 label-switching
!
interface Loopback 0
 ip address 30.30.30.30 255.255.255.255
!
router bgp 100
 neighbor 10.10.10.10 remote-as 100
```

```
 neighbor 10.10.10.10 update-source Loopback 0
 neighbor 34.34.34.3 remote-as 200
 address-family ipv4
  neighbor 10.10.10.10 send-label
  neighbor 34.34.34.3 send-label
  exit-address-family
!
router ospf 1
 router-id 30.30.30.30
 network 30.30.30.30 0.0.0.0 area 0
 network 23.23.23.0 0.0.0.255 area 0
 network 34.34.34.0 0.0.0.255 area 0
!
mpls router ldp
 ldp router-id interface Loopback 0
!
```

- PE3 configuration file

```
hostname PE3
!
mpls enable
!
interface GigabitEthernet 0/2
 ip address 34.34.34.3 255.255.255.0
 label-switching
!
interface Loopback 0
 ip address 40.40.40.40 255.255.255.255
!
router bgp 200
 neighbor 34.34.34.2 remote-as 100
 address-family ipv4
  network 40.40.40.40 mask 255.255.255.255
  neighbor 34.34.34.2 send-label
  exit-address-family
!
mpls router ldp
 ldp router-id interface Loopback 0
!
mpls bgp bfd interval 50 min-rx 50 multiplier 3
bfd bind bgp-lsp peer-ip 10.10.10.10 source-ip 40.40.40.40 local-discriminator 2
remote-discriminator 1
!
```

7. Common Errors

- BFD session parameters are not configured in the global configuration mode, or the configured intervals are too short.

- No LSP is created.
- The **mpls enable** command is not enabled globally.
- MPLS forwarding is not enabled on an interface (by running the **label-switching** command).
- The source address and destination address on two ends of a BFD session do not match.
- The discriminators configured (in manual configuration mode) on two ends of a BFD session do not match.
- The FEC of the detected LSP is not a host route.

3 L3VPN FRR

3.1 Overview

3.1.1 L3VPN FRR

L3VPN FRR can protect the P node and the PE on the tunnel endpoint. If the link between the PEs, the P node, or the PE on the tunnel endpoint fails, a quick link fault detection mechanism (such as BFD) can be used to quickly detect the fault of the primary PE or the primary LSP to quickly switch the outbound interface of VPN routes from the primary PE to the secondary PE. When BGP re-converges and generates new VPN routes, the secondary PE is used as the outbound interface for VPN routes to implement uninterrupted forwarding. After new VPN routes are generated, these new VPN routes are used for forwarding.

LDP FRR can only protect the P node or a link against a fault. However, VPN FRR can also provide effective protection for VPN services when the PE node fails. As VPN FRR changes the egress PE for VPN routes, the VPN label is also changed during the switchover process.

3.1.2 Basic Concept

1. Methods for Backup Next-Hop Selection

To back up the optimal next hop, you need to configure BGP optimal routes and apply a route map policy to the optimal routes to obtain the backup next hop based on the set rule in the route map policy by checking whether it matches a specific rule of the route map. The methods for backup next-hop selection (configured in the set rule of the route map policy) can be manual or auto.

- Manual mode

  Use the next hop specified in the set rule of the route map for backup. During the selection process, the device queries the corresponding route based on the next-hop address (It must be different from the primary next-hop address. Otherwise, the protection function does not take effect.) specified here. If the address does not exist, the device does not deliver a backup entry.

- Auto mode

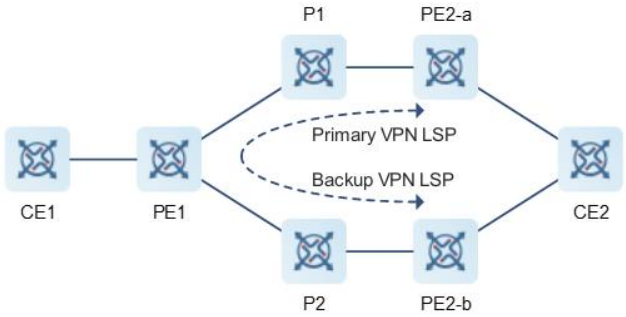
  The system selects another optimal route (secondary route as compared with the original optimal route) except the current optimal route and the primary next hop as the backup entry by referring to the algorithm for selecting a BGP optimal route. As the selected backup may use the same remote PE as the primary route, the protection function does not take effect if the remote PE fails. As a result, the route with the same remote PE as the primary route does not participate in automatic backup selection by the system.

3.1.3 Working Principles

As shown in the figure, after VPN FRR is enabled, the PE loads both the optimal VPN route with PE2-a as the next hop and the backup VPN route with PE2-b as the next hop to the forwarding plane when the network connection is normal. In this situation, the forwarding path between CE1 and CE2 is as follows: CE1 > PE1 > P1 > PE2-a > CE2. If PE1 finds that the primary PE or the MPLS link between PE1 and PE2-a fails, PE1 quickly

switches the traffic to the backup path to guarantee quick convergence of E2E services. In this situation, the forwarding path is CE1 > PE1 > P2 > PE2-b > CE2.

Figure 3-1 L3VPN FRR



3.2 Configuration Task Summary

The L3VPN FRR configuration includes the following tasks:

Configuring L3VPN FRR

3.3 Configuring L3VPN FRR

1. Overview

You can configure L3VPN FRR.

2. Restrictions and Guidelines

- To ensure successful backup by VPN FRR, it is recommended that the VRF instances of the remote primary and secondary PEs and the VRF instance of the local PE be configured with exactly the same or different RDs. Otherwise, you need to run the BGP command **import path selection all**.
- To ensure that Internet FRR has a higher priority than VPN FRR, the fault detection time of VPN FRR should be greater than the sum of the fault detection time of Internet FRR and the switching time of Internet FRR.
- To ensure that VPN FRR and LDP FRR are implemented based on their priorities, LDP FRR must be deployed on a P device. When LDP FRR is also deployed on a PE device, VPN FRR is implemented prior to LDP FRR.
- You are not allowed to enable or disable VPN FRR during GR.
- VPN FRR can only protect unidirectional traffic. To protect bidirectional traffic, VPN FRR must be used in combination with other high reliability technologies, such as Virtual Router Redundancy Protocol (VRRP) and IP FRR.
- In essence, VPN FRR is a protection technology applied to the egress PE nodes. To apply VPN FRR protection to the P nodes and Internet links, the two Internet LSPs from the ingress PE to the primary egress PE and secondary egress PE must be separated in topology and configuration. (That is, the two LSPs do not have the same transit node or link.)
- To prevent packet loss during the VPN FRR switchback process caused by black hole routes, you are

advised to configure the ordered control mode in Internet LDP.

3. Prerequisites

- Before you configure L3VPN FRR, the MPLS features must be enabled globally.
- Before you configure L3VPN FRR, the OSPF protocol must be configured to enable the network to forward MPLS traffic.
- Before you configure L3VPN FRR, the L3VPN network must be configured based on the application scenario.

4. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Create a routing policy and enter the route map configuration mode.

route-map *route-map-name* [{ **permit** | **deny** } *sequence*]

(4) Match a target network route whose redistributed next-hop IP address is permitted by an ACL rule or a prefix list rule.

match ip next-hop { { *acl-number* | *acl-name* } &<1-6> | **prefix-list** *prefix-list-name*&<1-6> }

The next-hop IP address is not matched by an ACL or prefix list by default.

(5) Configure the backup next hop for VPN FRR.

set vpn fast-reroute backup-next-hop { *address* | **auto** }

(6) Exit the route map configuration mode.

exit

(7) Enable VPN FRR by using one of the following methods:

- Run the following commands in sequence to enable VPN FRR in the single-protocol VRF instance:
  ip vrf *vrf-name*

  vpn fast-reroute { **auto | route-map** *route-map-name* }

  exit
- Run the following commands in sequence to enable VPN FRR in the multiprotocol VRF instance:
  vrf definition *vrf-name*

  address-family { ipv4 | ipv6 }

  vpn fast-reroute { **auto | route-map** *route-map-name* }

  exit-address-family

  exit

3.4 Monitoring

Run the **show** command to check the configuration.

Run the **debug** command to output debugging information.

Caution

Debugging occupies system resources, so disable it immediately if not required.

Table 3-1 L3VPN FRR Monitoring

Command	Purpose
show mpls forwarding-table [frr **] [** detail **]**	Displays MPLS primary and secondary forwarding entries.
debug mpls frr	Enables debugging for MPLS FRR-related route processing.

3.5 Configuration Examples

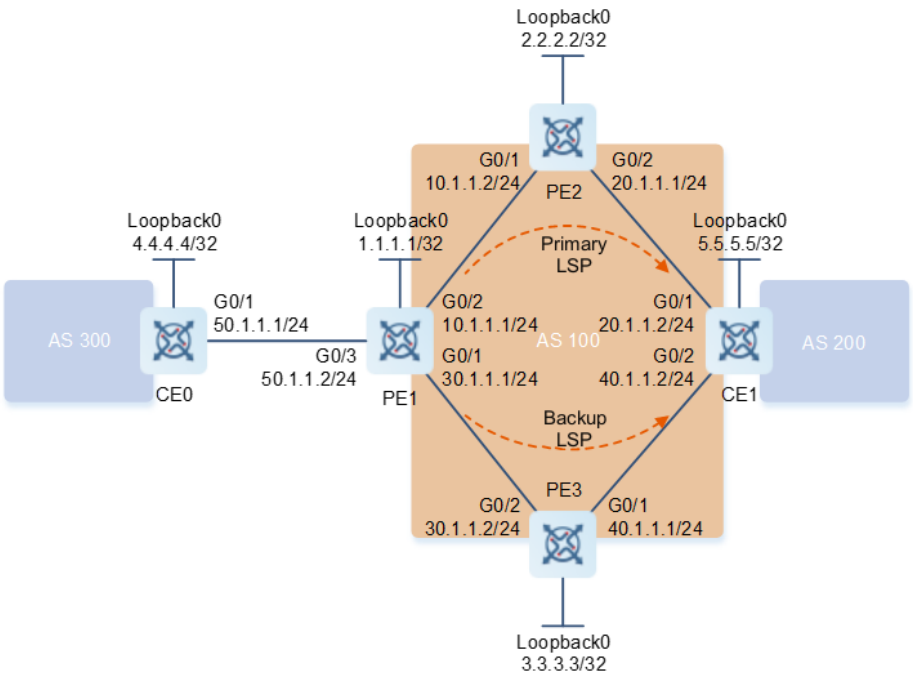
3.5.1 Configuring L3VPN FRR

1. Requirements

Configure L3VPN FRR.

2. Topology

Figure 3-2 Configuring L3VPN FRR



3. Notes

- Configure interface IP addresses and loopback addresses on each node.

- Configure OSPF on the MPLS backbone network (PE1, PE2, and PE3) to implement backbone network interoperability.
- On the MPLS backbone network, configure the MPLS basic capability, enable MPLS LDP, and establish LDP LSPs.
- Configure a VPN instance on each PE device (PE1, PE2, and PE3) and connect CE0 to PE1 and connect CE1 to PE2 and PE3.
- Create MP-IBGP peers between each two PEs.
- Configure OSPF to exchange VPN routes between CEs and PEs.
- On PE1, configure a VPN FRR routing policy, configure the backup next hop, and enable VPN FRR.
- On PE1 and PE2, configure BFD to detect BGP sessions.

4. Procedure

(1) Configure interface IP addresses (omitted).

(2) Configure OSPF on PE1, PE2, and PE3 to implement backbone network interoperability.

Configure OSPF on PE1. The configuration is similar on PE1, PE2, and PE3, and the configuration on PE1 is used as an example.

```
PE1> enable
PE1# configure terminal
PE1(config)# router ospf 1
PE1(config-router)# router-id 1.1.1.1
PE1(config-router)# network 1.1.1.1 0.0.0.0 area 0
PE1(config-router)# network 10.1.1.0 0.0.0.255 area 0
PE1(config-router)# network 30.1.1.0 0.0.0.255 area 0
PE1(config-router)# exit
```

(3) Configure the MPLS forwarding capability.

Configure the MPLS forwarding capability on PE1. The configuration is similar on PE1, PE2, and PE3, and the configuration on PE1 is used as an example.

```
PE1(config)# mpls enable
PE1(config)# interface GigabitEthernet 0/1
PE1(config-if-Gigabitethernet 0/1)# mpls ldp enable
PE1(config-if-Gigabitethernet 0/1)# label-switching
PE1(config-if-Gigabitethernet 0/1)# exit
PE1(config)# interface GigabitEthernet 0/2
PE1(config-if-Gigabitethernet 0/2)# mpls ldp enable
PE1(config-if-Gigabitethernet 0/2)# label-switching
PE1(config-if-Gigabitethernet 0/2)# exit
```

(4) Configure VPN instances on PE1, PE2, and PE3.

Configure a VPN instance on PE1. The configuration is similar on PE1, PE2, and PE3, and the configuration on PE1 is used as an example.

```
PE1(config)# ip vrf vpna
PE1(config-vrf)# rd 100:1
PE1(config-vrf)# route-target both 100:1
```

```
PE1(config-vrf)# exit
```

(5) Create MP-IBGP peers between each two PEs.

Create an MP-IBGP peer on PE1. The configuration is similar on PE1, PE2, and PE3, and the configuration on PE1 is used as an example.

```
PE1(config)# router bgp 100
PE1(config-router)# neighbor 2.2.2.2 remote-as 100
PE1(config-router)# neighbor 2.2.2.2 update-source loopback 0
PE1(config-router)# neighbor 3.3.3.3 remote-as 100
PE1(config-router)# neighbor 3.3.3.3 update-source loopback 0
PE1(config-router)# address-family vpnv4
PE1(config-router-af)# neighbor 2.2.2.2 activate
PE1(config-router-af)# neighbor 3.3.3.3 activate
PE1(config-router-af)# exit
PE1(config-router)# exit
```

(8) Configure OSPF to exchange VPN routes between CEs and PEs.

On PE1, configure OSPF to exchange VPN routes. The configuration is similar on PE1, PE2, and PE3, and the configuration on PE1 is used as an example.

```
PE1(config)# router ospf 10 vrf vpna
PE1(config-router)# network 0.0.0.0 255.255.255.255 area 0
PE1(config-router)# redistribute bgp subnets
PE1(config-router)# exit
PE1(config)# router bgp 100
PE1(config-router)# address-family ipv4 vrf vpna
PE1(config-router-af)# redistribute ospf 10
PE1(config-router-af)# exit
PE1(config-router)# exit
```

(6) On PE1, configure a VPN FRR routing policy, configure the backup next hop, and enable VPN FRR.

