

# 6 MPLS

---

Multiprotocol Label Switching (MPLS) was introduced to improve the forwarding speed. However, because of its excellent performance in traffic engineering (TE) and virtual private network (VPN), which are the two critical technologies, MPLS is becoming an important standard for extending the IP network.

## [6.1 Overview](#)

## [6.2 MPLS Reference Standards and Protocols](#)

## [6.3 MPLS Overview](#)

Multiprotocol Label Switching (MPLS) was introduced to improve the forwarding speed. However, because of its excellent performance in traffic engineering (TE) and virtual private network (VPN), which are the two critical technologies, MPLS is becoming an important standard for extending the IP network. This topic provides the introduction, availability, principle, and reference of the MPLS feature.

## [6.4 MPLS RSVP-TE](#)

MPLS RSVP-TE is a technology which integrates TE and the MPLS superimposed model. It provides high quality of service (QoS) and TE capability for users by establishing LSPs based on TE. This topic provides introduction to this feature and describes the principle and reference documents of this feature.

## [6.5 MPLS OAM](#)

MPLS OAM checks if an LSP is in the normal state through a mechanism, and reports the alarm information if the LSP fails. This topic provides introduction to this feature and describes the principle and reference documents of this feature.

## [6.6 MPLS TE Reliability](#)

## [6.7 Configuring the MPLS Service](#)

This topic describes the MPLS technology and how to configure the MPLS service on the MA5800.

## 6.1 Overview

Multi-protocol Label Switching (MPLS) is between the data link layer and the network layer in the TCP/IP protocol stack. The label in a short fixed length is used to encapsulate IP packets. On the data plane, fast label forwarding is implemented. On the control plane, MPLS can meet the requirements on the

network from various new applications with the help of the powerful and flexible routing functions of the IP network.

The MPLS feature includes the following sub features:

- **Basic MPLS functions**  
Basic MPLS functions provide a basis for other MPLS sub features. MPLS, which is not restricted by any specific link layer protocol, can use any Layer 2 medium to transmit network packets. This shows that MPLS is not a service or application, but a tunnel technology. This technology can support multiple higher-layer protocols and services, and ensure the security of information transmission at the same time.
- **MPLS RSVP-TE**  
To deploy engineered traffic on a large-scale backbone network, a simple solution with good expansibility must be adopted. MPLS, as a stacking model, can easily establish a virtual topology over a physical network and map traffic to this topology. Therefore, a technology that integrates MPLS with traffic engineering, namely, MPLS-TE is generated.
- **MPLS OAM**  
MPLS, as the key bearer technology for the extensible network-generation network, provides multiple services with QoS guarantee. In addition, MPLS introduces a unique network layer and therefore the faults caused by this new network layer may occur. Therefore, an MPLS network must have the OAM capability.

The MPLS feature supports the following functions:

- Functioning as a P device
- Capability of 100 pps for processing LDP and RSVP packets when functioning as a P device
- MPLS label switching
- Penultimate hop popping (PHP)
- Query of LSP packet statistics by label

## 6.2 MPLS Reference Standards and Protocols

The following lists the reference standards and protocols of this feature:

1. **PWE3**
  - RFC3985: Pseudo Wire Emulation Edge-to-Edge (PWE3) Architecture
  - RFC4447: Pseudowire Setup and Maintenance Using the Label Distribution Protocol (LDP)
  - RFC3916: Requirements for Pseudo-Wire Emulation Edge-to-Edge (PWE3)
  - RFC4446: IANA Allocations for Pseudowire Edge to Edge Emulation (PWE3)
  - RFC4717: Encapsulation Methods for Transport of Asynchronous Transfer Mode (ATM) over MPLS Networks
  - RFC4448: Encapsulation Methods for Transport of Ethernet over MPLS Networks

- RFC5085: Pseudowire Virtual Circuit Connectivity Verification (VCCV): A Control Channel for Pseudowires
  - RFC4553: Structure-Agnostic Time Division Multiplexing (TDM) over Packet (SAToP)
  - RFC5462: Multiprotocol Label Switching (MPLS) Label Stack Entry: EXP Field Renamed to Traffic Class Field
  - RFC4385: Pseudowire Emulation Edge-to-Edge (PWE3) Control Word for Use over an MPLS PSN
  - RFC6870: Pseudowire Preferential Forwarding Status Bit
2. RSVP
- RFC2205: Resource ReSerVation Protocol (RSVP) -- Version 1 Functional Specification
  - RFC3209: RSVP-TE: Extensions to RSVP for LSP Tunnels
  - RFC2210: The Use of RSVP with IETF Integrated Services
  - RFC2961: RSVP Refresh Overhead Reduction Extensions
  - RFC3270: Multi-Protocol Label Switching (MPLS) Support of Differentiated Services
  - RFC4090: Fast Reroute Extensions to RSVP-TE for LSP Tunnels
3. LDP
- RFC3031: Multiprotocol Label Switching Architecture
  - RFC5036: LDP Specification
  - RFC3215: LDP State Machine
  - RFC3478: Graceful Restart Mechanism for Label Distribution Protocol
  - RFC3815: Definitions of Managed Objects for the Multiprotocol Label Switching (MPLS), Label Distribution Protocol (LDP)
4. MPLS
- draft-ietf-mpls-lsp-ping-version-06
  - RFC4379: Detecting Multi-Protocol Label Switched (MPLS) Data Plane Failures
  - RFC3032: MPLS Label Stack Encoding
  - RFC3469: Framework for Multi-Protocol Label Switching (MPLS)-based Recovery
  - RFC3812: Multiprotocol Label Switching (MPLS) Traffic Engineering (TE) Management Information Base (MIB)
  - RFC3813: Multiprotocol Label Switching (MPLS) Label Switching Router (LSR) Management Information Base (MIB)
  - RFC3814: Multiprotocol Label Switching (MPLS) Forwarding Equivalence Class To Next Hop Label Forwarding Entry (FEC-To-NHLFE) Management Information Base (MIB)
  - Y.1710: Requirements for OAM functionality for MPLS networks
  - Y.1711: OAM mechanisms for MPLS networks
  - Y.1720: Protection switching for MPLS networks

## 6.3 MPLS Overview

Multiprotocol Label Switching (MPLS) was introduced to improve the forwarding speed. However, because of its excellent performance in traffic engineering (TE) and virtual private network (VPN), which are the two critical technologies, MPLS is becoming an important standard for extending the IP network. This topic provides the introduction, availability, principle, and reference of the MPLS feature.

### 6.3.1 Introduction

#### Definition

Basic MPLS features mainly refer to the MPLS Label Distribution Protocol (LDP) and LSP management function.

The LDP protocol is a standard MPLS label distribution protocol defined by the IETF. LDP, which is mainly used to allocate labels for the negotiation between LSRs to set up label switching paths (LSPs), regulates various types of information for the label distribution process, and the related processing. The LSRs form an LSP that crosses the entire MPLS domain according to the local forwarding table, which correlates in the label, network hop node, and out label of each specific FEC.

With the LSP management function, the MA5800 can manage and maintain the LSPs generated by various LDPs and can issue the hardware forwarding module.

#### Purpose

MPLS is initially put forth to improve the forwarding speed of routers. Compared with the traditional IP routing mode, during data forwarding, MPLS analyzes the IP packet header only on the edge of the network, but does not analyze the IP packet header at each hop. This saves the processing time.

With the development of the ASIC technology, the route search speed is not a bottleneck for network development. Thus, MPLS has not obvious advantages in forwarding speed. MPLS, however, is widely applied to the virtual private network (VPN), traffic engineering, and quality of service (QoS) due to its characteristics of supporting multi-layer labels and connected-oriented forwarding plane. Therefore, MPLS becomes an increasingly important standard for expanding the scale of the IP network.

### 6.3.2 Principle

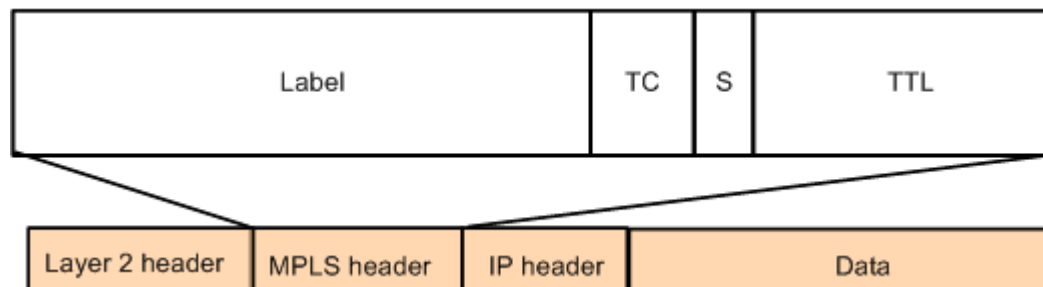
Multiprotocol label switching (MPLS) was introduced to improve the forwarding speed. However, because of its superb performance in traffic engineering (TE) and virtual private network (VPN), which are the two critical technologies in the current IP network, MPLS has become an important standard for extending the IP network.

IP technologies are connectionless at both the forwarding plane and control plane whereas ATM technologies are connection-oriented at the two planes. The MPLS technology combines the advantages of IP and ATM technologies and achieves a

connectionless control plane and a connection-oriented forwarding plane. Such a combination provides for flexible IP routing and convenient Layer 2 switching as well as expanded ATM service variety.

**Figure 6-1** shows the MPLS packet format.

**Figure 6-1** MPLS packet format



- Label: a 20-bit label value field, used as the forwarding pointer.
- TC: short for traffic class, a 3-bit field for QoS (note that this field was named EXP and is renamed TC in RFC5462).
- S: a 1-bit bottom of stack field. This bit set to 1 indicates the bottom label in the label stack.
- TTL: short for time to live, an 8-bit field, similar to the TTL field in an IP header.

## Basic MPLS Concepts

- Forwarding equivalence class (FEC)  
An FEC refers to a group of data streams which are forwarded in the same manner. These data streams are forwarded by the LSR in the same manner. Theoretically, FECs can be classified according to the IP address, service type, or QoS. For example, in the conventional IP forwarding by using the maximum matching algorithm, all the packets to the same route belong to an FEC. Currently, FECs are generally classified based on the address. The MA5800 supports only address-based FECs.
- Label  
A label is a short fixed length physically contiguous identifier which is used to identify an FEC, usually of local significance. In certain conditions, for example, when load sharing is required, one FEC may map multiple labels. On one device, however, one label can represent only one FEC.  
Label encapsulation is performed between the link layer and the network layer. Therefore, label can be supported by any link layer.
- Penultimate hop popping  
On the last hop node, the label no longer has any function. In this case, the label stack may be popped at the penultimate LSR of the LSP, rather than at the LSP Egress, to reduce the load of the last hop LSR. The last hop LSR directly forwards IP packets or next-layer labels, which are configured at the egress by the PHP.
- Label switching router (LSR)

An LSR, also called an MPLS node, is a network device which is capable of exchanging and forwarding MPLS labels. LSRs are the basic elements in an MPLS network. All LSRs support the MPLS protocol.

- Label edge router (LER)

An LSR on the edge of the MPLS domain is called the LER. If an LSR has a neighbor node that does not run the MPLS protocol, the LSR is an LER.

The LER is responsible for classifying the packets that enter the MPLS domain to FECs and adding labels to these FECs for forwarding in the MPLS domain. When the packets leave the MPLS domain, the FECs pop up the labels, resume the original packets, and then are forwarded accordingly.

- Label switched path (LSP)

The path that a packet in a particular FEC traverses in an MPLS network is called the LSP.

The LSP, similar to the ATM virtual circuit in function, is a unidirectional path from the ingress to the egress.

- Label distribution protocol (LDP)

LDP, also called the signaling protocol, is the MPLS control protocol. LDP is responsible for series of operations such as FEC classification, label distribution, and LSP establishment and maintenance.

MPLS can use multiple label distribution protocols, such as the Label Distribution Protocol (LDP) and Resource Reservation Protocol Traffic Engineering (RSVP-TE).

- LDP is a standard MPLS label distribution protocol defined by the IETF. LDP is responsible for FEC classification, label distribution, and LSP establishment and maintenance.
- RSVP-TE is an extension to RSVP and provides high QoS and TE capability for users by establishing TE LSPs.

- Label distribution mode

In an MPLS system, the downstream LSR determines the label to be advertised to a specific FEC, and then notifies the upstream LSR. That is, the label is specified by the downstream LSR, and is advertised from the downstream LSR to the upstream LSR.

The label advertisement modes on the upstream and downstream LSRs with label advertisement adjacencies must be the same. Otherwise, the LSP cannot be set up.

The two label advertisement modes are as follows:

- Downstream unsolicited (DU) mode  
In the DU mode, the LSR allocates labels to a specific FEC without asking for the label request message from upstream LSRs.
- Downstream on demand mode  
In the DoD mode, the LSR allocates labels to a specific FEC only after obtaining the label request message from upstream LSRs.

 **NOTE**

When a downstream LSR feeds back the label mapping information is determined by the label control mode used by the LSR.

- When an LSR supports the ordered label control mode, it sends the label mapping information to the upstream LSR only when it receives the label mapping message returned by the downstream LSR, or when it is the egress node of the FEC.
- When an LSR supports the independent label distribution control mode, it sends the label mapping message to the upstream LSR regardless of whether it receives the label mapping message returned by the downstream LSR.

- **Label distribution control mode**

The label distribution control mode is the mode used by the LSR to allocate labels during the establishment of LSPs.

The two label distribution control modes are as follows:

- **Independent label distribution control mode**

In the independent label distribution control mode, the local LSR can independently allocate a label to an FEC and binds the label to the FEC, and notify the upstream LSR of the label, without waiting for the label from the upstream LSR.

- **Ordered label control mode**

In the ordered label control mode, the LSR can send the label mapping message of an FEC to the upstream LSR only when the LSR has the label mapping message of the next hop of the FEC, or when the LSR is the egress node of the FEC.