```
PE1(config)# ip access-list standard stdacl1
PE1(config-std-nacl)# permit host 2.2.2.2
PE1(config-std-nacl)# exit
PE1(config)# route-map routemap1 permit 10
PE1(config-route-map)# match ip next-hop stdacl1
PE1(config-route-map)# set vpn fast-reroute backup-next-hop auto
PE1(config-route-map)# exit
PE1(config)# ip vrf vpna
PE1(config-vrf)# vpn fast-reroute route-map routemap1
PE1(config-vrf)# exit
```

(7) On PE1 and PE2, configure BFD to detect BGP sessions.

On PE1, configure BFD to detect BGP sessions. The configuration is similar on PE1 and PE2, and the configuration on PE1 is used as an example.

```
PE1(config)# interface GigabitEthernet 0/2
PE1(config-if-Gigabitethernet 0/1)# bfd interval 200 min_rx 200 multiplier 3
PE1(config-if-Gigabitethernet 0/1)# no bfd echo
```

```
PE1(config-if-Gigabitethernet 0/1)# exit
PE1(config)# router bgp 100
PE1(config-router)# bgp log-neighbor-changes
PE1(config-router)# neighbor 2.2.2.2 fall-over bfd
PE1(config-router)# exit
```

5. Verification

On PE1, check the primary and secondary forwarding entries.

```
PE1# show mpls forwarding-table frr
Label Operation Code:
PHbel OperatioPPbel OperatiSWbel OperatioSPbel Operation Code: and push new label
DPnd push new lPCnd push ne and continue lookup by IP or Label
PInd push ne and continue lookup by IPPNnd push ne and continue lookup by PMnd push
ne and continue lookup by IP PVnd push ne and continue lookup by IP or LabelIPnd push
ne and cont snd pushStatus codes: m  continue lookb – backup entry, * - active.
    Local   Outgoing OP FEC                    Outgoing       Nexthop
    label   label                             interface
m*   --     imp-null PH 2.2.2.2/32              Gi0/2          10.1.1.2
m*   --     imp-null PH 3.3.3.3/32              Gi0/1          30.1.1.2
m*   --     1536    PH 5.5.5.5/32(V)            Gi0/2          10.1.1.2
b    --     1536    PH 5.5.5.5/32(V)            Gi0/1          30.1.1.2
m*   --     1536    PH 20.1.1.0/24(V)           Gi0/2          10.1.1.2
b    --     1536    PH 20.1.1.0/24(V)           Gi0/1          30.1.1.2
m*   --     1536    PH 40.1.1.0/24(V)           Gi0/1          30.1.1.2
m*   1024   imp-null PP 2.2.2.2/32               Gi0/2          10.1.1.2
m*   1025   imp-null PP 3.3.3.3/32               Gi0/1          30.1.1.2
m*   1536   --      PI VRF(aa)                   --            0.0.0.0
```

6. Configuration Files

- CE0 configuration file

```
hostname CE0
!
interface GigabitEthernet 0/1
 ip address 50.1.1.1 255.255.255.0
!
interface Loopback 0
 ip address 4.4.4.4 255.255.255.255
!
router ospf 1
 router-id 4.4.4.4
 network 0.0.0.0 255.255.255.255 area 0
!
```

- PE1 configuration file

```
hostname PE1
!
```

```
mpls enable
!
route-map routemap1 permit 10
 match ip next-hop stdacl1
 set vpn fast-reroute backup-next-hop auto
!
ip vrf vpna
 rd 100:1
 route-target both 100:1
 vpn fast-reroute route-map routemap1
!
ip access-list standard stdacl1
 10 permit host 2.2.2.2
!
interface GigabitEthernet 0/1
 ip address 30.1.1.1 255.255.255.0
 label-switching
 mpls ldp enable
!
interface GigabitEthernet 0/2
 ip address 10.1.1.1 255.255.255.0
 label-switching
 mpls ldp enable
 bfd interval 200 min_rx 200 multiplier 3
 no bfd echo
!
interface GigabitEthernet 0/3
 ip vrf forwarding vpna
 ip address 50.1.1.2 255.255.255.0
!
interface Loopback 0
 ip address 1.1.1.1 255.255.255.255
!
router bgp 100
 bgp log-neighbor-changes
 neighbor 2.2.2.2 remote-as 100
 neighbor 2.2.2.2 update-source Loopback 0
 neighbor 2.2.2.2 fall-over bfd
 neighbor 3.3.3.3 remote-as 100
 neighbor 3.3.3.3 update-source Loopback 0
 !
 address-family ipv4
  neighbor 2.2.2.2 activate
  neighbor 3.3.3.3 activate
 exit-address-family
 !
```

```
 address-family vpnv4 unicast
  neighbor 2.2.2.2 activate
  neighbor 3.3.3.3 activate
 exit-address-family
 !
 address-family ipv4 vrf vpna
  redistribute ospf 10
 exit-address-family
!
router ospf 1
 router-id 1.1.1.1
 network 1.1.1.1 0.0.0.0 area 0
 network 10.1.1.0 0.0.0.255 area 0
 network 30.1.1.0 0.0.0.255 area 0
!
router ospf 10 vrf vpna
 redistribute bgp subnets
 network 0.0.0.0 255.255.255.255 area 0
!
mpls router ldp
 ldp router-id interface Loopback 0
!
```

- PE2 configuration file

```
hostname PE2
!
mpls enable
!
ip vrf vpna
 rd 100:2
 route-target both 100:1
!
interface GigabitEthernet 0/1
 ip address 10.1.1.2 255.255.255.0
 label-switching
 mpls ldp enable
 bfd interval 200 min_rx 200 multiplier 3
!
interface GigabitEthernet 0/2
 ip vrf forwarding vpna
 ip address 20.1.1.1 255.255.255.0
!
interface Loopback 0
 ip address 2.2.2.2 255.255.255.255
!
router bgp 100
 bgp log-neighbor-changes
```

```
 neighbor 1.1.1.1 remote-as 100
 neighbor 1.1.1.1 update-source Loopback 0
 neighbor 1.1.1.1 fall-over bfd
 !
 address-family ipv4
  neighbor 1.1.1.1 activate
 exit-address-family
 !
 address-family vpnv4 unicast
  neighbor 1.1.1.1 activate
 exit-address-family
 !
 address-family ipv4 vrf vpna
  redistribute ospf 10 match internal
 exit-address-family
!
router ospf 1
 router-id 2.2.2.2
 network 2.2.2.2 0.0.0.0 area 0
 network 10.1.1.0 0.0.0.255 area 0
!
router ospf 10 vrf vpna
 redistribute bgp subnets
 network 0.0.0.0 255.255.255.255 area 0
!
mpls router ldp
 ldp router-id interface Loopback 0
!
```

- PE3 configuration file

```
hostname PE3
!
mpls enable
!
ip vrf vpna
 rd 100:3
 route-target both 100:1
!
interface GigabitEthernet 0/1
 ip vrf forwarding vpna
 ip address 40.1.1.1 255.255.255.0
!
interface GigabitEthernet 0/2
 ip address 30.1.1.2 255.255.255.0
 label-switching
 mpls ldp enable
!
```

```
interface Loopback 0
 ip address 3.3.3.3 255.255.255.255
!
router bgp 100
 neighbor 1.1.1.1 remote-as 100
 neighbor 1.1.1.1 update-source Loopback 0
 !
 address-family ipv4
  neighbor 1.1.1.1 activate
 exit-address-family
 !
 address-family vpnv4 unicast
  neighbor 1.1.1.1 activate
 exit-address-family
 !
 address-family ipv4 vrf vpna
  redistribute ospf 10
 exit-address-family
!
router ospf 1
 router-id 3.3.3.3
 network 3.3.3.3 0.0.0.0 area 0
 network 30.1.1.0 0.0.0.255 area 0
!
router ospf 10 vrf vpna
 redistribute bgp subnets
 network 0.0.0.0 255.255.255.255 area 0
!
mpls router ldp
 ldp router-id interface Loopback 0
!
```

- CE1 configuration file

```
hostname CE1
!
interface GigabitEthernet 0/1
 ip address 20.1.1.2 255.255.255.0
!
interface GigabitEthernet 0/2
 ip address 40.1.1.2 255.255.255.0
!
interface Loopback 0
 ip address 5.5.5.5 255.255.255.255
!
router ospf 1
 router-id 5.5.5.5
 network 0.0.0.0 255.255.255.255 area 0
```

```
!
```

7. Common Errors

- The **mpls enable** command is not enabled globally.
- MPLS forwarding is not enabled on an interface (by running the **label-switching** command).
- IP FRR is not configured.

4 Configuring MPLS ECMP

4.1 Introduction

4.1.1 Overview

MPLS forwarding entries are established based on IP routes. If a forwarding equivalence class (FEC) has multiple equivalent next hops, the MPLS signaling protocol can establish multiple equivalent next hops for the FEC and traffic of the FEC can be forwarded on these equivalent routes. MPLS equal-cost multi-path routing (ECMP) maps MPLS forwarding entries of one FEC to multiple Next Hop Label Forwarding Entries (NHLFEs). Each next hop maps to an NHLFE. Packets of the FEC can be forwarded on these equivalent links, ensuring load balancing.

Load balancing has the following benefits:

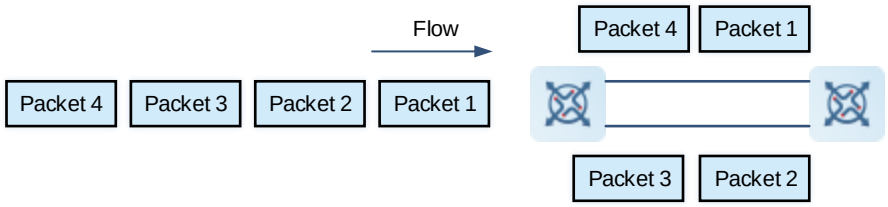
- Increase the bandwidth of the existing MPLS network without updating device hardware.
- Enhance MPLS network link protection. Distribute traffic to multiple links. When one link among load balancing links is faulty, traffic can be forwarded through other links, improving link reliability.
- Distribute MPLS traffic with the same destination address to multiple LSPs to make full use of network resources.

4.1.2 Principles

1. Per Flow Scheduling

In per flow scheduling mode, a router checks some fields in received packets and maps packets of the same type to the same next-hop link. As shown in Figure 4-1, there are four packets to be forwarded to the same destination network. Packets 1 and 4 are of the same type, and packets 2 and 3 are of the same type. By classifying the fields for identifying the packet type, the router forwards packets 1 and 4 to link 1 and packets 2 and 3 to link 2.

Figure 4-1 Per Flow Scheduling



In per flow scheduling mode, hash is performed using the following methods:

- Common MPLS traffic

  If the MPLS label stack is followed by an IPv4 header, the destination and source IP addresses are used for hash to select a next hop to forward traffic. If the MPLS label stack is not followed by an IPv4 header, the inner label is used for hash to select a next hop to forward traffic. If no inner label is available, hash is not performed and the first valid next hop is used to forward traffic.

- L3VPN traffic

  The destination and source IP addresses are used for hash.

2. MPLS ECMP Implementation

A routing protocol, such as OSPF or BGP, may find several different routes to the same destination network. If the routing protocol has the highest priority among all active routing protocols, these different routes are valid routes. When forwarding packets to the destination network, the routing protocol can use different paths, ensuring load balancing.

On an MPLS network, the outgoing labels of packets sent in load balancing mode can be the same or different. If the load balancing links are between the same pair of devices, and these links work on the label space of each device, the outgoing labels are the same. If multiple next-hop LSRs exist, the load balancing links may have different outgoing labels because each next-hop LSR is assigned with a label.

4.1.3 Protocols and Standards

- RFC 2992: Analysis of an Equal-Cost Multi-Path Algorithm
- RFC 4928: Avoiding Equal Cost Multipath Treatment in MPLS Networks

4.2 Configuration Task Summary

MPLS ECMP configuration includes the following tasks:

- Configuring MPLS ECMP

4.3 Configuring MPLS ECMP

1. Overview

MPLS ECMP applies to the following scenarios:

- Multiple equivalent public network LSPs exist.
- Multiple equivalent access PEs exist between L3VPN sites. Traffic of each PE can be forwarded through multiple equivalent LSPs.

2. Restrictions and Guidelines

- Due to the capacity limit of the forwarding information base (FIB), equivalent LSPs are established only for host routes when many equivalent routes exist. This saves the FIB space.
- MPLS forwarding must be enabled on each outbound interface of equivalent LSPs.

3. Prerequisites

- MPLS is enabled globally before LDP ECMP is configured.
- MPLS is enabled globally, BGP neighbors are configured, and ECMP is enabled before L3VPN ECMP is configured.

4. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enable LDP and enter the LDP configuration mode.

mpls router ldp [*vrf-name*]

(4) Enable BGP and enter the BGP routing configuration mode.

router bgp *as-number*

(5) Enter the corresponding BGP address family configuration mode and perform either of the following configurations.

(IPv4 network)

address-family ipv4 vrf *vrf-name*

(IPv6 network)

address-family ipv6 vrf *vrf-name*

(6) Configure the number of BGP equal-cost paths.

maximum-paths { **ebgp** | **ibgp** } *maximum-path-number*

Here, *maximum-path-number* indicates the number of equivalent next hops, ranging from 1 to device capacity. The default value is **1**. A larger value means more equivalent next hops allowed.

4.4 Monitoring

Run the **show** command to check the configuration.

Run the **debug** command to output debugging information.

⚠ Caution

Debugging occupies system resources, so disable it immediately if not required.

Table 4-1 Monitoring

Command	Purpose
show mpls forwarding-table	Displays generated equal-cost paths.
debug mpls fec A.B.C.D/32	Debugs MPLS-related route processing.

4.5 Configuration Examples

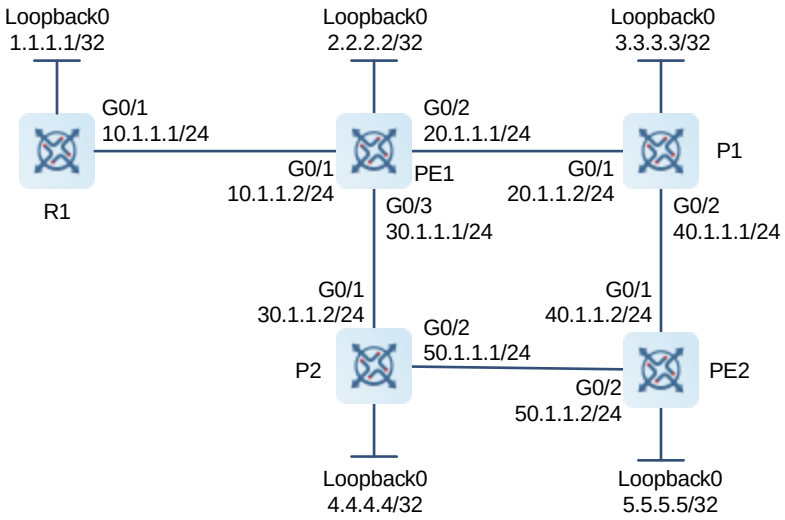
4.5.1 Configuring LDP ECMP

1. Requirements

Configure the LDP ECMP forwarding scenario.

2. Topology

Figure 4-2 Configuring LDP ECMP



3. Notes

- Configure interface IP addresses and OSPF on devices.
- Enable MPLS forwarding globally and on interfaces and configure LDP on devices.
- Generate equivalent LSPs for all routes on PE1 and PE2.

4. Procedure

(1) Configure interface IP addresses and OSPF on devices to ensure communication between them.

Configure R1.

```
R1> enable
R1# configure terminal
R1(config)# interface gigabitethernet 0/1
R1(config-if-Gigabitethernet 0/1)# ip address 10.1.1.1 255.255.255.0
R1(config-if-Gigabitethernet 0/1)# exit
R1(config)# interface loopback 0
R1(config-Loopback 0)# ip address 1.1.1.1 255.255.255.255
R1(config-Loopback 0)# exit
R1(config)# router ospf 1
R1(config-router)# network 10.1.1.0 0.0.0.255 area 0
R1(config-router)# network 1.1.1.1 0.0.0.0 area 0
R1(config-router)# exit
```

Configure PE1.

```
PE1> enable
PE1# configure terminal
PE1(config)# interface gigabitethernet 0/1
PE1(config-if-Gigabitethernet 0/1)# ip address 10.1.1.2 255.255.255.0
```

```
PE1(config-if-Gigabitethernet 0/1)# exit
PE1(config)# interface gigabitethernet 0/2
PE1(config-if-Gigabitethernet 0/2)# ip address 20.1.1.1 255.255.255.0
PE1(config-if-Gigabitethernet 0/2)# exit
PE1(config)# interface gigabitethernet 0/3
PE1(config-if-Gigabitethernet 0/3)# ip address 30.1.1.1 255.255.255.0
PE1(config-if-Gigabitethernet 0/3)# exit
PE1(config)#interface loopback 0
PE1(config-Loopback 0)#ip address 2.2.2.2 255.255.255.255
PE1(config-Loopback 0)#exit
PE1(config)# router ospf 1
PE1(config-router)# network 10.1.1.0 0.0.0.255 area 0
PE1(config-router)# network 20.1.1.0 0.0.0.255 area 0
PE1(config-router)# network 30.1.1.0 0.0.0.255 area 0
PE1(config-router)# network 2.2.2.2 0.0.0.0 area 0
PE1(config-router)# exit
```

Configure P1.

```
P1> enable
P1# configure terminal
P1(config)# interface gigabitethernet 0/1
P1(config-if-Gigabitethernet 0/1)# ip address 20.1.1.2 255.255.255.0
P1(config-if-Gigabitethernet 0/1)# exit
P1(config)# interface gigabitethernet 0/2
P1(config-if-Gigabitethernet 0/2)# ip address 40.1.1.1 255.255.255.0
P1(config-if-Gigabitethernet 0/2)# exit
P1(config)# interface loopback 0
P1(config-Loopback 0)# ip address 3.3.3.3 255.255.255.255
P1(config-Loopback 0)# exit
P1(config)# router ospf 1
P1(config-router)# network 20.1.1.0 0.0.0.255 area 0
P1(config-router)# network 40.1.1.0 0.0.0.255 area 0
P1(config-router)# network 3.3.3.3 0.0.0.0 area 0
P1(config-router)# exit
```

Configure P2.

```
P2> enable
P2# configure terminal
P2(config)# interface gigabitethernet 0/1
P2(config-if-Gigabitethernet 0/1)# ip address 30.1.1.2 255.255.255.0
P2(config-if-Gigabitethernet 0/1)# exit
P2(config)# interface gigabitethernet 0/2
P2(config-if-Gigabitethernet 0/2)# ip address 50.1.1.1 255.255.255.0
P2(config-if-Gigabitethernet 0/2)# exit
P2(config)# interface loopback 0
P2(config-Loopback 0)# ip address 4.4.4.4 255.255.255.255
P2(config-Loopback 0)# exit
```

```
P2(config)# router ospf 1
P2(config-router)# network 30.1.1.0 0.0.0.255 area 0
P2(config-router)# network 50.1.1.0 0.0.0.255 area 0
P2(config-router)# network 4.4.4.4 0.0.0.0 area 0
P2(config-router)# exit
```

Configure PE2.

```
PE2> enable
PE2# configure terminal
PE2(config)# interface gigabitethernet 0/1
PE2(config-if-Gigabitethernet 0/1)# ip address 40.1.1.2 255.255.255.0
PE2(config-if-Gigabitethernet 0/1)# exit
PE2(config)# interface gigabitethernet 0/2
PE2(config-if-Gigabitethernet 0/2)# ip address 50.1.1.2 255.255.255.0
PE2(config-if-Gigabitethernet 0/2)# exit
PE2(config)# interface loopback 0
PE2(config-Loopback 0)# ip address 5.5.5.5 255.255.255.255
PE2(config-Loopback 0)# exit
PE2(config)# router ospf 1
PE2(config-router)# network 40.1.1.0 0.0.0.255 area 0
PE2(config-router)# network 50.1.1.0 0.0.0.255 area 0
PE2(config-router)# network 5.5.5.5 0.0.0.0 area 0
PE2(config-router)# exit
```

(2) Configure MPLS forwarding and LDP.

Configure PE1.

```
PE1(config)# mpls enable
PE1(config)# interface gigabitethernet 0/1
PE1(config-if-Gigabitethernet 0/1)# label-switching
PE1(config-if-Gigabitethernet 0/1)# mpls ldp enable
PE1(config-if-Gigabitethernet 0/1)# exit
PE1(config)# interface gigabitethernet 0/2
PE1(config-if-Gigabitethernet 0/2)# label-switching
PE1(config-if-Gigabitethernet 0/2)# mpls ldp enable
PE1(config-if-Gigabitethernet 0/2)# exit
PE1(config)# interface gigabitethernet 0/3
PE1(config-if-Gigabitethernet 0/3)# label-switching
PE1(config-if-Gigabitethernet 0/3)# mpls ldp enable
PE1(config-if-Gigabitethernet 0/3)# exit
PE1(config)# mpls router ldp
PE1(config-mpls-router)# ldp router-id interface loopback 0 force
PE1(config-mpls-router)# exit
```

Configure P1.

```
P1(config)# mpls enable
P1(config)# interface gigabitethernet 0/1
P1(config-if-Gigabitethernet 0/1)# label-switching
```

```
P1(config-if-Gigabitethernet 0/1)# mpls ldp enable
P1(config-if-Gigabitethernet 0/1)# exit
P1(config)# interface gigabitethernet 0/2
P1(config-if-Gigabitethernet 0/2)# label-switching
P1(config-if-Gigabitethernet 0/2)# mpls ldp enable
P1(config-if-Gigabitethernet 0/2)# exit
P1(config)# mpls router ldp
P1(config-mpls-router)# ldp router-id interface loopback 0 force
P1(config-mpls-router)# exit
```

Configure P2.

```
P2(config)# mpls enable
P2(config)# interface gigabitethernet 0/1
P2(config-if-Gigabitethernet 0/1)# label-switching
P2(config-if-Gigabitethernet 0/1)# mpls ldp enable
P2(config-if-Gigabitethernet 0/1)# exit
P2(config)# interface gigabitethernet 0/2
P2(config-if-Gigabitethernet 0/2)# label-switching
P2(config-if-Gigabitethernet 0/2)# mpls ldp enable
P2(config-if-Gigabitethernet 0/2)# exit
P2(config)# mpls router ldp
P2(config-mpls-router)# ldp router-id interface loopback 0 force
P2(config-mpls-router)# exit
```

Configure PE2.

```
PE2(config)# mpls enable
PE2(config)# interface gigabitethernet 0/1
PE2(config-if-Gigabitethernet 0/1)# label-switching
PE2(config-if-Gigabitethernet 0/1)# mpls ldp enable
PE2(config-if-Gigabitethernet 0/1)# exit
PE2(config)# interface gigabitethernet 0/2
PE2(config-if-Gigabitethernet 0/2)# label-switching
PE2(config-if-Gigabitethernet 0/2)# mpls ldp enable
PE2(config-if-Gigabitethernet 0/2)# exit
PE2(config)# mpls router ldp
PE2(config-mpls-router)# ldp router-id interface loopback 0 force
PE2(config-mpls-router)# exit
```

(3) Generate equivalent LSPs for all routes on PE1 and PE2. This feature is enabled by default.

5. Verification

Run the **show mpls forwarding-table** command on PE1 to display the established equivalent LSPs.

```
PE1# show mpls forwarding-table
Label Operation Code:
PH--PUSH label
PP--POP label
SW--SWAP label
SP-SWAP topmost label and push new label
```

```
DP-DROP packet
PC-POP label and continue lookup( IP or Label )
PI--POP label and do ip lookup forward
PN--POP label and forward to nexthop
PM--POP label and do MAC lookup forward
PV--POP label and output to VC attach interface
IP--IP lookup forward
Local  Outgoing  OP   FEC           Outgoing      Next Hop
label  label                       interface
--     1024    PH   5.5.5.5/32     Gi0/2         20.1.1.2
--     1024    PH   5.5.5.5/32     Gi0/3         30.1.1.2
...
```

6. Configuration Files

R1 configuration file

```
hostname R1
!
interface GigabitEthernet 0/1
 ip address 10.1.1.1 255.255.255.0
!
interface Loopback 0
 ip address 1.1.1.1 255.255.255.255
!
router ospf 1
 router-id 1.1.1.1
 network 1.1.1.1 0.0.0.0 area 0
 network 10.1.1.0 0.0.0.255 area 0
!
```

PE1 configuration file

```
hostname PE1
!
mpls enable ip
!
interface GigabitEthernet 0/1
 ip address 10.1.1.2 255.255.255.0
 label-switching
 mpls ldp enable
!
interface GigabitEthernet 0/2
 ip address 20.1.1.1 255.255.255.0
 label-switching
 mpls ldp enable
!
interface GigabitEthernet 0/3
 ip address 30.1.1.1 255.255.255.0
```

```
 label-switching
 mpls ldp enable
!
interface Loopback 0
 ip address 2.2.2.2 255.255.255.0
!
router ospf 1
 router-id 2.2.2.2
 network 2.2.2.0 0.0.0.255 area 0
 network 10.1.1.0 0.0.0.255 area 0
 network 20.1.1.0 0.0.0.255 area 0
 network 30.1.1.0 0.0.0.255 area 0
!
mpls router ldp
 ldp router-id interface Loopback 0
!
```

P1 configuration file

```
hostname P1
!
mpls enable ip
!
interface GigabitEthernet 0/1
 ip address 20.1.1.2 255.255.255.0
 label-switching
 mpls ldp enable
!
interface GigabitEthernet 0/2
 ip address 40.1.1.1 255.255.255.0
 label-switching
 mpls ldp enable
!
interface Loopback 0
 ip address 3.3.3.3 255.255.255.255
!
router ospf 1
 router-id 3.3.3.3
 network 3.3.3.3 0.0.0.0 area 0
 network 20.1.1.0 0.0.0.255 area 0
 network 40.1.1.0 0.0.0.255 area 0
!
mpls router ldp
 ldp router-id interface Loopback 0
!
```

PE2 configuration file

```
hostname PE2
```

```
!
mpls ldp enable
!
interface GigabitEthernet 0/1
 ip address 40.1.1.2 255.255.255.0
 label-switching
 mpls ldp enable
!
interface GigabitEthernet 0/2
 ip address 50.1.1.2 255.255.255.0
 label-switching
 mpls ldp enable
!
interface Loopback 0
 ip address 5.5.5.5 255.255.255.255
!
router ospf 1
 router-id 5.5.5.5
 network 5.5.5.5 0.0.0.0 area 0
 network 40.1.1.0 0.0.0.255 area 0
 network 50.1.1.0 0.0.0.255 area 0
!
mpls router ldp
 ldp router-id interface Loopback 0 force
!
```

P2 configuration file

```
hostname P2
!
mpls ldp enable
!
interface GigabitEthernet 0/1
 ip address 30.1.1.2 255.255.255.0
 label-switching
 mpls ldp enable
!
interface GigabitEthernet 0/2
 ip address 50.1.1.1 255.255.255.0
 label-switching
 mpls ldp enable
!
interface Loopback 0
 ip address 4.4.4.4 255.255.255.0
!
router ospf 1
 router-id 4.4.4.4
 network 4.4.4.4 0.0.0.0 area 0
```

```
 network 30.1.1.0 0.0.0.255 area 0
 network 50.1.1.0 0.0.0.255 area 0
!
mpls router ldp
 ldp router-id interface Loopback 0 force
!
```

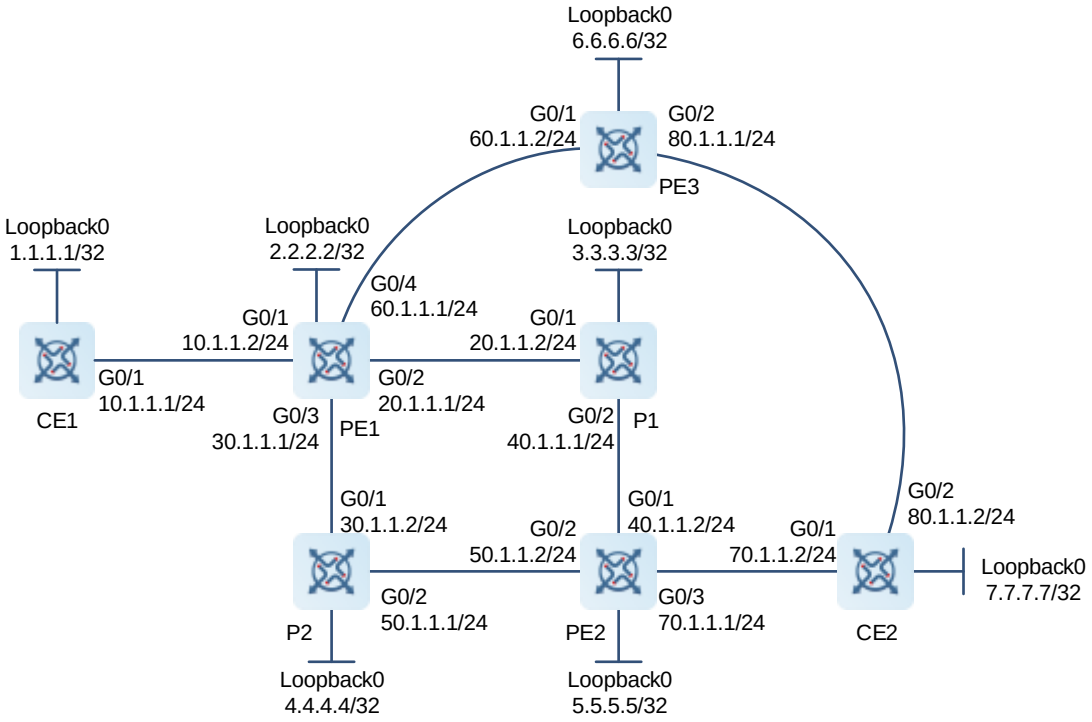
4.5.2 Configuring L3VPN ECMP

1. Requirements

Use L3VPN ECMP to ensure load balancing.

2. Topology

Figure 4-3 Configuring L3VPN ECMP



3. Notes

- Configure interface IP addresses and OSPF on MPLS backbone network nodes to ensure communication between them.
- Enable MPLS forwarding globally and on interfaces, configure LDP, and set up an LDP LSP.
- Configure VPN route instances on PE1 and PE2 and connect CE1 to PE1 and CE2 to PE2. Configure MP-IBGP neighbor relationship between PE1 and PE2 and between PE1 and PE3 to transmit VPN routing information.
- Generate equivalent LSPs for all routes on PE1 and PE2.
- Configure the number of equivalent paths that can be generated for the same FEC on PE1.

4. Procedure

(1) Configure interface IP addresses and OSPF on MPLS backbone network nodes to ensure communication between them.

Configure PE1.