- **Label retention mode**

The label retention mode is the mode adopted by the LSR to process the received label mapping messages that are not in use temporarily.

The two label retention modes are as follows:

- **Liberal retention mode**

If an LSR supports the liberal retention mode, it maintains the label mapping received from the neighbor LSR regardless of whether the neighbor LSR is its own next hop.

When the next hop neighbor changes due to the change of network topology, the LSR that supports the liberal retention mode can use the label sent from the non-next-hop neighbor to set up LSPs quickly. This, however, requires more memory and label space.

- **Conservative retention mode**

If an LSR supports the conservative retention mode, it maintains the label mapping received from the neighbor LSR only when the neighbor LSR is its next hop.

When the next hop neighbor changes due to the change of network topology, the LSR that supports the conservative retention mode can save memory and label space because the LSR maintains only the label from the next hop neighbor. The re-establishment of LSPs, however, lasts a long time.

**Figure 6-2** shows the protocol stack model for label distribution.

[illegible]

**Figure 6-3** shows the working principle of the MPLS feature

The diagram illustrates the MPLS network architecture. It features a central cloud-like shape representing the MPLS core, which contains several blue cylindrical nodes labeled 'R' (Routers). These are identified as 'MPLS core LSR'. On the left, an orange box labeled 'Ingress' is connected to the core. On the right, an orange box labeled 'Egress' is connected to the core. A path of arrows, labeled 'Label Switched Path (LSP)', starts at the Ingress node, passes through a series of core routers, and ends at the Egress node. The entire network is labeled 'Access Node' at the top. Below the core, the text 'MPLS Edge Router (LER)' is present.

1. First, enable MPLS and LDP on each router on the network, and enable LDP on the interconnected interfaces.
2. Consequently, LDP automatically sets up an LDP session between any two routers. The LDP packets are carried on this session.
3. LDP works with the traditional routing protocol such as OSPF and RIP to set LSPs in each LSR for the FEC with service requirements.

4. LDP does not need to be enabled for the establishment of static LSPs. Configure the FEC, and inbound and outbound labels on each MPLS router that the static LSP travels.

## LDP GR

The GR is a key technology for implementing the high availability (HA). The GR protocol collects the information about the protocol control plane from neighbors or remote peers but does not learn about the information about the control plane through the handshake and exchange of the protocol.

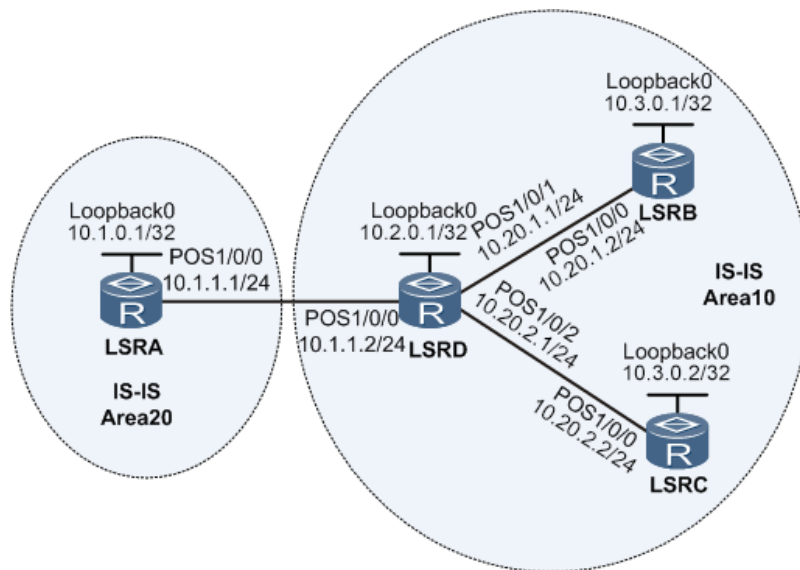
The LDP GR function ensures normal forwarding of the MPLS service during the active/standby switchover or upgrade of the system. In addition, the LDP GR function resumes the LDP session and completes the LSP establishment after the active/standby switchover or upgrade of the system

### NOTE

In actual application, to prevent services from being affected by the active control board failure, configure the system-level GR in the environment where both active and standby control boards are configured.

## LDP Extension for Inter-Area LSP

**Figure 6-4** Networking topology of LDP Extension for Inter-Area LSP



As shown in [Figure 6-4](#), there are two IGP areas, Area 10 and Area 20.

In the routing table of LSRD at the edge of Area 10, there are two host routes to LSRB and LSRC. Generally, to prevent a large number of routes from occupying too many resources, on LSRD, you can use IS-IS to aggregate the two routes to one route 10.3.0.0/24 and send this route to Area 20. Consequently, there is only one aggregated route (10.3.0.0/24) but not 32-bit host routes in the routing table of LSRA. By default, when establishing LSPs, LDP searches the routing table for the route that exactly matches the forwarding equivalence class (FEC) in the received Label Mapping message. [Table 6-1](#) shows routing entry information of LSRA and routing information carried in FEC in the situation as shown in [Figure 6-4](#).

**Table 6-1** Routing entry information of LSRA and routing information carried in FEC

| Routing entry information of LSRA | FEC         |
|-----------------------------------|-------------|
| 10.3.0.0/24                       | 10.3.0.1/32 |
|                                   | 10.3.0.2/32 |

LDP establishes liberal LSPs rather than inter-area LDP LSPs for aggregated routes. In this situation, LDP cannot provide required backbone network tunnels for VPN services.

Therefore, in the situation as shown in [Figure 6-4](#), you need to configure LDP to search for routes according to the longest match rule to establish LSPs. There is already an aggregated route 10.3.0.0/24 in the routing table of LSRA. When LSRA receives a Label Mapping message (such as the carried FEC is 10.3.0.1/32) from Area 10, LSRA searches for a route according to the longest match rule defined in RFC 5283. Then, LSRA finds information about the aggregated route 10.3.0.0/24, and uses the outbound interface and next hop of this route as those of the route 10.3.0.1/32. In this manner, LDP can establish inter-area LDP LSPs.

## 6.4 MPLS RSVP-TE

MPLS RSVP-TE is a technology which integrates TE and the MPLS superimposed model. It provides high quality of service (QoS) and TE capability for users by establishing LSPs based on TE. This topic provides introduction to this feature and describes the principle and reference documents of this feature.

### 6.4.1 Introduction

#### Definition

MPLS RSVP-TE is a technology that integrates TE with the MPLS technology. MPLS RSVP-TE establishes label switched path (LSP) tunnels along specified paths for resource reservation, enables network traffic to avoid the node where congestion occurs to balance network traffic.

To establish constraint-based LSPs in MPLS TE, RSVP is extended. The extended RSVP signaling protocol is called the RSVP-TE signaling protocol.

#### Purpose

To deploy engineered traffic on a large-scale backbone network, a simple solution with good expansibility must be adopted. MPLS, as a stacking model, can easily establish a virtual topology over a physical network and map traffic to this topology.

MPLS TE establishes the LSP tunnel along a specified path through RSVP-TE and reserves resources. Thus, carriers can accurately control the path that traffic

traverses to avoid the node where congestion occurs. This solves the problem that certain paths are overloaded and other paths are idle, utilizing the current bandwidth resources sufficiently. At the same time, MPLS TE can reserve resources during the establishment of LSP tunnels to ensure the QoS.

To ensure continuity of services, MPLS TE also introduces route backup to implement quick switching in case of link failure.

## 6.4.2 Principle

### Basic MPLS RSVP-TE Concepts

- CR-LSP

An LSP that is established based on certain constraints is called a constraint-based routed label switched path (CR-LSP). Different from a common LSP, the establishment of a CR-LSP depends on the routing information. In addition, some conditions must be met, for example, the specified bandwidth, the fixed route, and QoS parameters.

CR-LSPs can be classified into the following two categories:

- Static CR-LSP

The forwarding information and resources information about a static CR-LSP are configured manually and the signaling protocol and route calculation are not involved. Less resource is occupied because the MPLS control packets do not need to be exchanged. The static CR-LSP, however, is seldom applied because it cannot dynamically adjust according to the topology change of the network.

- Dynamic CR-LSP

A dynamic CR-LSP is established and maintained through the signaling mechanism, and route calculation is required.

- RSVP

Resource Reservation Protocol (RSVP) is designed for the integrated service model and is used to reserve resources on each node on a path. RSVP works on the transmission layer, but does not participate in the transmission of application data. RSVP, similar to ICMP, is a network control protocol.

- RSVP-TE

To establish the CR-LSP, RSVP is extended. The extended RSVP signaling protocol is called the RSVP-TE signaling protocol.

- Explicit route

A CR-LSP that is established along a specified path is called an explicit route. The two types of explicit route are as follows:

- Strict explicit route

On a strict explicit route, the next hop node must be directly connected to its preceding hop node. The route of the LSP can be precisely controlled by using the strict explicit route.

- Loose explicit route

The path between a loose node and its preceding node MAY include other network nodes that are not part of the strict node or its preceding abstract node.

 **NOTE**

The MPLS TE signaling can carry the strict or loose attributes of an explicit path, and establish a CR-LSP along a specified path.

## Composition of MPLS RSVP-TE

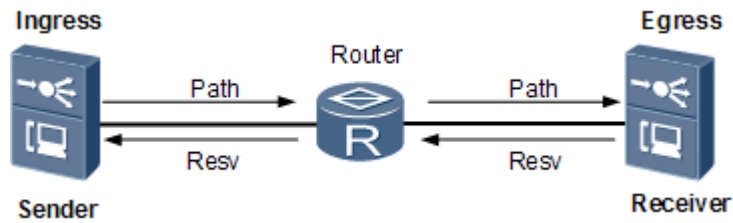
The following four components are necessary to the MPLS TE function:

- **Information advertisement component**  
In addition to the topology information about the network, TE also needs to know the load information about the network. Therefore, MPLS TE introduces the information advertisement component, that is, MPLS TE maintains the link attribute and topology attribute of the network on each node through IGP extensions to form the TE database (TEDB). The path that meets all types of constraints can be calculated by using the TEDB. The extended OSPF protocol adds certain TE-related attributes such as link bandwidth and color to the link connection status, where the maximum reservable bandwidth and unreserved bandwidth for the link with each priority are the most important.
- **Route selection component**  
After the information advertisement component forms the TEDB, the path that the LSP tunnel passes can be specified on each ingress node. This explicit path can be a strict or loose explicit path. In addition, the restraints such as the bandwidth can be specified.  
The route selection component calculates the path that meets the specified constraints by using the data in the TEDB through the constraint shortest path first (CSPF) algorithm.
- **Signaling component**  
After the shortest path from the ingress to the egress of the LSP is obtained, the TE tunnel, which is used to forward the traffic that enters the ingress of the LSP, needs to be established. This process is implemented by the signaling component.  
The MA5800 supports establishment of LSP tunnels through RSVP. The RSVP signaling can carry the constraint parameters such as the bandwidth of the LSP, certain explicit routes, and color.  
An LSP can also be established without the signaling protocol. That is, an LSP can be established through allocating labels manually hop by hop. An LSP established in this mode is called a static CR-LSP.
- **Packet forwarding component**  
The packet forwarding component of MPLS RSVP-TE is based on the label, that is, it forwards packets along the existing LSPs through labels. The defects of the IGP routing protocol can be avoided because the path of an LSP tunnel can be specified.

## Process of TE LSP Tunnel Establishment

The LSP established through RSVP-TE has the resource reservation capability, and certain resources of the LSR on the LSP can be allocated to the LSP. Thus, the services transmitted on the LSP can be guaranteed. [Figure 6-5](#) shows the process of TE LSP tunnel establishment.

**Figure 6-5** Process of TE LSP tunnel establishment



The process of TE LSP tunnel establishment is summarized as follows:

1. The ingress LSR generates the Path message and transmits it to the egress LSR.
2. After the egress LSR receives the Path message, the egress LSR generates the Resv message and transmits it to the ingress LSR. At the same time, the LSRs on the LSP reserves resources for the LSP through the Resv message.
3. When the ingress LSR receives the Resv message, it indicates that the LSP is successfully established.

## RSVP-TE GR

RSVP-TE graceful restart (GR) is a status recovery mechanism of RSVP-TE. When the control plane performs active/standby switchover, RSVP-TE GR can ensure the continuity of data transmission on the forwarding plane. At the same time, neighbor nodes help the GR node to recover in time.

RSVP-TE GR is based on the Hello mechanism of RSVP. The recovery of the local status depends on the upstream Path message or the downstream Recovery Path message.

RSVP GR has the following features: Shortening the information recovery of the control plane; reducing changes of temporary routes; ensuring the continuity of service forwarding on the forwarding plane.

## 6.5 MPLS OAM

MPLS OAM checks if an LSP is in the normal state through a mechanism, and reports the alarm information if the LSP fails. This topic provides introduction to this feature and describes the principle and reference documents of this feature.

### 6.5.1 Introduction

#### Definition

Operation Administration & Maintenance (OAM) has the following features:

- Simplifying network operations
- Checking the network performance anytime
- Reducing OPEX of the network

Deployment of an effective OAM mechanism is crucial to the running of the network, especially to the network with certain QoS requirements, namely, certain performance and usability requirements.

MPLS, as the key bearer technology for the extensible network generation network, provides multiple services with QoS guarantee. In addition, MPLS introduces a unique network layer and therefore there will be faults that are only relevant to this new network layer. Therefore, an MPLS network must have the OAM capability.

MPLS OAM provides both detection tools and mature protection switching mechanisms. In this way, MPLS can perform switching when a fault occurs on the MPLS layer. This minimizes the loss of data.