```
PE1> enable
PE1# configure terminal
PE1(config)# interface gigabitethernet 0/2
PE1(config-if-Gigabitethernet 0/2)# ip address 20.1.1.1 255.255.255.0
PE1(config-if-Gigabitethernet 0/2)# exit
PE1(config)# interface gigabitethernet 0/3
PE1(config-if-Gigabitethernet 0/3)# ip address 30.1.1.1 255.255.255.0
PE1(config-if-Gigabitethernet 0/3)# exit
PE1(config)# interface gigabitethernet 0/4
PE1(config-if-Gigabitethernet 0/4)# ip address 60.1.1.1 255.255.255.0
PE1(config-if-Gigabitethernet 0/4)# exit
PE1(config)# interface loopback 0
PE1(config-Loopback 0)# ip address 2.2.2.2 255.255.255.255
PE1(config-Loopback 0)# exit
PE1(config)# router ospf 1
PE1(config-router)# network 20.1.1.0 0.0.0.255 area 0
PE1(config-router)# network 30.1.1.0 0.0.0.255 area 0
PE1(config-router)# network 60.1.1.0 0.0.0.255 area 0
PE1(config-router)# network 2.2.2.2 0.0.0.0 area 0
PE1(config-router)# exit
```

Configure P1.

```
P1> enable
P1# configure terminal
P1(config)# interface gigabitethernet 0/1
P1(config-if-Gigabitethernet 0/1)# ip address 20.1.1.2 255.255.255.0
P1(config-if-Gigabitethernet 0/1)# exit
P1(config)# interface gigabitethernet 0/2
P1(config-if-Gigabitethernet 0/2)# ip address 40.1.1.1 255.255.255.0
P1(config-if-Gigabitethernet 0/2)# exit
P1(config)# interface loopback 0
P1(config-Loopback 0)# ip address 3.3.3.3 255.255.255.255
P1(config-Loopback 0)# exit
P1(config)# router ospf 1
P1(config-router)# network 20.1.1.0 0.0.0.255 area 0
P1(config-router)# network 40.1.1.0 0.0.0.255 area 0
P1(config-router)# network 3.3.3.3 0.0.0.0 area 0
P1(config-router)# exit
```

Configure P2.

```
P2> enable
P2# configure terminal
```

```
P2(config)# interface gigabitethernet 0/1
P2(config-if-Gigabitethernet 0/1)# ip address 30.1.1.2 255.255.255.0
P2(config-if-Gigabitethernet 0/1)# exit
P2(config)# interface gigabitethernet 0/2
P2(config-if-Gigabitethernet 0/2)# ip address 50.1.1.1 255.255.255.0
P2(config-if-Gigabitethernet 0/2)# exit
P2(config)# interface loopback 0
P2(config-Loopback 0)# ip address 4.4.4.4 255.255.255.255
P2(config-Loopback 0)# exit
P2(config)# router ospf 1
P2(config-router)# network 30.1.1.0 0.0.0.255 area 0
P2(config-router)# network 50.1.1.0 0.0.0.255 area 0
P2(config-router)# network 4.4.4.4 0.0.0.0 area 0
P2(config-router)# exit
```

Configure PE2.

```
PE2> enable
PE2# configure terminal
PE2(config)# interface gigabitethernet 0/1
PE2(config-if-Gigabitethernet 0/1)# ip address 40.1.1.2 255.255.255.0
PE2(config-if-Gigabitethernet 0/1)# exit
PE2(config)# interface gigabitethernet 0/2
PE2(config-if-Gigabitethernet 0/2)# ip address 50.1.1.1 255.255.255.0
PE2(config-if-Gigabitethernet 0/2)# exit
PE2(config)# interface loopback 0
PE2(config-Loopback 0)# ip address 5.5.5.5 255.255.255.255
PE2(config-Loopback 0)# exit
PE2(config)# router ospf 1
PE2(config-router)# network 40.1.1.0 0.0.0.255 area 0
PE2(config-router)# network 50.1.1.0 0.0.0.255 area 0
PE2(config-router)# network 5.5.5.5 0.0.0.0 area 0
PE2(config-router)# exit
```

Configure PE3.

```
PE3> enable
PE3# configure terminal
PE3(config)# interface gigabitethernet 0/1
PE3(config-if-Gigabitethernet 0/1)# ip address 60.1.1.2 255.255.255.0
PE3(config-if-Gigabitethernet 0/1)# exit
PE3(config)# interface loopback 0
PE3(config-Loopback 0)# ip address 6.6.6.6 255.255.255.255
PE3(config-Loopback 0)# exit
PE3(config)# router ospf 1
PE3(config-router)# network 60.1.1.0 0.0.0.255 area 0
PE3(config-router)# network 6.6.6.6 0.0.0.0 area 0
PE3(config-router)# exit
```

CE2 configuration

```
CE2> enable
CE2# configure terminal
CE2(config)# interface gigabitethernet 0/1
CE2(config-if-Gigabitethernet 0/1)# ip address 70.1.1.2 255.255.255.0
CE2(config-if-Gigabitethernet 0/1)# exit
CE2(config)# interface gigabitethernet 0/2
CE2(config-if-Gigabitethernet 0/2)# ip address 80.1.1.2 255.255.255.0
CE2(config-if-Gigabitethernet 0/2)# exit
CE2(config)# interface loopback 0
CE2(config-Loopback 0)# ip address 7.7.7.7 255.255.255.255
CE2(config-Loopback 0)# exit
CE2(config)# router ospf 1
CE2(config-router)# network 70.1.1.0 0.0.0.255 area 0
CE2(config-router)# network 80.1.1.0 0.0.0.255 area 0
CE2(config-router)# network 7.7.7.7 0.0.0.0 area 0
CE2(config-router)# exit
```

(2) Configure MPLS forwarding and LDP.

Configure PE1.

```
PE1(config)# mpls enable
PE1(config)# interface gigabitethernet 0/2
PE1(config-if-Gigabitethernet 0/2)# label-switching
PE1(config-if-Gigabitethernet 0/2)# mpls ldp enable
PE1(config-if-Gigabitethernet 0/2)# exit
PE1(config)# interface gigabitethernet 0/3
PE1(config-if-Gigabitethernet 0/3)# label-switching
PE1(config-if-Gigabitethernet 0/3)# mpls ldp enable
PE1(config-if-Gigabitethernet 0/3)# exit
PE1(config)# interface gigabitethernet 0/4
PE1(config-if-Gigabitethernet 0/4)# label-switching
PE1(config-if-Gigabitethernet 0/4)# mpls ldp enable
PE1(config-if-Gigabitethernet 0/4)# exit
PE1(config)# mpls router ldp
PE1(config-mpls-router)# ldp router-id interface loopback 0 force
PE1(config-mpls-router)# exit
```

Configure P1.

```
P1(config)# mpls enable
P1(config)# interface gigabitethernet 0/1
P1(config-if-Gigabitethernet 0/1)# label-switching
P1(config-if-Gigabitethernet 0/1)# mpls ldp enable
P1(config-if-Gigabitethernet 0/1)# exit
P1(config)# interface gigabitethernet 0/2
P1(config-if-Gigabitethernet 0/2)# label-switching
P1(config-if-Gigabitethernet 0/2)# mpls ldp enable
P1(config-if-Gigabitethernet 0/2)# exit
P1(config)# mpls router ldp
```

```
P1(config-mpls-router)# ldp router-id interface loopback 0 force
P1(config-mpls-router)# exit
```

Configure P2.

```
P2(config)# mpls enable
P2(config)# interface gigabitethernet 0/1
P2(config-if-Gigabitethernet 0/1)# label-switching
P2(config-if-Gigabitethernet 0/1)# mpls ldp enable
P2(config-if-Gigabitethernet 0/1)# exit
P2(config)# interface gigabitethernet 0/2
P2(config-if-Gigabitethernet 0/2)# label-switching
P2(config-if-Gigabitethernet 0/2)# mpls ldp enable
P2(config-if-Gigabitethernet 0/2)# exit
P2(config)# mpls router ldp
P2(config-mpls-router)# ldp router-id interface loopback 0 force
P2(config-mpls-router)# exit
```

Configure PE2.

```
PE2(config)# mpls enable
PE2(config)# interface gigabitethernet 0/1
PE2(config-if-Gigabitethernet 0/1)# label-switching
PE2(config-if-Gigabitethernet 0/1)# mpls ldp enable
PE2(config-if-Gigabitethernet 0/1)# exit
PE2(config)# interface gigabitethernet 0/2
PE2(config-if-Gigabitethernet 0/2)# label-switching
PE2(config-if-Gigabitethernet 0/2)# mpls ldp enable
PE2(config-if-Gigabitethernet 0/2)# exit
PE2(config)# mpls router ldp
PE2(config-mpls-router)# ldp router-id interface loopback 0 force
PE2(config-mpls-router)# exit
```

Configure PE3.

```
PE3(config)# mpls enable
PE3(config)# interface gigabitethernet 0/1
PE3(config-if-Gigabitethernet 0/1)# label-switching
PE3(config-if-Gigabitethernet 0/1)# mpls ldp enable
PE3(config-if-Gigabitethernet 0/1)# exit
PE3(config)# mpls router ldp
PE3(config-mpls-router)# ldp router-id interface loopback 0 force
PE3(config-mpls-router)# exit
```

(3) Configure VPN route instances on PE1 and PE2 and connect CE1 to PE1 and CE2 to PE2.

Configure PE1.

```
PE1> enable
PE1# configure terminal
PE1(config)# ip vrf vrf1
PE1(config-vrf)# rd 100:2
PE1(config-vrf)# route-target both 100:1
```

```
PE1(config-vrf)# exit
PE1(config)# interface gigabitethernet 0/1
PE1(config-if-Gigabitethernet 0/1)# ip vrf forwarding vrf1
PE1(config-if-Gigabitethernet 0/1)# ip address 10.1.1.2 255.255.255.0
PE1(config-if-Gigabitethernet 0/1)# exit
PE1(config)# router ospf 10 vrf vrf1
PE1(config-router)# redistribute bgp subnets
PE1(config-router)# network 0.0.0.0 255.255.255.255 area 0
PE1(config-router)# exit
```

Configure PE2.

```
PE2(config)# ip vrf vrf1
PE2(config-vrf)# rd 100:5
PE2(config-vrf)# route-target both 100:1
PE2(config-vrf)# exit
PE2(config)# interface gigabitethernet 0/3
PE2(config-if-Gigabitethernet 0/3)# ip vrf forwarding vrf1
PE2(config-if-Gigabitethernet 0/3)# ip address 70.1.1.1 255.255.255.0
PE2(config-if-Gigabitethernet 0/3)# exit
PE2(config)# router ospf 10 vrf vrf1
PE2(config-router)# redistribute bgp subnets
PE2(config-router)# network 0.0.0.0 255.255.255.255 area 0
PE2(config-router)# exit
```

Configure PE3.

```
PE3> enable
PE3# configure terminal
PE3(config)# ip vrf vrf1
PE3(config-vrf)# rd 100:6
PE3(config-vrf)# route-target both 100:1
PE3(config-vrf)# exit
PE3(config)# interface gigabitethernet 0/2
PE3(config-if-Gigabitethernet 0/2)# ip vrf forwarding vrf1
PE3(config-if-Gigabitethernet 0/2)# ip address 80.1.1.1 255.255.255.0
PE3(config-if-Gigabitethernet 0/2)# exit
PE3(config)# router ospf 10 vrf vrf1
PE3(config-router)# redistribute bgp subnets
PE3(config-router)# network 0.0.0.0 255.255.255.255 area 0
PE3(config-router)# exit
```

(4) Configure MP-IBGP neighbor relationship between PE1 and PE2 and between PE1 and PE3 to transmit VPN routing information.

Configure PE1.

```
PE1(config)# router bgp 1
PE1(config-router)# neighbor 5.5.5.5 remote-as 1
PE1(config-router)# neighbor 5.5.5.5 update-source Loopback 0
PE1(config-router)# neighbor 6.6.6.6 remote-as 1
```

```
PE1(config-router)# neighbor 6.6.6.6 update-source Loopback 0
PE1(config-router)# address-family vpnv4
PE1(config-router-af)# neighbor 5.5.5.5 active
PE1(config-router-af)# neighbor 6.6.6.6 active
PE1(config-router-af)# exit
PE1(config-router)# address-family ipv4 vrf vrf1
PE1(config-router-af)# maximum-paths ibgp 32
PE1(config-router-af)# redistribute connected
PE1(config-router-af)# redistribute static
PE1(config-router-af)# redistribute ospf 10
PE1(config-router-af)# exit
PE1(config-router)# exit
```

Configure PE2.

```
PE2(config)# router bgp 1
PE2(config-router)# neighbor 2.2.2.2 remote-as 1
PE2(config-router)# neighbor 2.2.2.2 update-source Loopback 0
PE2(config-router)# address-family vpnv4
PE2(config-router-af)# neighbor 2.2.2.2 active
PE2(config-router-af)# exit
PE2(config-router)# address-family ipv4 vrf vrf1
PE2(config-router-af)# redistribute connected
PE2(config-router-af)# redistribute static
PE2(config-router-af)# redistribute ospf 10
PE2(config-router-af)# exit
PE2(config-router)# exit
```

Configure PE3.

```
PE3(config)# router bgp 1
PE3(config-router)# neighbor 2.2.2.2 remote-as 1
PE3(config-router)# neighbor 2.2.2.2 update-source Loopback 0
PE3(config-router)# address-family vpnv4
PE3(config-router-af)# neighbor 2.2.2.2 active
PE3(config-router-af)# exit
PE3(config-router)# address-family ipv4 vrf vrf1
PE3(config-router-af)# redistribute connected
PE3(config-router-af)# redistribute static
PE3(config-router-af)# redistribute ospf 10
PE3(config-router-af)# exit
PE3(config-router)# exit
```

(5) Generate equivalent LSPs for all routes on PE1 and PE2. This feature is enabled by default.

(6) Configure the number of equivalent paths that can be generated for the same FEC on PE1.

```
PE1(config)# router bgp 1
PE1(config-router)# address-family ipv4 vrf vrf1
PE1(config-router-af)# maximum-paths ibgp 32
PE1(config-router-af)# end
```

5. Verification

Run the **show mpls forwarding-table** command on PE1 to verify that equivalent L3VPN forwarding paths are established.

```
PE1# show mpls forwarding-table
Label Operation Code:
PH--PUSH label
PP--POP label
SW--SWAP label
SP-SWAP topmost label and push new label
DP-DROP packet
PC-POP label and continue lookup( IP or Label )
PI--POP label and do ip lookup forward
PN--POP label and forward to nexthop
PM--POP label and do MAC lookup forward
PV--POP label and output to VC attach interface
IP--IP lookup forward


Local    Outgoing OP FEC           Outgoing       Next Hop
label    label                    interface
  --     imp-null PH 5.5.5.5/32     Gi0/2          20.1.1.2
  --     imp-null PH 5.5.5.5/32     Gi0/3          30.1.1.2
  --     imp-null PH 6.6.6.6/32     Gi0/4          60.1.1.2
  --     1536    PH 7.7.7.7/32(V)   Gi0/2          20.1.1.2
  --     1536    PH 7.7.7.7/32(V)   Gi0/3          30.1.1.2
  --     1536    PH 7.7.7.7/32(V)   Gi0/4          60.1.1.2
...
```

6. Configuration Files

CE1 configuration file

```
hostname CE1
!
interface GigabitEthernet 0/1
 ip address 10.1.1.1 255.255.255.0
!
interface Loopback 0
 ip address 1.1.1.1 255.255.255.255
!
router ospf 1
 router-id 1.1.1.1
 network 1.1.1.1 0.0.0.0 area 0
 network 10.1.1.0 0.0.0.255 area 0
!
```

PE1 configuration file

```
hostname PE1
```

```
!
mpls enable
!
ip vrf vrf1
 rd 100:2
 route-target both 100:1
!
interface GigabitEthernet 0/1
 ip vrf forwarding vrf1
 ip address 10.1.1.2 255.255.255.0
!
interface GigabitEthernet 0/2
 ip address 20.1.1.1 255.255.255.0
 label-switching
 mpls ldp enable
!
interface GigabitEthernet 0/3
 ip address 30.1.1.1 255.255.255.0
 label-switching
 mpls ldp enable
!
interface GigabitEthernet 0/4
 ip address 60.1.1.1 255.255.255.0
 label-switching
 mpls ldp enable
!
interface Loopback 0
 ip address 2.2.2.2 255.255.255.255
!
router bgp 1
 neighbor 5.5.5.5 remote-as 1
 neighbor 5.5.5.5 update-source Loopback 0
 neighbor 6.6.6.6 remote-as 1
 neighbor 6.6.6.6 update-source Loopback 0
 !
 address-family ipv4
  neighbor 5.5.5.5 activate
  neighbor 6.6.6.6 activate
 exit-address-family
 !
 address-family vpnv4 unicast
  neighbor 5.5.5.5 activate
  neighbor 6.6.6.6 activate
  exit-address-family
 !
 address-family ipv4 vrf vrf1
```

```
 maximum-paths ibgp 32
 redistribute connected
 redistribute static
 redistribute ospf 10 match internal
exit-address-family
!
router ospf 1
 router-id 2.2.2.2
 network 2.2.2.2 0.0.0.0 area 0
 network 20.1.1.0 0.0.0.255 area 0
 network 30.1.1.0 0.0.0.255 area 0
 network 60.1.1.0 0.0.0.255 area 0
!
router ospf 10 vrf vrf1
 redistribute bgp subnets
 network 0.0.0.0 255.255.255.255 area 0
!
mpls router ldp
 ldp router-id interface Loopback 0
!
```

P1 configuration file

```
hostname P1
!
mpls enable
!
interface GigabitEthernet 0/1
 ip address 20.1.1.2 255.255.255.0
 label-switching
 mpls ldp enable
!
interface GigabitEthernet 0/2
 ip address 40.1.1.1 255.255.255.0
 label-switching
 mpls ldp enable
!
interface Loopback 0
 ip address 3.3.3.3 255.255.255.255
!
router ospf 1
 router-id 3.3.3.3
 network 3.3.3.3 0.0.0.0 area 0
 network 20.1.1.0 0.0.0.255 area 0
 network 40.1.1.0 0.0.0.255 area 0
!
mpls router ldp
 ldp router-id interface Loopback 0
```

```
!
```

Configuration file of P2

```
hostname P2
!
mpls enable
!
interface GigabitEthernet 0/1
 ip address 30.1.1.2 255.255.255.0
 label-switching
 mpls ldp enable
!
interface GigabitEthernet 0/2
 ip address 50.1.1.1 255.255.255.0
 label-switching
 mpls ldp enable
!
interface Loopback 0
 ip address 4.4.4.4 255.255.255.255
!
router ospf 1
 router-id 4.4.4.4
 network 4.4.4.4 0.0.0.0 area 0
 network 30.1.1.0 0.0.0.255 area 0
 network 50.1.1.0 0.0.0.255 area 0
!
mpls router ldp
 ldp router-id interface Loopback 0
!
```

PE2 configuration file

```
hostname PE2
!
mpls enable
!
ip vrf vrf1
 rd 100:5
 route-target both 100:1
!
interface GigabitEthernet 0/1
 ip address 40.1.1.2 255.255.255.0
 label-switching
 mpls ldp enable
!
interface GigabitEthernet 0/2
 ip address 50.1.1.2 255.255.255.0
 label-switching
```

```
 mpls ldp enable
!
interface GigabitEthernet 0/3
 ip vrf forwarding vrf1
 ip address 70.1.1.1 255.255.255.0
!
interface Loopback 0
 ip address 5.5.5.5 255.255.255.255
!
router bgp 1
 neighbor 2.2.2.2 remote-as 1
 neighbor 2.2.2.2 update-source Loopback 0
 !
 address-family ipv4
  neighbor 2.2.2.2 activate
 exit-address-family
 !
 address-family vpnv4 unicast
  neighbor 2.2.2.2 activate
 exit-address-family
 !
 address-family ipv4 vrf vrf1
  redistribute connected
  redistribute static
  redistribute ospf 10 match internal
 exit-address-family
!
router ospf 1
 router-id 5.5.5.5
 network 5.5.5.5 0.0.0.0 area 0
 network 40.1.1.0 0.0.0.255 area 0
 network 50.1.1.0 0.0.0.255 area 0
!
router ospf 10 vrf vrf1
 redistribute bgp subnets
 network 0.0.0.0 255.255.255.255 area 0
!
mpls router ldp
 ldp router-id interface Loopback 0
!
```

PE3 configuration file

```
hostname PE3
!
mpls enable ip
!
ip vrf vrf1
```

```
 rd 100:6
 route-target both 100:1
!
interface GigabitEthernet 0/1
 ip address 60.1.1.2 255.255.255.0
 label-switching
 mpls ldp enable
!
interface GigabitEthernet 0/2
 ip vrf forwarding vrf1
 ip address 80.1.1.1 255.255.255.0
!
interface Loopback 0
 ip address 6.6.6.6 255.255.255.255
!
router bgp 1
 neighbor 2.2.2.2 remote-as 1
 neighbor 2.2.2.2 update-source Loopback 0
 !
 address-family ipv4
  neighbor 2.2.2.2 activate
 exit-address-family
 !
 address-family vpnv4 unicast
  neighbor 2.2.2.2 activate
 exit-address-family
 !
 address-family ipv4 vrf vrf1
  redistribute connected
  redistribute static
  redistribute ospf 10 match internal
 exit-address-family
!
router ospf 1
 router-id 6.6.6.6
 network 6.6.6.6 0.0.0.0 area 0
 network 60.1.1.0 0.0.0.255 area 0
!
router ospf 10 vrf vrf1
 redistribute bgp subnets
 network 0.0.0.0 255.255.255.255 area 0
!
mpls router ldp
 ldp router-id interface Loopback 0
!
```

CE2 configuration file

```
hostname CE2
!
interface GigabitEthernet 0/1
 ip address 70.1.1.2 255.255.255.0
!
interface GigabitEthernet 0/2
 ip address 80.1.1.2 255.255.255.0
!
interface Loopback 0
 ip address 7.7.7.7 255.255.255.255
!
router ospf 1
 router-id 7.7.7.7
 network 7.7.7.7 0.0.0.0 area 0
 network 70.1.1.0 0.0.0.255 area 0
 network 80.1.1.0 0.0.0.255 area 0
!
```

4.6 Common Errors

- MPLS forwarding is not enabled on an interface.
- The **mpls enable** command is not enabled globally.
- During L3VPN ECMP implementation, the BGP multi-path function is not enabled.

5 LDP FRR

5.1 Overview

5.1.1 LDP FRR

LDP fast reroute (FRR) can instantly switch the traffic from the primary LSP to a backup LSP when a fault occurs on the primary LSP and switch the traffic from the backup LSP to the re-generated new LSP upon route convergence. It guarantees traffic continuity in a short period before network convergence, improve the reliability of the MPLS basic network, and protects key services on the MPLS network.

5.1.2 Basic Concepts

LDP FRR involves three types of paths, including the primary LSP, secondary LSP, and backup LSP. The three types of paths do not have equal-cost values.

1. Primary LSP

The primary LSP is the optimal routed path that forwards services in case of stable network and route convergence.

2. Secondary LSP

The secondary LSP has a cost value higher than that of the primary LSP. When the primary LSP fails, routes will be converged to this path.

3. Backup LSP

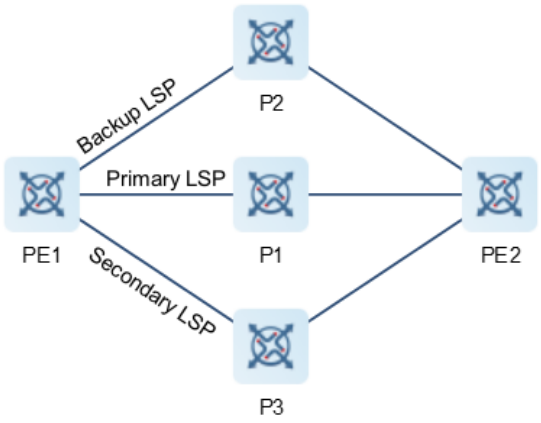
The backup LSP refers to the path specified by the backup next hop. It can be generated through LDP auto FRR.

- Auto configuration

  In LDP auto FRR mode, the device relies on IP FRR to establish a backup LSP based on the backup next hop of the IP address and delivers the backup LSP to the forwarding table. If the primary LSP fails, the device immediately switches the traffic to the backup LSP. By doing so, the traffic destined to the target network is forwarded over the backup LSP before routes are converged to the secondary LSP.

  Within several seconds after a link fault, a routing protocol is aware of the link fault and information is exchanged between devices to reselect a route, which is advertised to LDP. LDP re-generates the secondary LSP based on the new next hop in the advertised route. Then, the traffic destined to the target network is smoothly switched from the backup LSP to the secondary LSP. If the secondary LSP is the same as the backup LSP, there is no need to switch the traffic again. Anyway, traffic forwarding in this period undergoes two stages: backup LSP stage and secondary LSP stage after route convergence, just that the two stages use the same link.

Figure 5-1 LDP FRR



5.2 Configuration Task Summary

The LDP FRR configuration includes the following tasks:

Configuring LDP Auto FRR

5.3 Configuring LDP Auto FRR

1. Overview

You can configure LDP auto FRR to generate a backup LSP in auto mode, providing protection to the primary LSP.

2. Prerequisites

- Before you configure LDP auto FRR, the MPLS features must be enabled globally.
- Before you configure LDP auto FRR, the OSPF protocol must be configured to enable the network to forward MPLS traffic.
- Before you configure LDP auto FRR, IP FRR must be configured for OSPF.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enable LDP and enter the LDP configuration mode.

mpls router ldp [*vrf-name*]

(4) Enable LDP auto FRR.

auto-frr for { all | host | none | **acl** *acl-name* }

LDP is triggered to establish a backup LSP for backup host routes by default.

5.4 Configuration Examples

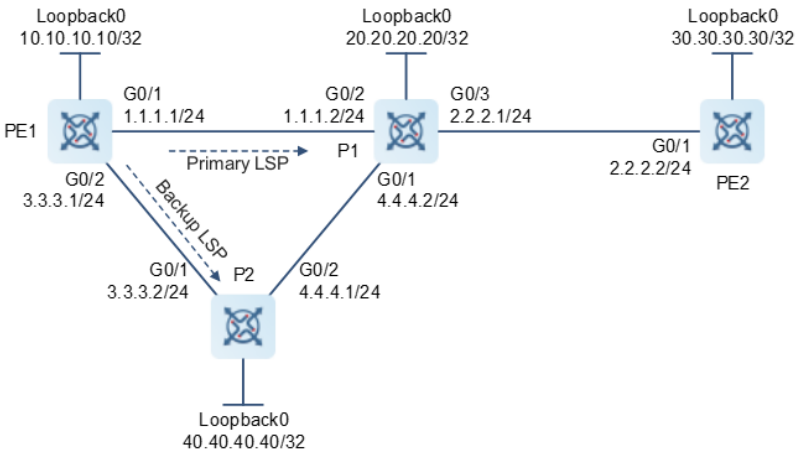
5.4.1 Configuring LDP Auto FRR

1. Requirements

Configure LDP auto FRR.

2. Topology

Figure 5-2 Configuring LDP Auto FRR



3. Notes

- Configure interface IP addresses on each node on the MPLS backbone network.
- Configure OSPF on each node on the MPLS backbone network to implement interoperability between the nodes.
- On each node, enable the MPLS forwarding capability globally and on interfaces, configure LDP, and establish LDP LSPs.
- Configure IP FRR for IGP.
- Configure auto FRR for LDP.
- Enable BFD on interfaces and configure BFD to detect the next hop.

4. Procedure

(1) Configure interface IP addresses on each node (omitted).

(2) Configure OSPF to implement interoperability between the nodes.

Configure OSPF on PE1. The configuration is similar on all the devices, and the configuration on PE1 is used as an example.