## Purpose

The MPLS OAM functions are as follows:

- Fault detection: Requirement-based query and continuous detection are provided to learn about anytime whether faults exist on the monitored LSP.
- Protection switching: After a fault occurs, it can be detected, analyzed, and located, and an alarm will be reported. In addition, the corresponding measures can be taken according to the fault type.

## 6.5.2 Principle

### Background Knowledge for MPLS OAM

1. MPLS OAM packets are classified as follows:

- Connectivity detection (CD) packets. The two types of CD packets are as follows:
  - Connectivity verification (CV)
  - Fast failure detection (FFD)
- Forward defect indication (FDI)
- Backward defect indication (BDI)

MPLS OAM is implemented by periodically transmitting detection packets CV or FFD over the detected LSPs.

2. Basic detection process

MPLS OAM is implemented by periodically transmitting detection packets CV and FFD over the detected LSPs.

- To detect the source by using the CV packet, a sliding window in the width of 3s is set on the source and the LSP status is checked by using the VC packet received in the sliding window.
- To detect the source by using the FFD packet, a sliding window in the width of three times of FFD transmit interval is set on the source and the LSP status is checked by using the FFD packet received in the sliding window.

3. CV and FFD

The FFD and CV detection packets are mutually exclusive. That is, only the FFD or CV detection packets can be applied to one LSP at a time.

4. Backward path

BDI packets are transmitted through the backward path. The ingress of a backward path is the egress of the detected LSP, and the egress of the backward path is the ingress of the detected LSP. That is, each forward LSP has a backward path.

5. Protection switching (PS)

When a fault occurs on the network, currently MPLS OAM provides the PS, a type of end to end tunnel protection technology, to recover the interrupted services.

The PS uses one tunnel to protect another tunnel. There is no relationship among the attributes of each tunnel in the protect group. For example, the protection tunnel with 10 Mbit/s bandwidth can protect a master tunnel with a requirement for 100 Mbit/s bandwidth.

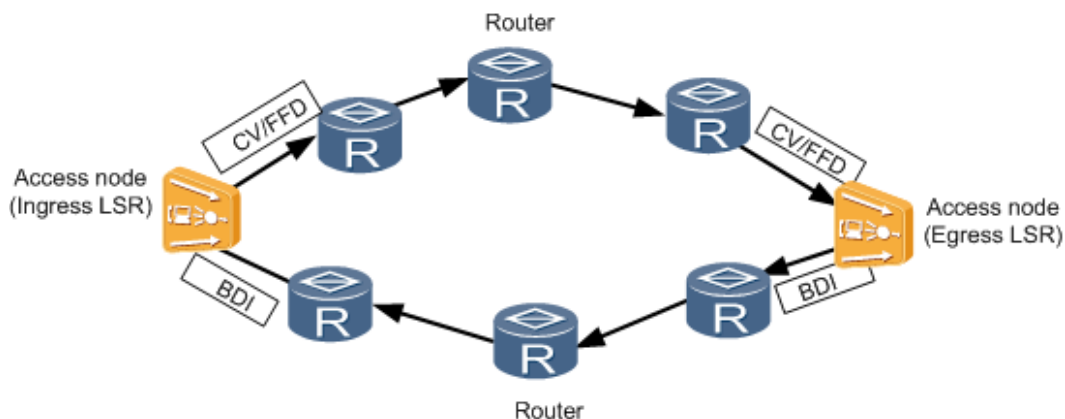
## MPLS OAM Detection Function

The basic process for MPLS OAM to detect the connectivity of a single LSP is as follows:

- The source transmits the CV/FFD packets to the destination through the detected LSP.
- The destination checks the correctness of the type and frequency information carried in the received detection packets and measures the number of correct and incorrect packets that are received within the detection period to monitor the connectivity of the LSP in real time.
- When the LSP fails, the destination detects the defect quickly and analyzes the defect type.

Bind a backward LSP to the detected LSP when configuring the OAM function for the detected LSP. A backward path is an LSP that has the opposite source and destination of the detected LSP, or a non-MPLS path that can be connected to the source and destination of the detected LSP.

After the destination detects a defect, the destination transmits the BDI packets that carry the defect information to the source through the backward path. The source learns about the status of the defect, and triggers the corresponding protection switching when the protect group is correctly configured. [Figure 6-6](#) shows the MPLS OAM CD.

**Figure 6-6 MPLS OAM CD**

## Working Modes of the MPLS OAM Protection Switching

The MPLS OAM protection switching aims at the entire LSP instead of one section or one node on the LSP. The route and bandwidth of the standby LSP for a specified active LSP are reserved.

Therefore, the protection switching is a thorough-assignment protection mechanism. To ensure that protection switching can be implemented effectively in all the possible cases that the active LSP fails, the standby LSP needs to use a physical path totally different from that of the active LSP.

The working mode of MPLS OAM protection switching is 1:1 protection mode. In this mode, each active LSP has a standby LSP.

- In normal conditions, data is transmitted through the active LSP and no traffic is transmitted through the standby LSP.
- When the destination detects a failure on the active LSP through the detection mechanism, the destination switches to the standby LSP, and then transmits the BDI packet to the source through the backward path, instructing the ingress to switch the traffic on the active LSP to the standby LSP. Thus, 1:1 protection switching is implemented.

## 6.6 MPLS TE Reliability

MPLS TE tunnels that transmit mission-critical services require high reliability. Access node supports the following network-level reliability.

- RSVP-TE FRR
- TE tunnel protection group
- CR-LSP backup

### 6.6.1 RSVP-TE FRR

RSVP-TE FRR is also called MPLS fast reroute. RSVP literally means the resource reservation protocol, TE means traffic engineering, and FRR means fast reroute.

## 6.6.1.1 Introduction

### Definition

The RSVP-TE FRR technology is applied to the MPLS TE network for implementing partial network protection. Specifically, when a certain link or node in the network fails, the LSP configured with FRR can automatically switch the data to the protection link.

To ensure the reliability of the MPLS network, the MPLS FRR technology is combined with the MPLS TE technology to provide LSPs with fast switching. In the MPLS FRR, a local backup path is created beforehand to protect the LSP from the impact of the link or node failure. When a failure occurs, the device that detects the failure can quickly switch the service from the faulty link to the backup path, thus reducing data loss.

### Purpose

Quick response and prompt switching are the features of MPLS FRR. Such features ensure the smooth switching of service data and prevent service interruption. In addition, the head node of the LSP will look for a new path for establishing a new LSP and will switch the service to the new LSP. Before the new LSP is set up, the service data is forwarded through the protection path.

## 6.6.1.2 Principle

### MPLS TE FRR

The basic principle of MPLS TE FRR is to protect one or more LSPs by using an LSP that is created beforehand. The LSP that is created beforehand is called the FRR LSP (bypass LSP), and the LSP that is protected is called a primary LSP. The purpose of MPLS TE FRR is to bypass the faulty link or node through the bypass LSP to protect the primary LSP. Creating the bypass LSP and primary LSP requires the participation of all the components of the MPLS TE system.

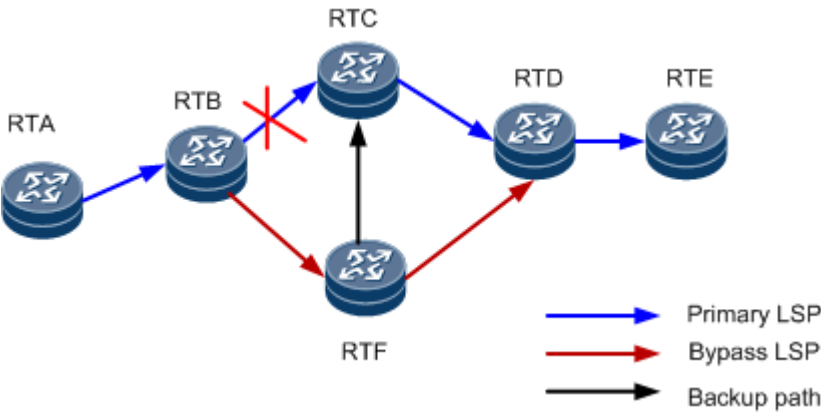
MPLS TE FRR is implemented based on RSVP TE and complies with RFC4090.

MPLS TE FRR can be implemented in the following two modes:

- Detour mode: This mode is also called the one-to-one backup mode. In this mode, one protection path is created to provide protection for each LSP. This protection path is called the detour LSP.
- Bypass mode: This mode is also called the facility backup mode. In this mode, one protection path provides protection for multiple LSPs. This protection path is called the bypass LSP.

The detour mode provides protection for each LSP, thus requiring more overheads. In the actual application, the bypass mode is more widely used. The MA5800 adopts the bypass mode. The following content of this topic mainly deals with the bypass mode. [Figure 6-7](#) illustrates the FRR function implemented in the bypass mode.

Figure 6-7 FRR in the bypass mode

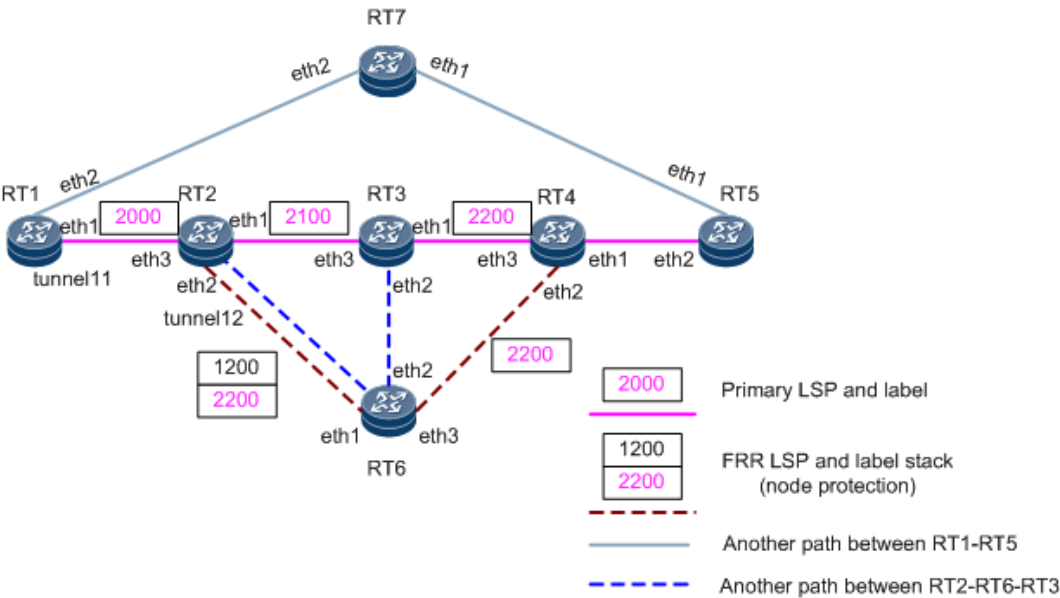


In [Figure 6-7](#), the blue path is the primary LSP and the red path is the bypass LSP. When the link between RTB and RTC fails or when RTC fails, the data on the primary LSP is switched to the bypass LSP. The top layer of the packet header sent from RTB adopts the label assigned to RTB by RTF, and the egress label of RTC is also added to the label stack as the lower layer. The packet on the RTB-RTF-RTD LSP carries two labels. After receiving the packet, RTD finds the label assigned to RTF by RTD, and continues to use the label assigned to RTC by RTD for forwarding the packet.

Implementation Process of FRR in the Bypass Mode

[Figure 6-8](#) illustrates the implementation process of FRR in the bypass mode.

Figure 6-8 FRR in the bypass mode



- Creating the primary LSP

The primary LSP is created in the same way as an ordinary LSP is. The head node (RT1) sends the RSVP PATH message to downstream nodes one by one (RT1-RT2-RT3-RT4-RT5), and the end node (RT5) sends the RESV message to upstream nodes one by one. When processing the RESV message, each node assigns the label and reserves the resources for creating the LSP.

In the protocol draft, some flag bits in the SESSION\_ATTRIBUTES and RECORD\_ROUTE objects are extended for FRR. The difference between the creating processes of the protected LSP and ordinary LSP lies in the processing of these flag bits. The flag bits added to the SESSION\_ATTRIBUTES object in the PATH message indicate whether the LSP needs partial protection, whether the label is recorded, and whether the bandwidth is protected.

The flag bits added to the RECORD\_ROUTE object in the RESV message indicate whether the LSP is protected, whether the switching is enabled, whether the bandwidth is protected, and whether the node is protected.

The creating of the primary LSP is triggered through the manual configuration of a tunnel on the head node (RT1). Before the primary LSP is created, if the FRR attribute is specified for the LSP by a command, the partial protection flag will be added to and the label flag and the SE style flag will be recorded in the SESSION\_ATTRIBUTES object in the RSVP PATH message. If bandwidth is also specified for the LSP, the RSVP will also add the bandwidth protection flag. After receiving the PATH message, through the local protection flag, the downstream node can determine that the LSP requires the FRR protection.

For the LSP that requires the FRR protection (determined according to the flag in the PATH message received), each node records the egress, LSR ID, and label of the RESV message in the RRO when sending the RESV message to the upstream node. Such information is passed on to each upstream node.

When receiving the RESV message for the first time, according to the information recorded in the RRO, each node selects a proper bypass LSP for the LSP to be protected (primary LSP). The process of selecting a proper bypass LSP for the primary LSP is called binding.

After the node performs the FRR binding calculation on the primary LSP, the node indicates whether the primary LSP has been protected in the RECORD\_ROUTE object in the RESV message sent to the upstream node. If the primary LSP has been protected, the egress (eth1 of RT2) of the protected LSP and the egress (eth3 of RT2) of the RESV message are recorded. If the primary LSP is not protected, the corresponding flag bit in the RRO is reset, and only the egress (eth3 of RT2) of the RESV message is recorded. Binding calculation is not performed on the egress. All the flag bits in the RRO sent from the egress to the upstream node are reset.