```
PE1> enable
PE1# configure terminal
PE1(config)# router ospf 1
PE1(config-router)# router-id 10.10.10.10
```

```
PE1(config-router)# network 0.0.0.0 255.255.255.255 area 0
PE1(config-router)# exit
```

(3) Configure the MPLS forwarding capability.

Configure the MPLS forwarding capability on PE1. The configuration is similar on all the devices, and the configuration on PE1 is used as an example.

```
PE1(config)# mpls enable
PE1(config)# interface gigabitethernet 0/1
PE1(config-if-Gigabitethernet 0/1)# mpls ldp enable
PE1(config-if-Gigabitethernet 0/1)# label-switching
PE1(config-if-Gigabitethernet 0/1)# exit
PE1(config)# interface gigabitethernet 0/2
PE1(config-if-Gigabitethernet 0/2)# mpls ldp enable
PE1(config-if-Gigabitethernet 0/2)# label-switching
PE1(config-if-Gigabitethernet 0/2)# exit
PE1(config)# mpls router ldp
PE1(config-mpls-router)# ldp router-id interface loopback 0 force
PE1(config-mpls-router)# exit
```

(4) Configure IP FRR for IGP.

On PE1, configure IP FRR for IGP.

```
PE1(config)# router ospf 1
PE1(config-router)# fast-reroute lfa
PE1(config-router)# exit
```

(5) Configure auto FRR for LDP.

On PE1, configure auto FRR for LDP.

```
PE1(config)# mpls router ldp
PE1(config-mpls-router)# auto-frr for all
PE1(config-router)# exit
```

(6) Enable BFD.

On an interface of PE1, configure BFD detection parameters.

```
PE1(config)# interface gigabitethernet 0/1
PE1(config-if-Gigabitethernet 0/1)# bfd interval 50 min_rx 50 multiplier 3
PE1(config-if-Gigabitethernet 0/1)# exit
```

On an interface of P1, configure BFD detection parameters.

```
P1(config)# interface gigabitethernet 0/2
P1(config-if-Gigabitethernet 0/2)# bfd interval 50 min_rx 50 multiplier 3
P1(config-if-Gigabitethernet 0/2)# exit
```

On PE1, configure association between BFD and IGP.

```
PE1(config)# router ospf 1
PE1(config-router)# bfd all-interfaces
```

On P1, configure association between BFD and IGP.

```
P1(config)# router ospf 1
```

```
P1(config-router)# bfd all-interfaces
```

5. Verification

On PE1, check the primary and secondary entries.

```
PE1#show mpls forwarding-table frr
Label Operation Code:
PH--PUSH label
PP--POP label
SW--SWAP label
SP--SWAP topmost label and push new label
DP--DROP packet
PC--POP label and continue lookup by IP or Label
PI--POP label and do ip lookup forward
PN--POP label and forward to nexthop
PM--POP label and do MAC lookup forward
PV--POP label and output to VC attach interface
IP--IP lookup forward
 s--stale
Status codes: m - main entry, b - backup entry, * - active.
    Local   Outgoing OP FEC                    Outgoing       Nexthop
    label   label                             interface
m*   --     imp-null PH 2.2.2.0/24              Gi0/2          1.1.1.2
b    --     9218     PH 2.2.2.0/24              Gi0/4          3.3.3.2
m*   --     imp-null PH 4.4.4.0/24              Gi0/2          1.1.1.2
m*   --     imp-null PH 20.20.20.20/32          Gi0/2          1.1.1.2
b    --     9220     PH 20.20.20.20/32          Gi0/4          3.3.3.2
m*   --     9227     PH 30.30.30.30/32          Gi0/2          1.1.1.2
b    --     9221     PH 30.30.30.30/32          Gi0/4          3.3.3.2
m*   --     imp-null PH 40.40.40.40/32          Gi0/4          3.3.3.2
b    --     9223     PH 40.40.40.40/32          Gi0/2          1.1.1.2
m*   9216   imp-null PP 2.2.2.0/24              Gi0/2          1.1.1.2
b    9216   9218     SW 2.2.2.0/24              Gi0/4          3.3.3.2
m*   9217   imp-null PP 4.4.4.0/24              Gi0/2          1.1.1.2
m*   9220   imp-null PP 20.20.20.20/32          Gi0/2          1.1.1.2
b    9220   9220     SW 20.20.20.20/32          Gi0/4          3.3.3.2
m*   9222   9227     SW 30.30.30.30/32          Gi0/2          1.1.1.2
b    9222   9221     SW 30.30.30.30/32          Gi0/4          3.3.3.2
m*   9223   imp-null PP 40.40.40.40/32          Gi0/4          3.3.3.2
b    9223   9223     PP 40.40.40.40/32          Gi0/2          1.1.1.2
```

6. Configuration Files

- PE1 configuration file

```
hostname PE1
!
mpls enable
!
```

```
interface GigabitEthernet 0/1
 ip address 1.1.1.1 255.255.255.0
 label-switching
 mpls ldp enable
 bfd interval 50 min_rx 50 multiplier 3
!
interface GigabitEthernet 0/2
 ip address 3.3.3.1 255.255.255.0
 label-switching
 mpls ldp enable
!
interface Loopback 0
 ip address 10.10.10.10 255.255.255.255
!
router ospf 1
 router-id 10.10.10.10
 fast-reroute lfa
 network 0.0.0.0 255.255.255.255 area 0
 bfd all-interfaces
!
mpls router ldp
 ldp router-id interface Loopback 0
 auto-frr for all
!
```

- P1 configuration file

```
hostname P1
!
mpls enable
!
interface GigabitEthernet 0/1
 ip address 4.4.4.2 255.255.255.0
 label-switching
 mpls ldp enable
!
interface GigabitEthernet 0/2
 ip address 1.1.1.2 255.255.255.0
 label-switching
 mpls ldp enable
 bfd interval 50 min_rx 50 multiplier 3
!
interface GigabitEthernet 0/3
 ip address 2.2.2.1 255.255.255.0
 label-switching
 mpls ldp enable
!
interface Loopback 0
```

```
 ip address 20.20.20.20 255.255.255.255
!
router ospf 1
 router-id 20.20.20.20
 network 0.0.0.0 255.255.255.255 area 0
 bfd all-interfaces
!
mpls router ldp
 ldp router-id interface Loopback 0
!
```

- P2 configuration file

```
hostname P2
!
mpls enable
!
interface GigabitEthernet 0/1
 ip address 3.3.3.2 255.255.255.0
 label-switching
 mpls ldp enable
!
interface GigabitEthernet 0/2
 ip address 4.4.4.1 255.255.255.0
 label-switching
 mpls ldp enable
!
interface Loopback 0
 ip address 40.40.40.40 255.255.255.255
!
router ospf 1
 router-id 40.40.40.40
 network 0.0.0.0 255.255.255.255 area 0
!
mpls router ldp
 ldp router-id interface Loopback 0
!
```

- PE2 configuration file

```
hostname PE2
!
mpls enable
!
interface GigabitEthernet 0/1
 ip address 2.2.2.2 255.255.255.0
 label-switching
 mpls ldp enable
!
```

```
interface Loopback 0
 ip address 30.30.30.30 255.255.255.255
!
router ospf 1
 router-id 30.30.30.30
 network 0.0.0.0 255.255.255.255 area 0
!
mpls router ldp
 ldp router-id interface Loopback 0
!
```

5.5 Common Errors

- The **mpls enable** command is not enabled globally.
- MPLS forwarding is not enabled on an interface (by running the **label-switching** command).
- IP FRR is not configured.

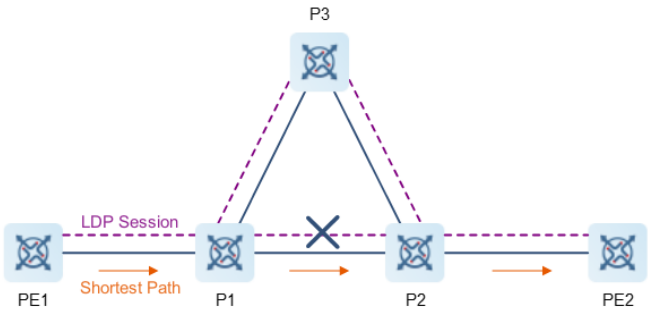
6 Configuring LDP-IGP Synchronization

6.1 Introduction

6.1.1 Overview

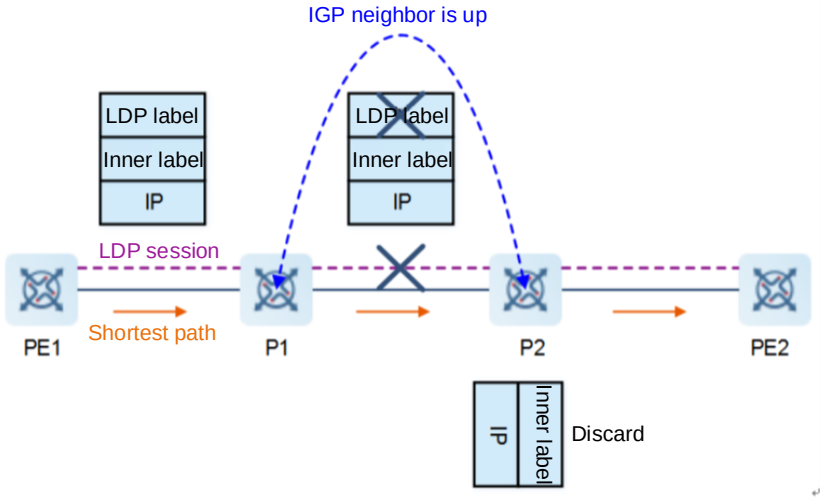
On an MPLS network, LDP establishes LSPs along the shortest path to the destination as determined by IP forwarding. When active and standby LSPs exist, traffic loss may occur due to inconsistent convergence conditions and speeds of the LDP LSP and the IP shortest path. LDP-IGP synchronization ensures consistent convergence between LDP and IGP by changing the IGP route distribution mode. This prevents traffic loss when the active LSP is faulty and ensures network reliability.

Figure 6-1 MPLS Network Topology When a Fault Occurs



As shown in Figure 6-1, devices can communicate with each other at the data link layer and run IGP and LDP. The shortest path from PE1 to PE2 is PE1-P1-P2-PE2, and the path covers the LDP LSP. When the LDP session between P1 and P2 is interrupted but the link and IGP between P1 and P2 are normal, the network topology remains unchanged and the routing protocol cannot perceive this change. LDP knows that the LSP is interrupted. However, it cannot trigger a switchover to a backup path because it is not a routing protocol. The shortest path from PE1 to PE2 is still PE1-P1-P2-PE2. However, the LSP is interrupted at P1-P2. If the current path is forwarding MPLS VPN/6PE traffic, the traffic is affected because the LSP from PE1 to PE2 is interrupted.

Figure 6-2 Forwarding MPLS VPN/6PE Traffic in an LSP

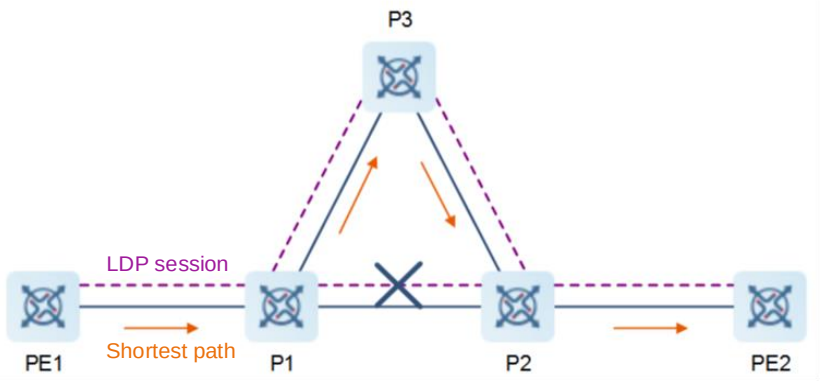


As shown in Figure 6-2, the LSP between PE1 and PE2 is used to forward MPLS VPN or 6PE traffic, and labeled packets are transmitted in the LDP LSP. When the LDP session between P1 and P2 is interrupted, packets have only an incoming label and do not have an outgoing label at P1. Then, P1 removes the LDP label and forwards the packets with the inner label to P2. P2 cannot identify the inner label. As a result, the packet is discarded between P1 and P2, resulting in a traffic forwarding black hole. Generally, the IPv4 route table of public network core device P does not have private network routes. The inner label is not distributed by P2, and therefore P2 cannot identify it.

For MPLS VPNs (including L3VPN) and 6PE that establish end-to-end LSPs based on MPLS LDP, MPLS route black holes may occur if the LDP LSP and the IP shortest path have inconsistent convergence speeds.

To solve the preceding problem, configure LDP-IGP synchronization on core devices.

Figure 6-3 MPLS Network Topology



As shown in Figure 6-3, the LSP between PE1 and PE2 is used to forward MPLS VPN or 6PE traffic, and labeled packets are transmitted in the LDP LSP. LDP-IGP synchronization is enabled on P1, P2, and P3. When the LDP session between P1 and P2 is interrupted, LDP-IGP synchronization triggers IGP and LDP LSP convergence to the backup path P1-P3-P2. The new path covers both IGP and LDP LSPs and no MPLS route black hole occurs.

Note

In the network, a backup path must be deployed for the primary link. If no backup path is configured, LDP-IGP synchronization is meaningless.

6.1.2 Principles

1. Cut-edge interface

If a device does not have a backup link to a directly connected network, the interface used to connect to the directly connected network is a cut-edge interface to the device. When the cut-edge interface is Down, the network is divided into two subnets.

2. Implementation

(1) When a device establishes adjacency with a broadcast network for the first time, the device determines whether the interface of the link to be advertised to the broadcast network is a cut-edge interface.

(2) If it is a cut-edge interface, the device advertises the normal metric value immediately.

(3) If it is not a cut-edge interface, the device checks LDP convergence of the link. For a broadcast network, it is regarded that LDP of a link is converged only when the link has established LDP sessions and completed label binding with all other LDP peers in the network.

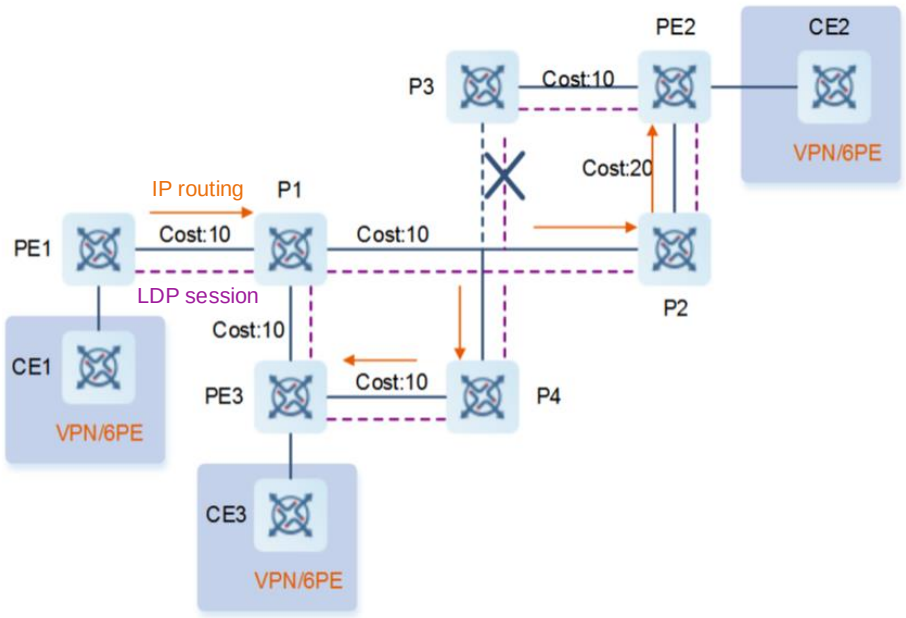
(4) If LDP of the link is converged, the device advertises the normal metric value immediately.

(5) If LDP of the link is not converged, the device advertises the normal metric value until LDP is converged.

(6) When the LDP adjacency of the link is interrupted, the device also needs to determine whether the interface of the link is a cut-edge interface. If it is a cut-edge interface, the device retains the IGP status. If it is not a cut-edge interface, the device deletes the link from the link state database (LSDB) of IGP.

(7) When LDP of the link reconverges, the device adds the link to the LSDB and advertises the normal metric value to the network.

Figure 6-4 Broadcast Network Topology



As shown in Figure 6-4, when the interface on P3 used to connected to the broadcast network is Up, the interface is not a cut-edge interface because a backup path (P3-PE2-P2) to the directly connected network exists. IGP suppresses adding the new Up link to the LSDB. Therefore, traffic does not pass through the link. When LDP of the link used to connect to the broadcast network is converged, P3 updates the normal metric value and adds the link to the LSDB for SPF and route calculation. The new path covers both IGP and LDP LSPs, and no MPLS route black hole occurs.

6.2 Configuration Task Summary

Configuration of LDP-IGP synchronization includes the following tasks:

(1) Enabling LDP-IGP Synchronization

(2) (Optional) Configuring the Time for IGP to Wait for LDP Synchronization Completion

6.3 Enabling LDP-IGP Synchronization

1. Overview

Enable LDP-IGP synchronization to ensure consistent LDP and IGP convergence. To enable LDP-IGP synchronization, use either of the following methods:

- Run the **mpls ldp sync** command in IGP instance configuration mode to enable LDP-IGP synchronization globally. This method applies when LDP-IGP synchronization needs to be enabled for multiple interfaces.
- Run the **mpls ldp igp sync** command in interface configuration mode to enable LDP-IGP synchronization for an interface. This method applies when LDP-IGP synchronization needs to be enabled for an interface.

2. Restrictions and Guidelines

- When LDP-IGP synchronization is enabled globally in IGP instance configuration mode, only IS-IS and OSPF are supported and other IGPs are not supported.
- Generally, the **mpls ldp igp sync** command is used together with the **mpls ldp sync** command. When LDP-IGP synchronization is enabled globally in IGP instance configuration mode by running the **mpls ldp sync** command, the function is enabled for all interfaces that belong to the instance. You can run the **no mpls ldp igp sync** or **mpls ldp igp sync** command in interface configuration mode to enable or disable LDP-IGP synchronization for an specified interface.

3. Prerequisites

In a network, a backup path must be deployed for the primary link. If no backup path is configured, LDP-IGP synchronization is meaningless.

4. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the IS-IS routing process configuration mode.

router isis [*tag*]

(4) Enable LDP-IGP synchronization globally.

mpls ldp sync

Enable LDP-IGP synchronization for all interfaces that run IGP.

(5) Enter the Layer 3 Ethernet interface configuration mode.

interface *ethernet-type interface-number*

(6) (Optional) Enable LDP-IGP synchronization for an interface.

mpls ldp igp sync

LDP-IGP synchronization is enabled for all interfaces by default.

6.4 Configuring the Time for IGP to Wait for LDP Synchronization Completion

1. Overview

Configure the time for IGP to wait for LDP synchronization completion. When the primary link fault is restored but the LDP session is not reestablished before the time for IGP to wait for LDP synchronization completion, IGP does not establish neighbor relationship. This ensures that LDP and IGP traffic is switched back to the primary link at the same time.

2. Restrictions and Guidelines

The time for IGP to wait for LDP synchronization completion cannot be smaller than the delay time for LDP-IGP synchronization. Otherwise, IGP is be converged before LDP.

3. Prerequisites

In a network, a backup path must be deployed for the primary link. If no backup path is configured, LDP-IGP synchronization is meaningless.

4. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the Layer 3 Ethernet interface configuration mode.

interface *ethernet-type interface-number*

(4) Configure the time for IGP to wait for LDP synchronization completion.

mpls ldp igp sync holddown { *holddown-time* **| infinite }**

By default, the time for IGP to wait for LDP synchronization completion is 10s**.**

6.5 Monitoring

Run the **show** command to check the configuration.

Table 6-1 Monitoring

Command	Purpose
show mpls ldp igp sync [**all** | **interface** *interface-type interface-number* | **vrf** *vrf-name*]	Displays information related to LDP-IGP synchronization.
show isis [*tag*] **mpls ldp interface** [*interface-type interface-number*]	Displays LDP-IGP synchronization information on an interface of the IS-IS process.

6.6 Configuration Examples

6.6.1 Configuring LDP-IGP Synchronization

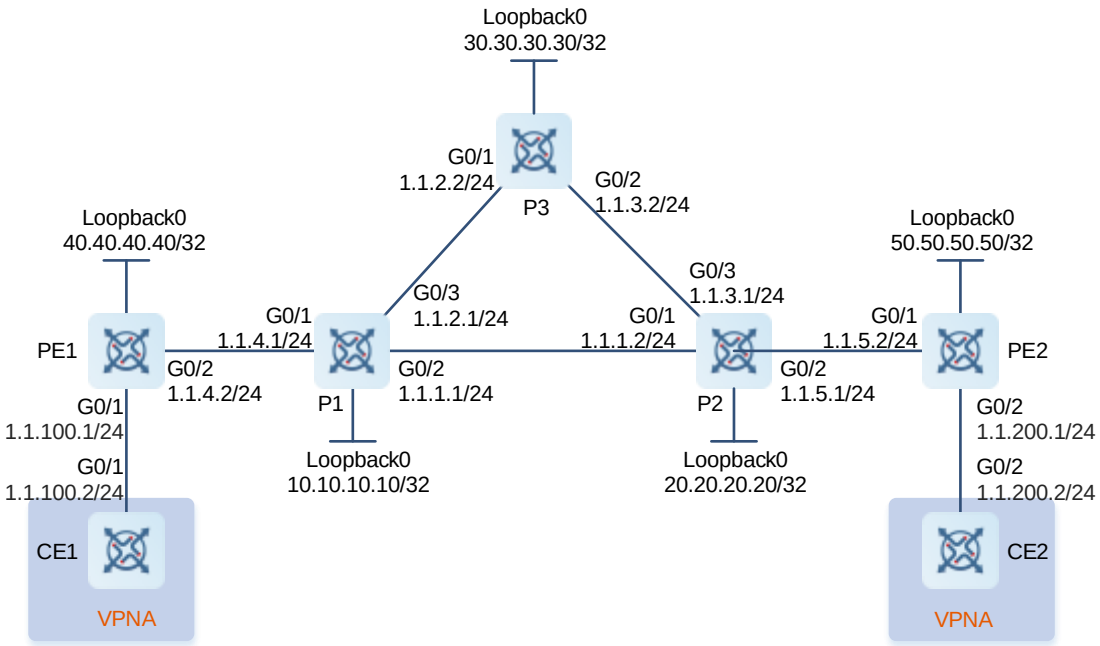
1. Requirements

Primary and secondary LSPs exist. PE1->P1->P2->PE2 is the primary LSP, and PE1->P1->P3->P2->PE2 is the secondary LSP.

- When the primary LSP is faulty, IGP and LSP traffic can be switched to the secondary LSP.
- When the primary LSP is restored, IGP and LSP traffic can be switched back to the primary LSP.

2. Topology

Figure 6-5 Configuring LDP-IGP Synchronization



3. Notes

- Configure the interface IP addresses and IS-IS protocol on the MPLS backbone network nodes.
- Configure MPLS forwarding and LDP and establish an LDP LSP.

- Configure VPN instances and MP-IBGP neighbors on PE1 and PE2 to transmit VPN routing information.
- Enable LDP-IGP synchronization on P1, P2, and P3.

4. Procedure

(1) Configure interface IP addresses and IS-IS protocol on the MPLS backbone network nodes to ensure interconnection between PEs and Ps.

Configure PE1.

```
PE1> enable
PE1# configure terminal
PE1(config)# router isis
PE1(config-router)# net 49.0000.0000.0011.00
PE1(config-router)# exit
PE1(config)# interface Loopback 0
PE1(config-if-Loopback 0)# ip address 40.40.40.40 255.255.255.255
PE1(config-if-Loopback 0)# ip router isis
PE1(config-if-Loopback 0)# exit
PE1(config)# interface gigabitethernet 0/2
PE1(config-if-Gigabitethernet 0/2)# ip address 1.1.4.2 255.255.255.0
PE1(config-if-Gigabitethernet 0/2)# ip router isis
PE1(config-if-Gigabitethernet 0/2)# exit
```

Configure P1.

```
P1> enable
P1# configure terminal
P1(config)# router isis
P1(config-router)# net 49.0000.0000.0001.00
P1(config-router)# exit
P1(config)# interface Loopback 0
P1(config-if-Loopback 0)# ip address 10.10.10.10 255.255.255.255
P1(config-if-Loopback 0)# ip router isis
P1(config-if-Loopback 0)# exit
P1(config)# interface gigabitethernet 0/1
P1(config-if-Gigabitethernet 0/1)# ip address 1.1.4.1 255.255.255.0
P1(config-if-Gigabitethernet 0/1)# ip router isis
P1(config-if-Gigabitethernet 0/1)# exit
P1(config)# interface gigabitethernet 0/2
P1(config-if-Gigabitethernet 0/2)# ip address 1.1.1.1 255.255.255.0
P1(config-if-Gigabitethernet 0/2)# ip router isis
P1(config-if-Gigabitethernet 0/2)# exit
P1(config)# interface gigabitethernet 0/3
P1(config-if-Gigabitethernet 0/3)# ip address 1.1.2.1 255.255.255.0
P1(config-if-Gigabitethernet 0/3)# ip router isis
P1(config-if-Gigabitethernet 0/3)# exit
```

Configure P2.

```
P2> enable
```

```
P2# configure terminal
P2(config)# router isis
P2(config-router)# net 49.0000.0000.0002.00
P2(config-router)# exit
P2(config)# interface Loopback 0
P2(config-if-Loopback 0)# ip address 20.20.20.20 255.255.255.255
P2(config-if-Loopback 0)# ip router isis
P2(config-if-Loopback 0)# exit
P2(config)# interface gigabitethernet 0/1
P2(config-if-Gigabitethernet 0/1)# ip address 1.1.1.2 255.255.255.0
P2(config-if-Gigabitethernet 0/1)# ip router isis
P2(config-if-Gigabitethernet 0/1)# exit
P2(config)# interface gigabitethernet 0/2
P2(config-if-Gigabitethernet 0/2)# ip address 1.1.5.1 255.255.255.0
P2(config-if-Gigabitethernet 0/2)# ip router isis
P2(config-if-Gigabitethernet 0/2)# exit
P2(config)# interface gigabitethernet 0/3
P2(config-if-Gigabitethernet 0/3)# ip address 1.1.3.1 255.255.255.0
P2(config-if-Gigabitethernet 0/3)# ip router isis
P2(config-if-Gigabitethernet 0/3)# exit
```

Configure P3.

```
P3> enable
P3# configure terminal
P3(config)# router isis
P3(config-router)# net 49.0000.0000.0003.00
P3(config)# interface Loopback 0
P3(config-if-Loopback 0)# ip address 30.30.30.30 255.255.255.255
P3(config-if-Loopback 0)# ip router isis
P3(config-if-Loopback 0)# exit
P3(config)# interface gigabitethernet 0/1
P3(config-if-Gigabitethernet 0/1)# ip address 1.1.2.2 255.255.255.0
P3(config-if-Gigabitethernet 0/1)# ip router isis
P3(config-if-Gigabitethernet 0/1)# exit
P3(config)# interface gigabitethernet 0/2
P3(config-if-Gigabitethernet 0/2)# ip address 1.1.3.2 255.255.255.0
P3(config-if-Gigabitethernet 0/2)# ip router isis
P3(config-if-Gigabitethernet 0/2)# exit
```

Configure PE2.