The primary LSP requiring the FRR protection is created in a similar way to an ordinary LSP. The differences are that, in the creating process of the primary LSP, the binding calculation is added, and related flag bits and sub-objects are added to the PATH and RESV messages.

- Creating the bypass LSP

A bypass LSP can be created in two modes: the manual mode and the automatic mode.

In the manual mode, after a tunnel without the FRR attribute is specified for protecting a physical interface, the LSP corresponding to this tunnel becomes a bypass LSP. A manual bypass LSP (tunnel12 on RT2) is configured manually on the PLR (RT2). The configuration of a manual bypass LSP is similar to an

ordinary LSP. The difference is that the bypass LSP cannot be configured with the FRR attribute. In other words, a bypass LSP cannot be a primary LSP at the same time. An LSP cannot be protected by itself.

The automatic mode of the bypass LSP simplifies the configuration of the manual mode. In the automatic mode, when the primary LSP requires the FRR protection, the PLR can select or automatically create a bypass LSP for protecting this primary LSP. A bypass LSP can protect multiple primary LSPs in so far as it meets the requirements of these primary LSPs.

A bypass LSP can protect multiple physical interfaces, but it cannot protect its own egress.

FRR can implement link protection or node protection. In the configuration of the bypass LSP, the links or nodes to be protected should be planned, and whether the link protection mode or node protection mode is to be adopted should be determined. Generally, node protection is a superior mode because it can protect the protected nodes and the links between the PLR and the protected nodes. If conditions permit, the customer tends to require node protection. Huawei device provides flexible protection modes. When node protection fails, the protection mode supported by Huawei device can automatically shift to link protection. When node protection becomes valid again, node protection will be adopted.

The bandwidth of the bypass tunnel is generally used for protecting the primary LSP. All the resources of the bypass tunnel are used only after the switching occurs. Make sure that the configured bandwidth of the bypass LSP is greater than or equal to the sum of the bandwidth required by all the protected LSPs. Otherwise, after FRR takes effect, the bypass LSP will fail to provide the protection that meets the service quality requirements.

A bypass LSP is generally in the idle state and does not carry data. If the bypass tunnel is required to forward data as well as protecting the primary LSP, sufficient bandwidth should be configured.

- Binding calculation

Binding can refer to specifying a bypass tunnel for protecting a physical interface. Then, the bypass tunnel can be said to be bound to the physical interface.

Binding can also refer to selecting a proper bypass LSP for protecting a primary LSP. Then, the primary LSP can be said to be bound to the bypass LSP. The binding calculation is a process of binding a primary LSP to the bypass LSP. The result derived from the binding calculation is the necessary data to be forwarded in the switching, such as the interface of the bypass tunnel, the egress and NHLFE of the bypass LSP, and the label assigned by the MP. If the binding calculation is successful, the node sends the RESV message to inform the upstream node that the primary LSP has been protected.

The binding calculation must be completed before the switching occurs. In the following conditions, binding calculation is triggered:

- When a primary LSP is created
- When the system periodically calculates the binding relations of all the LSPs whose egress is the protected physical interface

The binding calculation always uses the known information of a primary LSP to traverse the bypass LSPs on the egress through which the primary LSP is protected, thus to find a most suitable bypass LSP. If automatic bypass LSP is

supported, when a suitable bypass LSP is not found, the system will automatically try to create a bypass LSP for protecting the primary LSP.

When the primary LSP is created, the interface address of each node is recorded. The CSPF can obtain the corresponding LSR ID according to the interface address. Hence, the LSR ID of the next hop (NHP) or next next hop (NNHOP) of the primary LSP is known. When the primary LSP is created, the RRO records the LSR ID of each hop. If the egress LSR ID and the NHP LSR ID of a bypass LSP are the same, link protection can be realized; if the egress LSR ID and NNHOP LSR ID of a bypass LSP are the same, node protection can be realized.

If the bandwidth of a primary LSP is 0, it can be protected only by a bypass LSP whose bandwidth is 0. After a primary LSP comes into the protection of a bypass LSP whose bandwidth is 0, the protection count of this bypass LSP is plus 1. If the bandwidth of a primary LSP is not 0, it can be protected only by a bypass LSP with sufficient remaining bandwidth. The initial remaining bandwidth of a bypass LSP whose bandwidth is not 0 is the configured value. Each time a primary LSP comes into the protection of the bypass LSP, the remaining bandwidth of the bypass LSP is minus the bandwidth of the primary LSP.

When multiple bypass LSPs are available for protecting a primary LSP, the following priority is adopted:

- Node protection is prior to link protection.
- If the bandwidth of the primary LSP is 0, a bypass LSP whose bandwidth is 0 is selected. If the bandwidth of the primary LSP is not 0, the bypass LSP whose remaining bandwidth is greater than or equal to the bandwidth of the primary LSP is selected.

The result derived from the binding calculation contains the following items, which are used for sending the data and signaling message from the bypass tunnel after the switching.

- Protection type (link protection or node protection), and the LSR ID of the MP.
- The label assigned to the last hop by the MP. This label is the label corresponding to the MP LSR ID in the RRO of the primary LSP.
- Egress and NHLFE of the bypass tunnel.

The binding calculation result is saved and can be immediately used when partial failure occurs. This is why MPLS TE FRR can respond quickly to failure.

- Failure detection

The purpose of failure detection is to detect the failure of a link (RT2-RT3) or a node (RT3) as soon as possible so that switching can be triggered to reduce packet loss. Failure detection does not specifically distinguish between a link and a node, and the result of failure detection is presented as "interface failure" (eth1 of RT2).

The "interface failure" triggers the FRR switching on all the LSPs that use the interface as the egress. If an LSP has been determined by the binding calculation to be in the link protection, the LSP will switch to link protection. If the actual failure is a node failure, the switching fails. As a result, the LSP is deleted. If an LSP has been determined by the binding calculation to be in the node protection, the LSP will switch to node protection. If the actual failure is a link failure and even if the next hop is available, the next hop will be skipped by the bypass tunnel.

Certain link or node failures can be detected by the link layer protocol. The detection speed of the link layer protocol is directly related to the interface type. Other link or node failures are detected through the hello mechanism of the RESV. The detection speed of the hello mechanism is relatively slow.

The hello function can be enabled on each physical interface that needs protection and on its interconnected interface. Then, the hello message and the response will be sent between the two routers periodically. In case of a link or node failure, the hello message or the response is lost. When the messages are lost for three successive times, it is regarded that a failure occurs.

- Switching

Switching refers to adopting the bypass LSP for sending the data and RSVP messages that used to be sent through the primary LSP. When the interface (eth1 of RT2) is shut down by a command or when "interface failure" (of eth1 of RT2) is detected through the failure detection mechanism, switching is triggered. In the switching, the data and signaling of the protected LSPs on the faulty interface are switched to the bypass LSP for sending, and the upstream node is informed that switching occurs.

Switching first occurs on the forwarding components. During the binding calculation by the forwarding component involved in the switching, the inner label (2200) required for the forwarding has been saved in the NHLFE. Now, it only needs to indicate that the LSP has been switched, and the data can be forwarded through the bypass tunnel.

Then, the node will respond to the switching event through the RESV message. For the LSP that has been bound to the bypass LSP, the node sends the upstream node the RSVP PathError message with the switching flag bit. The bypass tunnel is mainly used for temporary protection. The head node will properly process the LSPs that have been switched. If an LSP is not bound to the bypass LSP, the node directly sends the RSVP ResvTear message to inform the upstream node to delete the LSP.

- Maintenance of the LSP after the switching

After the switching, the original link is not available. To prevent the LSP from being deleted after timeout, the information between the PLR (RT2) and the MP (RT4) needs to be refreshed through RSVP messages.

After being modified, the PATH message is sent to the MP through the bypass tunnel (Tunnel12 of RT2). After receiving the PATH message, the MP confirms itself as an MP. Then, the RESV message is modified and forwarded to the PLR through the IP addresses of multicast hops (RT4-RT6-RT2).

After the switching, the message sent from the PLR to the upstream node is also changed. That is, the address of the egress (eth2 of RT2) of the bypass LSP is added to the RRO.

After the switching, the sending path of the PTEAR, RERR, RTEAR and PERR messages of the primary LSP are changed accordingly.

After the switching in node protection, the protected node (RT3) may send the PATHTEAR message to the downstream node because the PATH message times out. In this case, the MP (RT4) ignores this message. In addition, in the switching, the MP sends the ResvTear message from the ingress (eth3 of RT4) of the original LSP. Thus, the protected node (RT3) will release the corresponding resource as soon as possible.

- Re-optimization

Re-optimization refers to calculating the path for a created LSP at the preset intervals. According to the calculated path, the router initiates the creating of a new LSP. After the new LSP is created, the original LSP is deleted, and the data of the original LSP tunnel is switched to the new LSP for forwarding.

Re-optimization can be configured for each LSP tunnel. After the LSP is created, re-optimization is enabled.

In the case of FRR, another function of re-optimization is to restore the tunnel (Tunnel1 of RT1) protected by the bypass LSP to the normal state. This is because the FRR protection is temporary. Therefore, a tunnel with the FRR attribute is generally configured with re-optimization. When the primary LSP has not switched, a new LSP is created only when the path calculated through re-optimization is different from the original path. When the primary LSP has switched, a new LSP is created even when the path calculated through re-optimization is the same as the original path.

A bypass LSP that has been bound to a physical interface can also be re-optimized. The bypass LSP, however, cannot be re-optimized if a primary LSP already switches to this bypass LSP. After a bypass LSP is re-optimized, the binding relations between the bypass LSP and the primary LSPs are refreshed.

Before the primary LSP is switched, the data forwarding is the same as that of an ordinary LSP; after the primary LSP is switched to the bypass tunnel, the data is forwarded through the bypass tunnel to the MP.

When the primary LSP is successfully bound to the bypass LSP, the NHLFE entry and the inner label (2200, the label assigned to the last upstream node by the MP) of the bypass LSP are recorded in the NHLFE entry of the primary LSP. In the switching, the forwarding component sets the switching flag bit in the NHLFE entry of the primary LSP.

When the packet arrives at the PLR, the forwarding component searches for the NHLFE entry to the primary LSP. If switching has not occurred, the component performs label switching and data forwarding; if the switching flag bit is found in the NHLFE entry, the component continues searching for the NHLFE entry to the corresponding bypass LSP. After finding the NHLFE entry, the component adds inner label 2200 to the label stack, and performs forwarding according to the information of the NHLFE entry of the bypass LSP.

At the egress of the bypass tunnel (or at the last but one hop), inner label 2200 is removed from the label stack, and then MP can perform forwarding by using the original label 2200. The inner label may be used on different interfaces of the MP. Therefore, the MP must assign a label to each platform.

As previously mentioned, certain failures are detected at the link layer. After a failure is detected at the link layer, the forwarding component can reset the switching flag bit in the NHLFE entry of the primary LSP if the failure recovers before a corresponding failure occurs at the upper layer. Hence, the data of the primary LSP is still forwarded through the original path, and the switching flag in the RESV message is not processed.

One thing should be noted that, after the switching, the RSVP message from the PLR to the MP is sent through the bypass tunnel. In other words, the message is forwarded as a common IP packet through the MPLS tunnel. The RSVP message from the MP to the PLR is forwarded as a common IP packet.

## 6.6.2 TE Tunnel Protection Group

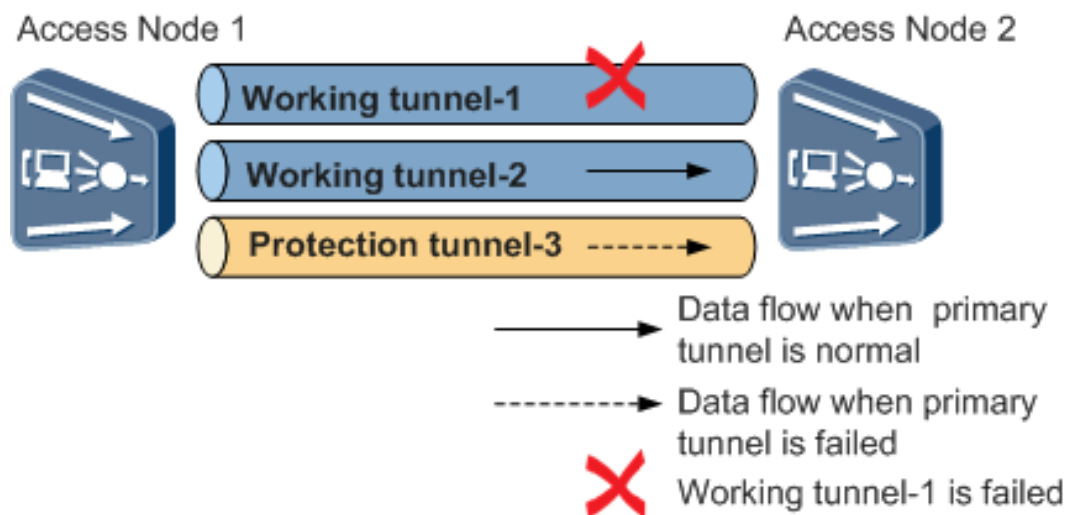
A tunnel protection group protects end-to-end MPLS TE tunnels. If a working tunnel in a protection group fails, traffic switches to a protection tunnel, minimizing traffic interruptions.

### 6.6.2.1 Related Concepts

As shown in the [Figure 6-9](#), concepts related to a tunnel protection group are as follows:

- Working tunnel: a tunnel to be protected.
- Protection tunnel: a tunnel that protects a working tunnel.
- Protection switchover: switches traffic from a faulty working tunnel to a protection tunnel in a tunnel protection group, which improves network reliability.

**Figure 6-9** Tunnel protection group



Primary tunnel-1 and tunnel-2, and the bypass tunnel-3 are established on the ingress Access Node shown in the [Figure 6-9](#).