```
PE2> enable
PE2# configure terminal
PE2(config)# router isis
PE2(config-router)# net 49.0000.0000.0012.00
PE2(config-router)# exit
PE2(config)# interface Loopback 0
PE2(config-if-Loopback 0)# ip address 50.50.50.50 255.255.255.255
```

```
PE2(config-if-Loopback 0)# ip router isis
PE2(config-if-Loopback 0)# exit
PE2(config)# interface gigabitethernet 0/1
PE2(config-if-Gigabitethernet 0/1)# ip address 1.1.5.2 255.255.255.0
PE2(config-if-Gigabitethernet 0/1)# ip router isis
PE2(config-if-Gigabitethernet 0/1)# exit
```

(2) Configure MPLS forwarding and LDP.

Configure PE1.

```
PE1(config)# mpls enable
PE1(config)# mpls router ldp
PE1(config-mpls-router)# ldp rouer-id interface Loopback 0 force
PE1(config-mpls-router)# exit
PE1(config)# interface gigabitethernet 0/2
PE1(config-if-Gigabitethernet 0/2)# mpls ldp enable
PE1(config-if-Gigabitethernet 0/2)# label-switching
PE1(config-if-Gigabitethernet 0/2)# exit
```

Configure PE2.

```
PE2(config)# mpls enable
PE2(config)# mpls router ldp
PE2(config-mpls-router)# ldp rouer-id interface Loopback 0 force
PE2(config-mpls-router)# exit
PE2(config)# interface gigabitethernet 0/1
PE2(config-if-Gigabitethernet 0/1)# mpls ldp enable
PE2(config-if-Gigabitethernet 0/1)# label-switching
PE2(config-if-Gigabitethernet 0/1)# exit
```

Configure P1.

```
P1> enable
P1# configure terminal
P1(config)# mpls enable
P1(config)# mpls router ldp
P1(config-mpls-router)# ldp rouer-id interface Loopback 0 force
P1(config-mpls-router)# exit
P1(config)# interface gigabitethernet 0/1
P1(config-if-Gigabitethernet 0/1)# mpls ldp enable
P1(config-if-Gigabitethernet 0/1)# label-switching
P1(config-if-Gigabitethernet 0/1)# exit
P1(config)# interface gigabitethernet 0/2
P1(config-if-Gigabitethernet 0/2)# mpls ldp enable
P1(config-if-Gigabitethernet 0/2)# label-switching
P1(config-if-Gigabitethernet 0/2)# exit
P1(config)# interface gigabitethernet 0/3
P1(config-if-Gigabitethernet 0/3)# mpls ldp enable
P1(config-if-Gigabitethernet 0/3)# label-switching
P1(config-if-Gigabitethernet 0/3)# exit
```

Configure P2.

```
P2(config)# mpls enable
P2(config)# mpls router ldp
P2(config-mpls-router)# ldp rouer-id interface Loopback 0 force
P2(config-mpls-router)# exit
P2(config)# interface gigabitethernet 0/1
P2(config-if-Gigabitethernet 0/1)# mpls ldp enable
P2(config-if-Gigabitethernet 0/1)# label-switching
P2(config-if-Gigabitethernet 0/1)# exit
P2(config)# interface gigabitethernet 0/2
P2(config-if-Gigabitethernet 0/2)# mpls ldp enable
P2(config-if-Gigabitethernet 0/2)# label-switching
P2(config-if-Gigabitethernet 0/2)# exit
P2(config)# interface gigabitethernet 0/3
P2(config-if-Gigabitethernet 0/3)# mpls ldp enable
P2(config-if-Gigabitethernet 0/3)# label-switching
P2(config-if-Gigabitethernet 0/3)# exit
```

Configure P3.

```
P3(config)# mpls enable
P3(config)# mpls router ldp
P3(config-mpls-router)# ldp rouer-id interface Loopback 0 force
P3(config-mpls-router)# exit
P3(config)# interface gigabitethernet 0/1
P3(config-if-Gigabitethernet 0/1)# mpls ldp enable
P3(config-if-Gigabitethernet 0/1)# label-switching
P3(config-if-Gigabitethernet 0/1)# exit
P3(config)# interface gigabitethernet 0/2
P3(config-if-Gigabitethernet 0/2)# mpls ldp enable
P3(config-if-Gigabitethernet 0/2)# label-switching
P3(config-if-Gigabitethernet 0/2)# exit
```

(3) Configure VPN route instances on PE1 and PE2 and connect CE1 to PE1 and CE2 to PE2.

Configure PE1.

```
PE1(config)# ip vrf vpna
PE1(config-vrf)# rd 65001:20
PE1(config-vrf)# route-target both 65001:20
PE1(config-vrf)# exit
PE1(config)# interface gigabitethernet 0/1
PE1(config-if-Gigabitethernet 0/1)# ip vrf forwarding vpna
PE1(config-if-Gigabitethernet 0/1)# ip address 1.1.100.1 255.255.255.0
PE1(config-if-Gigabitethernet 0/1)# exit
PE1(config)# router ospf 10 vrf vpna
PE1(config-router)# network 1.1.100.0 0.0.0.255 area 0
PE1(config-router)# exit
```

Configure PE2.

```
PE2(config)# ip vrf vpna
PE2(config-vrf)# rd 65001:20
PE2(config-vrf)# route-target both 65001:20
PE2(config-vrf)# exit
PE2(config)# interface gigabitethernet 0/2
PE2(config-if-Gigabitethernet 0/2)# ip vrf forwarding vpna
PE2(config-if-Gigabitethernet 0/2)# ip address 1.1.200.1 255.255.255.0
PE2(config-if-Gigabitethernet 0/2)# exit
PE2(config)# router ospf 10 vrf vpna
PE2(config-router)# network 1.1.200.0 0.0.0.255 area 0
PE2(config-router)# exit
```

Configure CE1.

```
CE1> enable
CE1# configure terminal
CE1(config)# interface gigabitethernet 0/1
CE1(config-if-Gigabitethernet 0/1)# ip address 1.1.100.2 255.255.255.0
```

Configure CE2.

```
CE2> enable
CE2# configure terminal
CE2(config)# interface gigabitethernet 0/1
CE2(config-if-Gigabitethernet 0/1)# ip address 1.1.200.2 255.255.255.0
```

(4) Configure MP-IBGP neighbor relationship between PE1 and PE2 to transmit VPN routing information.

Configure PE1.

```
PE1(config)# router bgp 65001
PE1(config-router)# neighbor 50.50.50.50 remote-as 65001
PE1(config-router)# neighbor 50.50.50.50 update-source Loopback 0
PE1(config-router)# address-family vpnv4
PE1(config-router-af)# neighbor 50.50.50.50 activate
PE1(config-router-af)# neighbor 50.50.50.50 send-community both
PE1(config-router-af)# exit
PE1(config-router)# address-family ipv4 vrf vpna
PE1(config-router-af)# redistribute connected
```

Configure PE2.

```
PE2(config)# router bgp 65001
PE2(config-router)# neighbor 40.40.40.40 remote-as 65001
PE2(config-router)# neighbor 40.40.40.40 update-source Loopback 0
PE2(config-router)# address-family vpnv4
PE2(config-router-af)# neighbor 40.40.40.40 activate
PE2(config-router-af)# neighbor 40.40.40.40 send-community both
PE2(config-router-af)# exit
PE2(config-router)# address-family ipv4 vrf vpna
PE2(config-router-af)# redistribute connected
```

(5) Enable LDP-IGP synchronization on P1, P2, and P3. P1 is used as an example. Configurations on P2 and P3 are similar to those on P1.

Configure P1.

```
P1(config)# router isis
P1(config-router)# mpls ldp sync
P1(config-router)# end
```

5. Verification

Check whether LDP-IGP synchronization is enabled. P1 is used as an example.

```
P1# show mpls ldp igp sync
Default VRF:
  Gigabitethernet 0/1:
    LDP-IGP Sync configured: enable
    Family IPv4:
      SYNC status: sync required; LSP status: achieved
        SYNC delay time: 5 seconds (0 seconds left)
        Peer Ident: 40.40.40.40
        IGP enabled: ISIS
  Gigabitethernet 0/2:
    LDP-IGP Sync configured: enable
    Family IPv4:
      SYNC status: sync required; LSP status: achieved
        SYNC delay time: 5 seconds (0 seconds left)
        Peer Ident: 20.20.20.20
        IGP enabled: ISIS
  Gigabitethernet 0/3:
    LDP-IGP Sync configured: enable
    Family IPv4:
      SYNC status: sync required; LSP status: achieved
        SYNC delay time: 5 seconds (0 seconds left)
        Peer Ident: 30.30.30.30
        IGP enabled: ISIS
```

Verify the LDP-IGP synchronization function.

- When the primary link (PE1->P1->P2->PE2) is normal, CE1 communicates with CE2 through this link.
- When the primary link is faulty, traffic between CE1 and CE2 is switched to the secondary link (PE1->P1->P3->P2->PE2). When the primary link is restored, IGP and LSP traffic between CE1 and CE2 can be switched back to the primary link at the same time without traffic loss.

6. Configuration Files

CE1 configuration file

```
hostname CE1
!
interface GigabitEthernet 0/1
 ip address 1.1.100.2 255.255.255.0
!
```

PE1 configuration file

```
hostname PE1
!
mpls enable
!
ip vrf vpna
 rd 65001:20
 route-target both 65001:20
!
interface GigabitEthernet 0/1
 ip vrf forwarding vpna
 ip address 1.1.100.1 255.255.255.0
ip router isis
!
interface GigabitEthernet 0/2
 ip address 1.1.4.2 255.255.255.0
 ip router isis
 mpls ldp enable
 label-switching
!
interface Loopback 0
 ip address 40.40.40.40 255.255.255.255
 ip router isis
!
router bgp 65001
 neighbor 50.50.50.50 remote-as 65001
 neighbor 50.50.50.50 update-source Loopback 0
 address-family vpnv4
  neighbor 50.50.50.50 activate
  neighbor 50.50.50.50 send-community both
 exit-address-family
!
 address-family ipv4 vrf vpna
  redistribute connected
 exit-address-family
!
router isis
 net 49.0000.0000.0011.00
!
router ospf 10 vrf vpna
 network 1.1.100.0 0.0.0.255 area 0
!
mpls router ldp
 ldp router-id interface Loopback 0
!
```

P1 configuration file

```
hostname P1
```

```
!
mpls enable
!
interface GigabitEthernet 0/1
 ip address 1.1.4.1 255.255.255.0
 ip router isis
 mpls ldp enable
 label-switching
!
interface GigabitEthernet 0/2
 ip address 1.1.1.1 255.255.255.0
 ip router isis
 mpls ldp enable
 label-switching
!
interface GigabitEthernet 0/3
 ip address 1.1.2.1 255.255.255.0
 ip router isis
 mpls ldp enable
 label-switching
!
interface Loopback 0
 ip address 10.10.10.10 255.255.255.255
 ip router isis
!
router isis
 net 49.0000.0000.0001.00
 mpls ldp sync
!
mpls router ldp
 ldp router-id interface Loopback 0
!
```

P2 configuration file

```
hostname P2
!
mpls enable
!
interface GigabitEthernet 0/1
 ip address 1.1.1.2 255.255.255.0
 ip router isis
 mpls ldp enable
 label-switching
!
interface GigabitEthernet 0/2
 ip address 1.1.5.1 255.255.255.0
 ip router isis
```

```
 mpls ldp enable
 label-switching
!
interface GigabitEthernet 0/3
 ip address 1.1.3.1 255.255.255.0
 ip router isis
 mpls ldp enable
 label-switching
!
interface Loopback 0
 ip address 20.20.20.20 255.255.255.255
 ip router isis
!
router isis
 net 49.0000.0000.0002.00
!
mpls router ldp
 ldp router-id interface Loopback 0
!
```

P3 configuration file

```
hostname P3
!
mpls enable
!
interface GigabitEthernet 0/1
 ip address 1.1.2.2 255.255.255.0
 ip router isis
 mpls ldp enable
 label-switching
!
interface GigabitEthernet 0/2
 ip address 1.1.3.2 255.255.255.0
 ip router isis
 mpls ldp enable
 label-switching
!
interface Loopback 0
 ip address 30.30.30.30 255.255.255.255
 ip router isis
!
router isis
 net 49.0000.0000.0003.00
!
mpls router ldp
 ldp router-id interface Loopback 0
!
```

PE2 configuration file

```
hostname PE2
!
mpls enable
!
ip vrf vpna
 rd 65001:20
 route-target both 65001:20
!
interface GigabitEthernet 0/1
 ip address 1.1.5.2 255.255.255.0
 ip router isis
 mpls ldp enable
 label-switching
!
interface GigabitEthernet 0/2
 ip vrf forwarding vpna
 ip address 1.1.200.1 255.255.255.0
 ip router isis
!
interface Loopback 0
 ip address 50.50.50.50 255.255.255.255
 ip router isis
!
router bgp 65001
 neighbor 40.40.40.40 remote-as 65001
 neighbor 40.40.40.40 update-source Loopback 0
 address-family vpnv4
  neighbor 40.40.40.40 activate
  neighbor 40.40.40.40 send-community both
 exit-address-family
!
 address-family ipv4 vrf vpna
  redistribute connected
 exit-address-family
!
router isis
 net 49.0000.0000.0012.00
!
router ospf 10 vrf vpna
 network 1.1.200.0 0.0.0.255 area 0
!
mpls router ldp
 ldp router-id interface Loopback 0
!
```

CE2 configuration file

```
hostname CE2
!
interface GigabitEthernet 0/1
 ip address 1.1.200.2 255.255.255.0
!
```

7. Common Errors

- Static FTN and ILM entries do not take effect.
- No complete LSP is established.
- MPLS forwarding is not enabled globally.
- MPLS forwarding is not enabled on an interface.

7 LDP NSR

7.1 Overview

7.1.1 LDP NSR

LDP Non-Stop Routing (NSR) backs up LDP-related information from the master supervisor module to the slave supervisor module, without the support by LDP neighbors. If a primary/secondary switchover occurs on the device (due to master supervisor module fault or manual switchover), LDP entries can be automatically recovered to ensure uninterrupted data forwarding. During this period, the LDP control plane of neighbors is not aware of the situation.

7.2 Monitoring

Run the **show** command to check the configuration.

Table 1-1 LDP NSR Monitoring

Command	Purpose
show mpls ldp nsr [**detail**] [**all** | **vrf** *vrf-name*] **show mpls ldp nsr backup** { { **attr** [**neighbor** *ipv4-address*] | **fec** | **local-address** | **route** | **withdraw-address** } [**all** | **vrf** *vrf-name*] | **label** } **show mpls ldp nsr ha-sock** *ipv4-address* [**all** | **vrf** *vrf-name*] **show mpls ldp nsr retry-wait-list** [**detail**] **show mpls ldp nsr statistics**	Displays LDP NSR information.