Tunnel-3 is specified as a protection tunnel for primary tunnels tunnel-1 and tunnel-2 on Access Node. If the configured fault detection mechanism on the ingress detects a fault in tunnel-1, traffic switches to tunnel-3. Access Node attempts to reestablish tunnel-1. If tunnel-1 is successfully established, traffic switches back to the primary tunnel.

### 6.6.2.2 Principle

#### Implementation

A TE tunnel protection group uses a configured protection tunnel to protect traffic on the working tunnel to improve tunnel reliability. To ensure the improved

performance of the protection tunnel, the protection tunnel must exclude links and nodes through which the working tunnel passes during network planning.

**Table 6-2** shows the implementation procedure of a tunnel protection group.

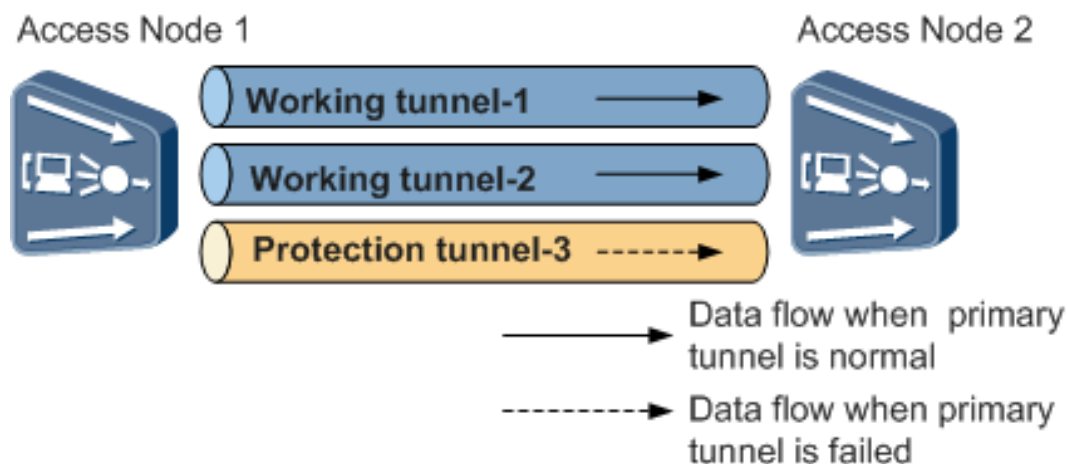
**Table 6-2** Implementation procedure of a tunnel protection group

| Sequence Number | Process                                            | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|-----------------|----------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1               | Establishment                                      | <p>The working and protection tunnels must have the same ingress and destination address. The protection tunnel is established in the same procedure as a regular tunnel. The protection tunnel can use attributes that differ from those for the working tunnel. Ensure that the working and protection tunnels are established over different paths as much as possible.</p> <p><b>NOTE</b></p> <ul style="list-style-type: none"><li>• A protection tunnel cannot be protected or enabled with TE FRR.</li><li>• Attributes for a protection tunnel can be configured independently of those for the working tunnel, which facilitates the network planning.</li></ul> |
| 2               | Binding between the working and protection tunnels | <p>The protection tunnel is bound to the tunnel ID of the working tunnel so that the two tunnels form a tunnel protection group.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| 3               | Fault detection                                    | <p>In addition to MPLS TE's own detection mechanism, MPLS OAM and BFD for CR-LSP are used to detect faults in a tunnel protection group to speed up protection switching.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| 4               | Protection switching                               | <p>The tunnel protection group supports either of the following protection switching modes:</p> <ul style="list-style-type: none"><li>• Manual switching: Traffic is forcibly switched to the protection tunnel.</li><li>• Automatic switching: Traffic automatically switches to the protection tunnel if the working tunnel fails.</li></ul> <p>A time interval can be set for automatic switching.</p>                                                                                                                                                                                                                                                                 |
| 5               | Switchback                                         | <p>After a traffic switchover is implemented, the ingress attempts to reestablish the working tunnel. If the working tunnel is reestablished, the ingress can switch traffic back to the working tunnel or still forward traffic over the protection tunnel.</p>                                                                                                                                                                                                                                                                                                                                                                                                          |

## Protection mode

A tunnel protection group works in either 1:1 or N:1 mode. The 1:1 mode enables a protection tunnel to protect only a single working tunnel. The N:1 mode enables a protection tunnel to protect more than one working tunnel. The following figure shows the N:1 protection mode.

**Figure 6-10** N:1 protection mode



## Differences Between CR-LSP Backup and a Tunnel Protection Group

CR-LSP backup and a tunnel protection group are both E2E protection mechanisms for MPLS TE. [Table 6-3](#) shows the comparison between these two mechanisms.

**Table 6-3** Comparison between CR-LSP backup and a tunnel protection group

| Item                   | CR-LSP Backup                                                                                                                  | Tunnel Protection Group                                                        |
|------------------------|--------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------|
| Object to be protected | Primary and backup CR-LSPs are established on the same tunnel interface. A backup CR-LSP protects traffic on a primary CR-LSP. | One tunnel protects traffic over another tunnel in a tunnel protection group.  |
| TE FRR                 | A primary CR-LSP supports TE FRR. A backup CR-LSP does not support TE FRR.                                                     | A working tunnel supports TE FRR. A protection tunnel does not support TE FRR. |

| Item            | CR-LSP Backup                                                                            | Tunnel Protection Group                                                                                                                                                                                                           |
|-----------------|------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| LSP attributes  | Primary and backup CR-LSPs have the same attributes, except for the TE FRR attribute.    | The attributes of one tunnel in a tunnel protection group are independent of the attributes of the other tunnel. For example, a protection tunnel with no bandwidth can protect traffic on a working tunnel that has a bandwidth. |
| Protection mode | A 1:1 protection mode is supported. Each primary CR-LSP is protected by a backup CR-LSP. | An N:1 protection mode is supported. Many tunnels share one protection tunnel. If any protected tunnel fails, traffic switches to the protection tunnel.                                                                          |

## 6.6.3 CR-LSP Backup

CR-LSP backup techniques protect E2E MPLS TE tunnels. If the ingress detects that the primary CR-LSP is unavailable, the ingress switches traffic to a backup CR-LSP. After the primary CR-LSP recovers, traffic switches back.

### 6.6.3.1 Related Concepts

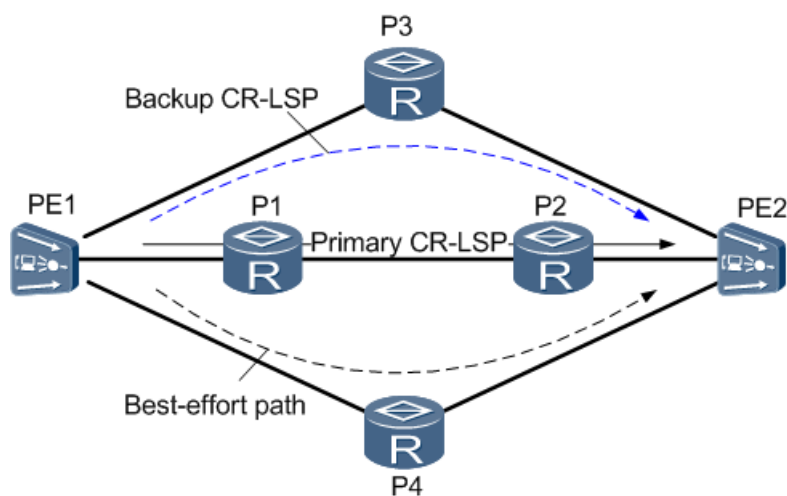
CR-LSP backup functions include hot standby, ordinary backup, and the best-effort path function. CR-LSP backup functions are as follows:

- Hot standby: A hot-standby CR-LSP is established immediately after a primary CR-LSP is created. If the primary CR-LSP fails, the hot-standby CR-LSP takes over traffic from the primary CR-LSP. After the primary CR-LSP recovers, traffic switches back.
- Ordinary backup: An ordinary backup CR-LSP can be established only after a primary CR-LSP fails. The ordinary backup CR-LSP takes over traffic if the primary CR-LSP fails. After the primary CR-LSP recovers, traffic switches back.

- Best-effort path

If both the primary and backup CR-LSPs fail, a best-effort path is established and takes over traffic.

For example, the primary CR-LSP is established over the path PE1 → P1 → P2 → PE2, and the backup CR-LSP is established over the path PE1 → P3 → PE2 shown in [Figure 6-11](#). If both CR-LSPs fail, PE1 establishes a best-effort path PE1 → P4 → PE2 to take over traffic.

**Figure 6-11** Best-effort path**NOTE**

A best-effort path has no bandwidth reserved for traffic, but has an affinity and a hop limit configured as needed.

### 6.6.3.2 Principle

#### Implementation

The procedure of CR-LSP backup is as follows:

1. CR-LSP backup is deployed.

Plan the paths, bandwidth values, and deployment modes. [Table 6-4](#) lists CR-LSP backup deployment items.

**Table 6-4** CR-LSP backup deployment

| Item                      | Hot Standby                                                                                                                                                                                                                                                                                                           | Ordinary Backup                                                                                                                                                                                                                        | Best-Effort Path                                                                                                                                                                 |
|---------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Path                      | Determine whether the primary and hot-standby CR-LSPs entirely or partially overlap. A hot-standby CR-LSP can be established over an explicit path.<br>A hot-standby CR-LSP supports the following attributes: <ul style="list-style-type: none"><li>• Explicit path</li><li>• Affinity</li><li>• Hop limit</li></ul> | Allowed to use the path of the primary CR-LSP in all scenarios.<br>An ordinary backup CR-LSP supports the following attributes: <ul style="list-style-type: none"><li>• Explicit path</li><li>• Affinity</li><li>• Hop limit</li></ul> | Automatically calculated by the ingress.<br>A best-effort path supports the following attributes: <ul style="list-style-type: none"><li>• Affinity</li><li>• Hop limit</li></ul> |
| Bandwidth                 | A hot-standby CR-LSP and a primary CR-LSP have the same bandwidth by default.                                                                                                                                                                                                                                         | An ordinary backup CR-LSP and a primary CR-LSP have the same bandwidth.                                                                                                                                                                | A best-effort path is only a protection path that does not have reserved bandwidth.                                                                                              |
| Configuration combination | A hot-standby CR-LSP can be used together with a best-effort path.                                                                                                                                                                                                                                                    | An ordinary CR-LSP can only be used alone.                                                                                                                                                                                             | –                                                                                                                                                                                |

2. Fault detection is implemented.

CR-LSP backup supports the RSVP-TE fault advertisement mechanism, who sends signaling packets to detect faults at a low speed.

3. A traffic switchover is implemented.

If a primary CR-LSP fails, the ingress attempts to switch traffic from the primary CR-LSP to a hot-standby CR-LSP. If the hot-standby CR-LSP is unavailable, the ingress attempts to switch traffic to an ordinary backup CR-LSP. If the ordinary backup CR-LSP is unavailable, the ingress attempts to switch traffic to a best-effort path.

4. A traffic switchback is implemented.

Traffic switches back to a path based on the available CR-LSPs. Traffic will switch first to the primary CR-LSP, which has the highest priority. If the primary CR-LSP is unavailable, traffic will switch to the hot-standby CR-LSP. The ordinary CR-LSP has the lowest priority.

## Overlapping Path for a Hot-standby CR-LSP

The overlapping path function can be configured for a hot-standby CR-LSP. The path of the hot-standby CR-LSP can overlap the path of a primary CR-LSP in all scenarios.

## Coexistence of CR-LSP Backup and TE FRR

1. CR-LSP backup functions can be used together with TE FRR.
  - Hot standby and TE FRR: If TE FRR detects a link fault, traffic switches to a TE FRR bypass CR-LSP and then to a hot-standby CR-LSP.
  - Ordinary backup and TE FRR: If TE FRR detects a link fault, traffic switches to a TE FRR bypass CR-LSP. If both the primary and TE FRR bypass CR-LSPs fail, an ordinary backup CR-LSP is established and takes over traffic.
2. CR-LSP backup can be associated with TE FRR.

The association improves tunnel security. The association provides the following functions based on backup modes:

- Association between an ordinary backup CR-LSP and a TE FRR bypass CR-LSP provides the following functions:

If a protected link or node fails, traffic switches to a bypass CR-LSP. The ingress attempts to reestablish the primary CR-LSP, while attempting to establish an ordinary backup CR-LSP.

If the ordinary backup CR-LSP is established successfully before the primary CR-LSP is restored, traffic switches to the ordinary backup CR-LSP.

After the primary CR-LSP recovers, traffic switches back to the primary CR-LSP.

If the ordinary backup CR-LSP fails to be established, and the primary CR-LSP does not recover, the traffic still passes through the bypass CR-LSP.

- Association between a hot-standby CR-LSP and a TE FRR bypass CR-LSP provides the following functions:

If a hot-standby CR-LSP is Up and a protected link or node fails, traffic switches to a TE FRR bypass CR-LSP and then immediately switches to the hot-standby CR-LSP. At the same time, the ingress attempts to restore the primary CR-LSP.

If the hot-standby CR-LSP is Down, the traffic switching procedure is the same as that when the ordinary backup is used.

Association between ordinary backup CR-LSPs and TE FRR is recommended. An ordinary backup CR-LSP without additional bandwidth needed is established only after the primary CR-LSP enters the FRR-in-use state. Although the primary CR-LSP is Up, the system attempts to establish a hot-standby CR-LSP with additional bandwidth needed.

## 6.7 Configuring the MPLS Service

This topic describes the MPLS technology and how to configure the MPLS service on the MA5800.

### Basic concept

- The path that an FEC traverses in an MPLS network is called LSP. The LSP, whose function is the same as the virtual circuit in ATM and frame relay, is a unidirectional path from the ingress to the egress. Each node on the LSP is an LSR.
- The static LSP is the label forwarding path manually set up for label distribution to each FEC.
- The dynamic LSP is the label forwarding path dynamically established through the label distribution protocol (LDP or RSVP-TE).

### Configuration logic

In the MPLS configuration, the core is to configure the LSP and the second is to configure fault detection and protection for the LSP. At the same time, According to the protocol for creating LSPs, LSPs are categorized as static LSP, LDP LSP, and RSVP-TE LSP.

Therefore, configure MPLS as follows:

1. Configure LSPs.
  - Configure a static LSP.
  - Configure an LDP LSP.
  - Configure an RSVP-TE LSP.
2. Configure LSP protection. Configure the MPLS OAM.

### 6.7.1 Configuring the Static LSP

Static LSP is configured manually. A static LSP can work in the normal state only when all the LSRs along the static LSP are configured.

### Prerequisites

1. The IP address of the loopback interface must be configured.
2. The LSR ID must be configured.
3. The global MPLS, VLAN MPLS, and VLAN interface MPLS must be enabled.
4. A static or dynamic route must be successfully configured on each device in the network (so that LSRs can reach each other through the IP route).

### Context

The administrator needs to manually distribute labels to each LSR when configuring the static lsp. Principle: The out label value of a node must be equal to the in label value of its next node. LSRs on a static LSP cannot perceive the entire LSP. Therefore, static LSP is a local concept.

The MA5800 can function as a label switching edge router (LER) or a label switching router (LSR). According to the position of the LER or LSR in a network, the configuration of the static LSP involves the ingress configuration, transit node configuration, and egress configuration.

An LSP corresponds to a unidirectional forwarding path. To ensure bidirectional communication of the MPLS service, two static LSPs are required. The two LSPs have opposite directions. Their ingress and egress are reverse. Their transit nodes can be the same or different according to the networking requirements, or even free of being configured.

## Procedure

- When the MA5800 functions as an LER, configure the static LSP as follows:
  - a. Run the **static-cr-lsp ingress** command to configure the ingress parameters of a static LSP.

An LER is generally located at the edge of an MPLS network. The PE or PTN device can be considered an LER.

Format:

```
static-cr-lsp ingress { tunnel-interface tunnel interface-number | tunnel-name } destination destination-address { nexthop next-hop-address | outgoing-interface interface-type interface-number } * out-label out-label [ bandwidth ct0 bandwidth ]
```

- You can create a static LSP by using the LSP name or the tunnel. To create a static LSP by using the tunnel, you must run the **interface tunnel** command to create a tunnel interface and then configure its attributes.
  - **destination** *ip-addr*: Indicates the destination IP address of the LSP, that is, the loopback interface IP address of the PE or PTN device.
  - **nexthop** *ip-addr*: Indicates the next hop IP address, that is, the VLAN interface IP address of the adjacent LSR.
  - **out-label** *out-label*: Indicates the out label value, which must be the same as the in label value of the downstream LSR.
- b. Run the **static-cr-lsp egress** command to configure the egress parameters of a static LSP.

Format:

```
static-lsp egress lsp-name incoming-interface vlanif vlanid in-label in-label [ lsrid ingress-lsr-id tunnel-id tunnel-id ]
```

- In the egress configuration of a static LSP, only a VLAN interface can be used as the ingress interface.
  - **in-label** *in-label*: Indicates the in label value of the egress, which must be the same as the out label value of the upstream LSR.
- c. Run the **display mpls static-cr-lsp** command to query the configuration of a static LSP.

- When the MA5800 functions as an LSR, configure the static LSP as follows:
  - a. Run the **static-cr-lsp transit** command to configure the transit node parameters of a static LSP.

An LSR is generally located in the middle of an MPLS network. The P device can be considered an LSR that forwards MPLS labels.

Format:

```
static-cr-lsp transit lsp-name incoming-interface interface-type interface-number in-label in-label { nexthop next-hop-address | outgoing-interface interface-type interface-number } * out-label out-label [ ingress-lsrid ingress-lsrid egress-lsrid egress-lsrid tunnel-id tunnel-id ] [ bandwidth [ ct0 ] bandwidth ] [ description description-text ]
```

- The ingress interface of the transit node on a static LSP can only be the VLAN interface, that is, the VLAN interface of the upstream egress.
- **in-label** *in-label*: Indicates the in label value of the transit node, which must be the same as the out label value of the upstream ingress.
- **nexthop** *next-hop-address*: Indicates the next hop IP address, that is, the VLAN interface IP address of the adjacent LSR.
- **out-label** *out-label*: Indicates the out label value of the transit node, which must be the same as the in label value of the downstream LSR.

---

**NOTICE**

Because the LSP is unidirectional, you must configure the transit node parameters twice with opposite directions to ensure bidirectional communication of the MPLS service.

---

- b. Run the **display mpls static-cr-lsp** command to query the configuration of a static LSP.

----End

## Example

When the MA5800 functions as an LER, to configure the ingress and egress of a static LSP, set the parameters as follows:

- Ingress node name of the static LSP: lsp1; egress name of the static LSP: lsp2
- IP address of local VLAN interface 100: 10.1.1.2/24
- Destination IP address of the LSP: 10.3.3.3/32
- Out label: 8200; in label: 8300
- Next hop IP address: 10.1.1.3

```
huawei(config)#static-cr-lsp ingress lsp1 destination 10.3.3.3 nexthop 10.1.1.3 out-label 8200  
huawei(config)#static-cr-lsp egress lsp2 incoming-interface vlanif 100 in-label 8300
```

```
huawei(config)#display mpls static-cr-lsp
{ <cr>|STRING<1-19>|exclude<K>|include<K>|verbose<K>||<K> };
```

Command:

```
display mpls static-lsp
TOTAL      :      2      STATIC LSP(S)
UP         :      0      STATIC LSP(S)
DOWN       :      2      STATIC LSP(S)
Name       FEC          I/O Label  I/O If      Status
lsp1       10.3.3.3      NULL/8200  -/-        Down
lsp2       -            8300/NULL  vlanif100/- Down
```

When the MA5800 functions as an LSR, to configure the transit node parameters of a static LSP, set the parameters as follows:

- LSP name of the transit node in the positive direction: lsp1; LSP name of the transit node in the negative direction: lsp2
- IP address of local VLAN interface 100: 10.1.1.2/24
- IP address of local VLAN interface 200: 10.2.2.2/24
- Out label in the positive direction: 8200; in label in the positive direction: 8300
- Out label in the negative direction: 8200; in label in the negative direction: 8300
- Next hop IP address in the positive direction: 10.2.2.3
- Next hop IP address in the negative direction: 10.1.1.3

```
huawei(config)#static-cr-lsp transit lsp1 incoming-interface vlanif 100 in-label 82 00 nexthop 10.2.2.3
out-label 8300
huawei(config)#static-lsp transit lsp2 incoming-interface vlanif 200 in-label 83 00 nexthop 10.1.1.2
out-label 8200
huawei(config)#display mpls static-cr-lsp
{ <cr>|STRING<1-19>|exclude<K>|include<K>|verbose<K>||<K> };
```

Command:

```
display mpls static-lsp
TOTAL      :      2      STATIC LSP(S)
UP         :      0      STATIC LSP(S)
DOWN       :      2      STATIC LSP(S)
Name       FEC          I/O Label  I/O If      Status
lsp1       -/-          8200/8300  vlanif100/- Down
lsp2       -/-          8300/8200  vlanif200/- Down
```

## 6.7.2 Configuring the LDP LSP

Set up an MPLS LDP session between LSRs along the LSP. After the MPLS LDP session is set up, the LDP LSP is automatically created.

### Prerequisites

1. The IP address of the loopback interface must be configured.
2. The LSR ID must be configured.
3. The VLAN for MPLS label forwarding must be created.
4. Global MPLS must be enabled.
5. A static or dynamic route must be successfully configured on each device in the network (so that LSRs can reach each other through the IP route).

### Context

- The MA5800 supports LDP and RSVP-TE, both of which generate dynamic LSPs.

- LDP is a standard MPLS label distribution protocol defined by IETF. LDP, which is mainly used to distribute labels for the negotiation between LSRs to set up label switching paths (LSPs), regulates various types of information for the label distribution process, and the related processing. The LSRs form an LSP that crosses the entire MPLS domain according to the local forwarding table, which correlates the in label, network hop node, and out label of each specific FEC.

## Procedure

### Step 1 Configure the MPLS LDP session.

The MPLS-LDP session is used for information exchange such as label mapping and release between LSRs. The MPLS-LDP session is classified into two types:

- Local LDP session: Two LSRs between which a session is set up are connected directly.
- Remote LDP session: Two LSRs between which a session is set up are not connected directly. Remote LDP sessions are mainly set up between nonadjacent LSRs. They can also be set up between adjacent LSRs.

#### NOTE

If local adjacency with the specified remote peer exists, remote adjacency cannot be set up; if remote adjacency exists and local adjacency is set up for the remote peer, the remote peer will be deleted. In other words, only one session can exist between two LSRs and a local LDP session takes priority over a remote LDP session.

- Configure the local LDP session.
  - a. In the global config mode, run the **mpls ldp** command to enable global MPLS LDP.
  - b. Run the **interface vlanif** command to enter the VLAN interface mode.
  - c. In the VLAN interface mode, run the **mpls** command to enable the MPLS function of the VLAN interface and run the **mpls ldp** command to enable the MPLS LDP function of the VLAN interface.

#### NOTE

The VLAN 1 is the system default VLAN. All the upstream ports have been added to this VLAN by default. Do not use this VLAN as the MPLS VLAN or enable the MPLS function on this VLAN.

- d. Run the **quit** command to quit the VLAN interface mode.
- Configure the remote LDP session.
    - a. In the global config mode, run the **mpls ldp** command to enable global MPLS LDP.
    - b. Run the **mpls ldp remote-peer** command to create an LDP remote peer and then enter the remote peer mode.
    - c. Run the **remote-ip** command to configure the IP address of the LDP remote peer.

#### NOTE

The IP address of the remote LDP peer should be the LSR ID of the remote LSR. When the LSR ID is used as the transmission address of a remote peer, two remote peers set up a TCP connection between them using the LSR ID as the transmission address.

- d. (Optional) Run the **mpls ldp advertisement** command to set the label distribution mode to DoD (downstream on demand) or DU (downstream unsolicited, default).

In a network with a large scale, it is recommended to set the mode to DoD to reduce unnecessary MPLS forwarding entries.

**Step 2** (Optional) Configure the LDP MTU signaling function.

Run the **mtu-signalling** command to enable the sending of the MTU type, length, and value (TLV). This enables the LDP to automatically calculate and negotiate the minimum MTU value for all ports on each LSP. In this way, the MPLS determines the size of the MPLS forwarding packet at the ingress according to the minimum MTU, thereby avoiding the forwarding failure on transit nodes caused by oversize packets at the ingress.

By default, the LDP MTU signaling is enabled.

**Step 3** (Optional) Configure the route trigger policy for setting up an LSP.

Run the **lsp-trigger host** command to configure the route trigger policy for setting up an LSP. The default route trigger policy is used to set up an LSP by triggering the LDP through the host address. To modify the default route trigger policy, run this command.

 **NOTE**

It is recommended that you configure the route trigger policy for setting up an LSP to host (default), that is, the host route triggers the LDP to set up an LSP. In this way, the setup of useless LSPs can be prevented.

**Step 4** (Optional) Configure the trigger policy set up by the transit LSP.

Run the **propagate mapping** command to filter certain routes received by the LDP by using the IP prefix table. Only the route that matches the specified IP prefix table is used by the local LDP for creating the transit LSP. By default, the LDP does not filter the received routes when creating the transit LSP.

**Step 5** Query the relevant information about the LDP LSP configuration.

- Run the **display mpls ldp lsp** command to query the relevant information about the created LDP LSP.
- Run the **display mpls ldp session** command to check whether the created remote MPLS LDP session is in the normal (operational) state.
- Run the **display mpls interface** command to check whether the MPLS interface is in the normal (up) state.

----End

## Example

To configure an LDP LSP between two adjacent LSRs by using VLAN interface 200 as the MPLS forwarding interface and using default values for other parameters, do as follows:

```
huawei(config)#mpls ldp
huawei(config-mpls-ldp)#quit
huawei(config)#interface vlanif 200
huawei(config-if-vlanif200)#mpls ldp
huawei(config-if-vlanif200)#quit
huawei(config)#display mpls interface vlanif 200
```

```
{ <cr>|verbose<K> }:
```

Command:

| Interface | Status | TE Attr | LSP Count | CRLSP Count | Effective MTU |
|-----------|--------|---------|-----------|-------------|---------------|
| vlanif200 | Down   | Dis     | 0         | 0           | 1500          |

To configure an LDP LSP between two nonadjacent LSRs by configuring the local lsr-id to 10.3.3.3, configuring the remote lsr-id to 10.5.5.5, and using default values for other parameters, do as follows:

huawei(config)#mpls ldp  
huawei(config-mpls-ldp)#quit  
huawei(config)#mpls ldp remote-peer session1  
huawei(config-mpls-ldp-remote-session1)#remote-ip 10.5.5.5  
huawei(config-mpls-ldp-remote-session1)#quit  
huawei(config)#display mpls ldp remote-peer  
{ <cr>|peer-id<K>|string<S><Length 1-32>||<K> }:

Command:

display mpls ldp remote-peer

LDP Remote Entity

Information

-----

Remote Peer Name : session1  
Remote Peer IP : 10.5.5.5 LDP ID : 10.1.1.1:0  
Transport Address : 10.1.1.1 Entity Status : Active  
Configured Keepalive Hold Timer : 45  
Sec  
Configured Keepalive Send Timer : ---  
Configured Hello Hold Timer : 45 Sec  
Negotiated Hello Hold Timer : 45 Sec  
Configured Hello Send Timer : ---  
Configured Delay Timer : 10 Sec  
Hello Packet sent/received : 0/0  
Label Advertisement Mode : Downstream Unsolicited  
Remote Peer Deletion Status : No  
Auto-config : ---  
-----

TOTAL: 1 Peer(s) Found.

6.7.3 Configure an RSVP-TE LSP

MPLS TE is a technology that integrates TE with MPLS. Through the MPLS TE technology, you can create an LSP tunnel to a specified path, to reserve resources and implement re-optimization.

Prerequisites

- 1. The IP address of the loopback interface must be configured.
- 2. The LSR ID must be configured.
- 3. The VLAN for MPLS label forwarding must be created.
- 4. Global MPLS and VLAN MPLS must be enabled.
- 5. The OSPF protocol must be successfully configured on each device in the network (the host route of each port must be successfully advertised).

Context

- To create constraint-based LSPs in MPLS TE, RSVP is extended. The extended RSVP signaling protocol is called the RSVP-TE signaling protocol.
- MPLS TE creates the LSP tunnel along a specified path through RSVP-TE and reserves resources. Thus, carriers can accurately control the path that traffic

traverses to avoid the node where congestion occurs. This solves the problem that certain paths are overloaded and other paths are idle, utilizing the current bandwidth resources sufficiently. In addition, MPLS TE can reserve resources during the creation of LSP tunnels to ensure the QoS.

## Procedure

### Step 1 Enable MPLS TE and RSVP-TE.

1. In the global config mode, run the **mpls** command to enter the MPLS mode.
2. In the MPLS mode, run the **mpls te** command to enable global MPLS TE, run the **mpls rsvp-te** command to enable global RSVP-TE, and run the **mpls te cspf** command to enable Constraint Shortest Path First (CSPF).
3. Run the **quit** command to quit the MPLS mode and run the **interface vlanif** command to enter the VLAN interface mode.
4. In the VLAN interface mode, run the **mpls** command to enable the VLAN interface MPLS, run the **mpls te** command to enable the VLAN interface MPLS TE, and run the **mpls rsvp-te** command to enable the VLAN interface RSVP-TE.

#### NOTE

- CSPF provides a way to select the path in an MPLS area. Enable CSPF before configuring other CSPF functions.
- It is recommended that you configure CSPF on all transit nodes lest the ingress cannot calculate the entire path.

### Step 2 (Optional) Configure the line bandwidth.

To guarantee the bandwidth of the service transmitted on the MPLS TE tunnel, perform this operation.

1. In the VLAN interface mode, run the **mpls te bandwidth max-reservable-bandwidth** command to configure the maximum reservable bandwidth for the MPLS TE tunnel on the VLAN interface.
2. In the VLAN interface mode, run the **mpls te bandwidth { bc0 bandwidth | bc1 bandwidth }** command to configure the bandwidth that can be obtained from BC0 and BC1 of the VLAN interface when an MPLS TE tunnel is created.

#### NOTE

- BC0: Indicates the global pool bandwidth of an MPLS TE tunnel.
- BC1: Indicates the sub-pool bandwidth type of an MPLS TE tunnel. It is used to transmit services with higher priority and higher performance requirements.
- The bandwidth values must meet the following requirement: maximum reservable bandwidth  $\geq$  BC0 bandwidth  $\geq$  BC1 bandwidth.

### Step 3 Enable MPLS TE for the OSPF area.

The MA5800 enables the MPLS TE to know the relevant dynamic TE attributes of each link by extending the OSPF protocol. The extended OSPF enables the link status entry to add TE attributes, such as link bandwidth and affinity attribute. Each router in the network collects all the TE information in OSPF area and generates traffic engineering database (TEDB).

1. In the global config mode, run the **ospf** command to start the OSPF process and enter the OSPF mode.

2. Run the **opaque-capability enable** command to enable the OSPF opaque capability.

After the opaque capability of the MA5800 is enabled, it can export TEDB information to neighbor devices.

3. Run the **area** command to enter the OSPF area mode and run the **mpls-te enable** command to enable the OSPF area TE.

#### Step 4 (Optional) Configure an MPLS TE explicit path.

An explicit path consists of a series of nodes, which constitute a vector path according to the configured sequence. The IP address in an explicit path is the IP address of the interface on the node. Generally, the loopback interface IP address on the egress is used as the destination IP address of the explicit path.

To specify a known path for a special traffic stream in the MPLS network, you can run the **explicit-path** command in the global config mode to configure an explicit path, and then run the **mpls te path explicit-path** command in the tunnel mode to specify the explicit path for the tunnel.

After an explicit path is created, you can run the **next hop**, **modify hop**, and **delete hop** command to add a next hop node, modify a node, and delete a node respectively for the explicit path.

#### Step 5 Configure an MPLS TE tunnel interface.

1. In the global config mode, run the **interface tunnel** command to create a tunnel interface and enter the tunnel interface mode.
2. Run the **tunnel-protocol mpls te** command to configure the tunnel protocol to MPLS TE.
3. Run the **destination ip-address** command to configure the destination IP address of the tunnel. Generally, the egress LSR ID is used.
4. Run the **mpls te tunnel-id** command to configure the tunnel ID.
5. Run the **mpls te signal-protocol rsvp-te** command to configure the signaling protocol of the tunnel to RSVP-TE.
6. (Optional) Run the **mpls te bandwidth** command to configure the bandwidth for the tunnel. After the configuration is completed, only the VLAN interface that meets this bandwidth value can be selected as the node traversed by the MPLS TE tunnel path when the MPLS TE tunnel is created.

If the MPLS TE tunnel is only used to change the data transmission path, you may not configure the tunnel bandwidth.

7. (Optional) Run the **mpls te path explicit-path** command to configure the explicit path used by the MPLS TE tunnel.

If only the bandwidth used by the MPLS TE tunnel is limited but the transmission path is not limited, you may not configure the explicit path used by the MPLS TE tunnel.

#### Step 6 Check the configuration.

1. Run the **display mpls te cspf tedb** command to query the CSPF TEDB information.
2. Run the **display mpls te link-administration admission-control** command to check the CR LSP information allowed on the link, including the bandwidth and priority.

3. Run the **display mpls te tunnel** command to query details about a specified tunnel.
4. Run the **display mpls te tunnel path** command to query the path information about a tunnel on a local node.
5. Run the **display mpls te tunnel-interface** command to query the tunnel interface information about a local node.

----End

## Example

To configure the RSVP-TE LSP from the MA5800 to the PTN, set the parameters as follows.

- Set the parameters on the MA5800.
  - LSR ID: 10.3.3.3
  - Layer 3 interface IP address of VLAN 20 for MPLS forwarding: 10.1.1.3/24
  - Maximum reservable bandwidth of the VLAN interface: 20480 kbit/s; BCO bandwidth: 10240 kbit/s
  - OSPF process ID: 100; OSPF area ID: 1
  - MPLS TE tunnel ID: 10; tunnel interface ID: 10
  - Required BCO bandwidth when an MPLS TE tunnel is created: 5120 kbit/s
  - Other parameters: default settings
- Set the LSR ID of the PTN to 10.5.5.5.

```
huawei(config)#interface loopback 0
huawei(config-if-loopback0)#ip address 10.3.3.3 32
huawei(config-if-loopback0)#quit
huawei(config)#mpls lsr-id 10.3.3.3
huawei(config)#mpls
huawei(config-mpls)#mpls te
huawei(config-mpls)#mpls rsdp-te
//Configure the MPLS TE to use CSPF to calculate the shortest path to a node. huawei(config-mpls)#mpls
te cspf
huawei(config-mpls)#quit

huawei(config)#interface vlanif 20
//Configure the IP address of the VLAN interface.
huawei(config-if-vlanif20)#ip address 10.1.1.3 24
//Enable MPLS for the VLAN interface.
huawei(config-if-vlanif20)#mpls
//Enable MPLS TE for the VLAN interface.
huawei(config-if-vlanif20)#mpls te
//Enable MPLS RSVP-TE for the VLAN interface.
huawei(config-if-vlanif20)#mpls rsdp-te
huawei(config-if-vlanif20)#quit
huawei(config)#ospf 100
//Enable the opaque capability to send the engineering data base information to peripheral devices.
huawei(config-ospf-100)#opaque-capability enable
huawei(config-ospf-100)#area 1
//Enable MPLS TE for the OSPF area.

huawei(config-ospf-100-area-0.0.0.1)#mpls-te enable standard-complying
huawei(config-ospf-100-area-0.0.0.1)#quit
huawei(config-ospf-100)#quit
huawei(config)#interface vlanif 20
//Configure the maximum reservable bandwidth of the Layer 3 interface.
huawei(config-if-vlanif20)#mpls te bandwidth max-reservable-bandwidth 20480
//Configure the obtainable maximum bandwidth of the Layer 3 interface from BCO when the MPLS TE
tunnel is created.
```

```
huawei(config-if-vlanif20)#mpls te bandwidth bc0 10240
huawei(config-if-vlanif20)#quit
huawei(config)#interface tunnel 10
//Configure the link layer encapsulation protocol to MPLS TE for the tunnel interface, that is, configure the
//tunnel interface to work in the CR-LSP tunnel mode.
huawei(config-if-tunnel10)#tunnel-protocol mpls te
//Configure the destination IP address of the MPLS TE tunnel.
huawei(config-if-tunnel10)#destination 10.3.3.3
//Configure the MPLS TE tunnel ID, which, along with the LSR-ID, uniquely indicates an MPLS TE tunnel.
huawei(config-if-tunnel10)#mpls te tunnel-id 10
//Configure the protocol of the MPLS TE tunnel to RSVP-TE.
huawei(config-if-tunnel10)#mpls te signal-protocol rsvp-te
//Configure the global pool bandwidth required by the MPLS TE tunnel.

huawei(config-if-tunnel10)#mpls te bandwidth ct0 5120
//Allow the MPLS TE tunnel to be bound to a VPN instance, that is, the MPLS TE tunnel can function as the
//outer tunnel of the PWE3 service.

huawei(config-if-tunnel10)#mpls te reserved-for-binding
huawei(config-if-tunnel10)#quit
```

## 6.7.4 Configuring the MPLS RSVP-TE FRR

The RSVP TE FRR technology is applied to the MPLS TE network for implementing partial network protection. Specifically, when a certain link or node in the network fails, the LSP configured with FRR can automatically switch the data to the protect link.

### Prerequisites

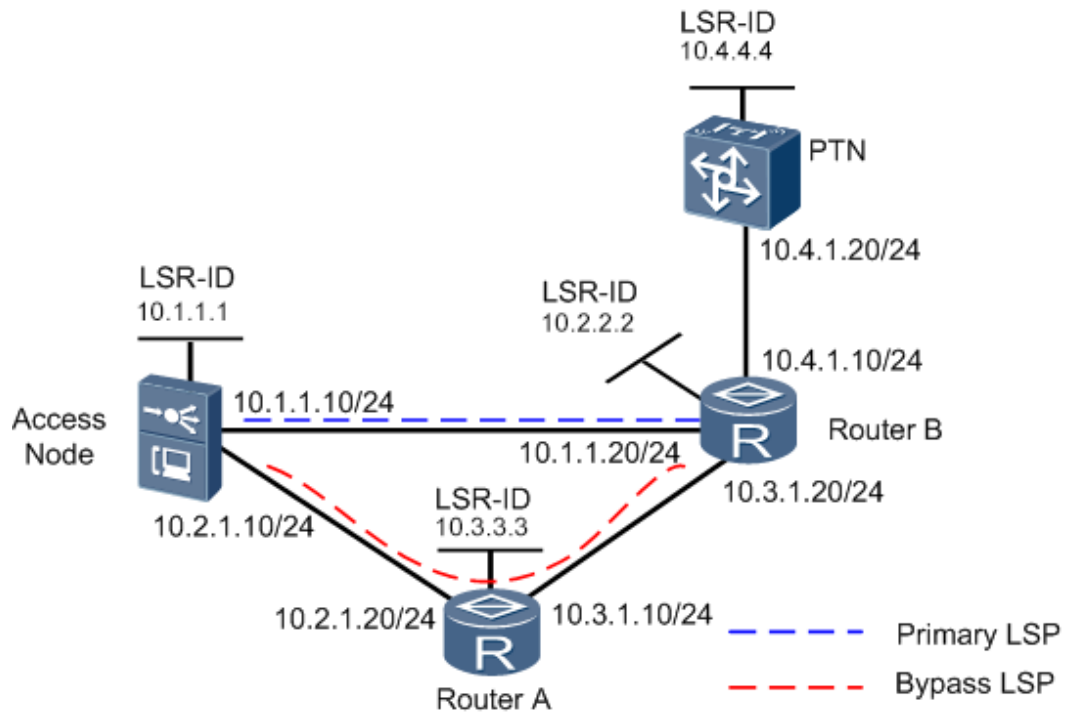
1. The IP address of the loopback interface must be configured.
2. The LSR ID must be configured.
3. The VLAN for MPLS label forwarding must be created.
4. Global MPLS and VLAN MPLS must be enabled.
5. The OSPF protocol must be successfully configured on each device in the network (the host route of each port must be successfully advertised).

### Context

- The implementation of the FRR is based on the extended RSVP-TE signaling. For the FRR, a protect tunnel is created in advance to protect the working tunnel. This prevents the broadcast delay of the notification between NEs and the duration for re-selecting the tunnel if the working tunnel fails. Therefore, the FRR can implement the second-level protection switchover.
- The MA5800 adopts the bypass mode (that is, using a protect path to protect multiple LSPs; the protect path is called the bypass LSP). [Figure 6-12](#) shows the FRR function implemented in the bypass mode.

As shown in the figure, the blue dotted line indicates the primary LSP and the red dotted line indicates the bypass LSP. When the link or node between the MA5800 and Router B is faulty, services are switched to the bypass link MA5800->Router A->Router B. In this manner, the LSP is not affected by the link or node fault.

**Figure 6-12** Example network of the MPLS RSVP-TE FRR



## Procedure

### Step 1 Enable MPLS TE and RSVP-TE.

1. In the global config mode, run the **mpls** command to enter the MPLS mode.
2. In the MPLS mode, run the **mpls te** command to enable global MPLS TE, run the **mpls rsvp-te** command to enable global RSVP-TE, and run the **mpls te cspf** command to enable Constraint Shortest Path First (CSPF).
3. Run the **quit** command to quit the MPLS mode and run the **interface vlanif** command to enter the VLAN interface mode.
4. In the VLAN interface mode, run the **mpls** command to enable the VLAN interface MPLS, run the **mpls te** command to enable the VLAN interface MPLS TE, and run the **mpls rsvp-te** command to enable the VLAN interface RSVP-TE.

#### NOTE

- CSPF provides a way to select the path in an MPLS area. Enable CSPF before configuring other CSPF functions.
- It is recommended that you configure CSPF on all transit nodes lest the ingress cannot calculate the entire path.

### Step 2 (Optional) Configure the line bandwidth.

To guarantee the bandwidth of the service transmitted on the MPLS TE tunnel, perform this operation.

1. In the VLAN interface mode, run the **mpls te bandwidth max-reservable-bandwidth** command to configure the maximum reservable bandwidth for the MPLS TE tunnel on the VLAN interface.

2. In the VLAN interface mode, run the **mpls te bandwidth { bc0 bandwidth | bc1 bandwidth }** command to configure the bandwidth that can be obtained from BC0 and BC1 of the VLAN interface when an MPLS TE tunnel is created.

 **NOTE**

- BC0: Indicates the global pool bandwidth of an MPLS TE tunnel.
- BC1: Indicates the sub-pool bandwidth type of an MPLS TE tunnel. It is used to transmit services with higher priority and higher performance requirements.
- The bandwidth values must meet the following requirement: maximum reservable bandwidth  $\geq$  BC0 bandwidth  $\geq$  BC1 bandwidth.

**Step 3** Enable MPLS TE for the OSPF area.

The MA5800 enables the MPLS TE to know the relevant dynamic TE attributes of each link by extending the OSPF protocol. The extended OSPF enables the link status entry to add TE attributes, such as link bandwidth and affinity attribute. Each router in the network collects all the TE information in OSPF area and generates traffic engineering database (TEDB).

1. In the global config mode, run the **ospf** command to start the OSPF process and enter the OSPF mode.
2. Run the **opaque-capability enable** command to enable the OSPF opaque capability.

After the opaque capability of the MA5800 is enabled, it can export TEDB information to neighbor devices.

3. Run the **area** command to enter the OSPF area mode and run the **mpls-te enable** command to enable the OSPF area TE.

**Step 4** Set up the primary tunnel on the MA5800.

1. Configure the explicit path of the primary LSP.

An explicit path consists of a series of nodes, which constitute a vector path according to the configured sequence. The IP address in an explicit path is the IP address of the interface on the node. Generally, the loopback interface IP address on the egress is used as the destination IP address of the explicit path.

To specify a known path for a special traffic stream in the MPLS network, you can run the **explicit-path** command in the global config mode to configure an explicit path, and then run the **mpls te path explicit-path** command in the tunnel mode to specify the explicit path for the tunnel.

After an explicit path is created, you can run the **next hop**, **modify hop**, and **delete hop** command to add a next hop node, modify a node, and delete a node respectively for the explicit path.

2. Configure the MPLS TE tunnel of the primary LSP.
  - a. In the global config mode, run the **interface tunnel** command to create a tunnel interface and enter the tunnel interface mode.
  - b. Run the **tunnel-protocol mpls te** command to configure the tunnel protocol to MPLS TE.
  - c. Run the **destination ip-address** command to configure the destination IP address of the tunnel. Generally, the egress LSR ID is used.
  - d. Run the **mpls te tunnel-id** command to configure the tunnel ID.
  - e. Run the **mpls te signal-protocol rsvp-te** command to configure the signaling protocol of the tunnel to RSVP-TE.

- f. (Optional) Run the **mpls te bandwidth** command to configure the bandwidth for the tunnel. After the configuration is completed, only the VLAN interface that meets this bandwidth value can be selected as the node traversed by the MPLS TE tunnel path when the MPLS TE tunnel is created.  
If the MPLS TE tunnel is only used to change the data transmission path, you may not configure the tunnel bandwidth.
  - g. Run the **mpls te path explicit-path** command to configure the explicit path used by the MPLS TE tunnel.
3. Enable the FRR function of the tunnel.  
Run the **mpls te fast-reroute [bandwidth]** command to enable TE FRR of the tunnel interface and allow bandwidth protection. By default, the FRR function is prohibited.

 **NOTE**

Bandwidth protection configured through this command is used only for selecting the bypass tunnel policy. When the primary tunnel is faulty and needs to switch to a bypass tunnel, the bypass tunnel that meets the bandwidth requirement is preferred. If no bypass tunnel meets the bandwidth requirement, the primary tunnel selects an optimal bypass tunnel from the existing bypass tunnels.

**Step 5** Set up a bypass LSP tunnel on the MA5800.

1. Configure the explicit path of the bypass LSP.
  - a. In the global config mode, run the **explicit-path** command to configure the explicit path. In the tunnel mode, run the **mpls te path explicit-path** command to specify the explicit path for the tunnel.
  - b. Run the **next hop**, **modify hop**, and **delete hop** command to add a next hop node, modify a node, and delete a node respectively for the explicit path.
2. Configure the MPLS TE tunnel of the bypass LSP.

---

**NOTICE**

MPLS TE tunnel IDs of the primary and bypass LSPs cannot be the same.

---

- a. In the global config mode, run the **interface tunnel** command to create a tunnel interface and enter the tunnel interface mode.
- b. Run the **tunnel-protocol mpls te** command to configure the tunnel protocol to MPLS TE.
- c. Run the **destination ip-address** command to configure the destination IP address of the tunnel. Generally, the egress LSR ID is used.
- d. Run the **mpls te tunnel-id** command to configure the tunnel ID.
- e. Run the **mpls te signal-protocol rsvp-te** command to configure the signaling protocol of the tunnel to RSVP-TE.
- f. (Optional) Run the **mpls te bandwidth** command to configure the bandwidth for the tunnel. After the configuration is completed, only the VLAN interface that meets this bandwidth value can be selected as the node traversed by the MPLS TE tunnel path when the MPLS TE tunnel is created.

If the MPLS TE tunnel is only used to change the data transmission path, you may not configure the tunnel bandwidth.

- g. Run the **mpls te path explicit-path** command to configure the explicit path used by the MPLS TE tunnel.
3. Bind the bypass LSP tunnel to the protected interface.
  - a. In the tunnel mode, run the **mpls te bypass-tunnel** command to configure a bypass tunnel of the FRR.

 **NOTE**

The total bandwidth of all LSPs that use bypass tunnels does not exceed the bandwidth of the primary tunnel. If multiple bypass tunnels exist, the system uses the best-fit algorithm to determine which bypass to use.

- b. Run the **mpls te protected-interface** command to specify the interface to be protected by the bypass tunnel. When the interface is faulty, a bypass tunnel switching is triggered.

 **NOTE**

One bypass tunnel can protect up to three interfaces, and MPLS TE must be enabled for the protected interfaces.

----End

## Result

Enter the VLAN interface mode, and run the **shutdown** command to shut down the VLAN interface to disable the protected egress on the primary LSP. Then run the **display interface tunnel** command to query the status of the primary LSP on the MA5800. You can see that the tunnel interface is still in the up state. Finally, run the **tracert lsp te tunnel** command to check the path traversed by the tunnel. You can see that the link is switched to the bypass tunnel.

## Example

As shown in [Figure 6-12](#), when the link or node between the MA5800 and Router B is faulty, services are switched to the standby link MA5800->Router A->Router B. In this manner, the LSP is not affected by the fault of link or node. Set the parameters as follows:

- Set the parameters on the MA5800.
  - LSR ID: 10.1.1.1
  - IP address of VLAN interface 10 connected to Router B: 10.1.1.10/24
  - IP address of VLAN interface 20 connected to Router A: 10.2.1.10/24
- Set the parameters on the Router B.
  - LSR ID: 10.2.2.2
  - IP address of the interface connected to the MA5800: 10.1.1.20/24
  - IP address of the interface connected to Router A: 10.3.1.20/24
  - IP address of the interface connected to the PTN: 10.4.1.10/24
- Set the parameters on the Router A.
  - LSR ID: 10.3.3.3

- IP address of the interface connected to the MA5800: 10.2.1.20/24
  - IP address of the interface connected to Router B: 10.3.1.10/24
- Set the parameters on the PTN.
  - LSR ID: 10.4.4.4
  - IP address of the interface connected to Router B: 10.4.1.20/24

```
//Configure the LSR-ID.
huawei(config)#interface loopback 0
huawei(config-if-loopback0)#ip address 10.1.1.1 32
huawei(config-if-loopback0)#quit
huawei(config)#mpls lsr-id 10.1.1.1
//Enable RSVP-TE.
huawei(config)#mpls
huawei(config-mpls)#mpls te
huawei(config-mpls)#mpls rsdp-te
huawei(config-mpls)#mpls te cspf
huawei(config-mpls)#quit
//Configure the IP address of VLAN interface 10 and enable RSVP-TE of the VLAN interface.
huawei(config)#vlan 10 standard
huawei(config)#interface vlanif 10
huawei(config-if-vlanif10)#ip address 10.1.1.10 24
huawei(config-if-vlanif10)#mpls
huawei(config-if-vlanif10)#mpls te
huawei(config-if-vlanif10)#mpls rsdp-te
huawei(config-if-vlanif10)#quit
//Configure the IP address of VLAN interface 20 and enable RSVP-TE of the VLAN interface.
huawei(config)#vlan 20 standard
huawei(config)#interface vlanif 20
huawei(config-if-vlanif20)#ip address 10.2.1.10 24
huawei(config-if-vlanif20)#mpls
huawei(config-if-vlanif20)#mpls te
huawei(config-if-vlanif20)#mpls rsdp-te
huawei(config-if-vlanif20)#quit
//Configure OSPF TE.
huawei(config)#ospf 100
huawei(config-ospf-100)#opaque-capability enable
huawei(config-ospf-100)#area 0
huawei(config-ospf-100-area-0.0.0.0)#mpls-te enable standard-complying
huawei(config-ospf-100-area-0.0.0.0)#quit
huawei(config-ospf-100)#quit
//Configure the explicit path of the primary LSP.
huawei(config)#explicit-path pri-path
huawei(config-explicit-path-pri-path)#next hop 10.1.1.20
huawei(config-explicit-path-pri-path)#next hop 10.4.1.20
huawei(config-explicit-path-pri-path)#quit
//Configure the MPLS TE tunnel of the primary LSP.
huawei(config)#interface tunnel 10
huawei(config-if-tunnel10)#tunnel-protocol mpls te
huawei(config-if-tunnel10)#destination 10.2.2.2
huawei(config-if-tunnel10)#mpls te tunnel-id 10
huawei(config-if-tunnel10)#mpls te signal-protocol rsdp-te
huawei(config-if-tunnel10)#mpls te path explicit-path pri-path
huawei(config-if-tunnel10)#mpls te fast-reroute
huawei(config-if-tunnel10)#mpls te commit
huawei(config-if-tunnel10)#quit
//Configure the explicit path of the bypass LSP.
huawei(config)#explicit-path bypass-path
huawei(config-explicit-path-bypass-path)#next hop 10.2.1.20
huawei(config-explicit-path-bypass-path)#next hop 10.3.1.20
huawei(config-explicit-path-bypass-path)#quit
//Configure the MPLS TE tunnel of the bypass LSP.
huawei(config)#interface tunnel 20
huawei(config-if-tunnel20)#tunnel-protocol mpls te
huawei(config-if-tunnel20)#destination 10.2.2.2
huawei(config-if-tunnel20)#mpls te tunnel-id 20
```

```
huawei(config-if-tunnel20)#mpls te signal-protocol rsvp-te
huawei(config-if-tunnel20)#mpls te path explicit-path bypass-path
huawei(config-if-tunnel20)#mpls te bypass-tunnel
huawei(config-if-tunnel20)#mpls te protected-interface vlanif 10
huawei(config-if-tunnel20)#mpls te commit
huawei(config-if-tunnel20)#quit
```

## 6.7.5 Configuring the MPLS OAM

The MPLS OAM function uses an effective OAM mechanism to detect whether an LSP is normal and report an alarm in time when an LSP fault occurs. In addition, the MPLS OAM function features a complete protection switching mechanism, which triggers a switchover when a defect at the MPLS layer is detected to minimize the data loss.

### Context

Through the MPLS OAM mechanism, the MA5800 can effectively detect, confirm, and locate internal defects at the MPLS layer of a network. Then, the system reports and handles the defects. In addition, the system provides a mechanism for triggering 1:1 protection switching when a fault occurs.

The basic process of the MPLS OAM connectivity check and protection switching is as follows:

1. The source transmits the CV/FFD packets to the destination through the detected LSP.
2. The destination checks the correctness of the type and frequency carried in the received detection packets and measures the number of correct and incorrect packets that are received within the detection period to monitor the connectivity of the LSP in real time.
3. After detecting a defect, the destination transmits the BDI packets that carry the defect information to the source through the backward path.
4. The source learns about the status of the defect, and triggers the corresponding protection switching when the protect group is correctly configured.

Configure the MPLS OAM as follows:

1. Configure the active LSP at the source end (ingress).
2. Configure the standby LSP at the source end.
3. Create a tunnel protect group.
4. Enable the MPLS OAM function at the source end.
5. Configure the backward LSP at the destination end (egress).
6. Enable the MPLS OAM function at the destination end.

#### NOTE

If only the MPLS OAM connectivity check needs to be enabled and 1:1 protection is not required for the LSP, you need not configure the standby LSP or the tunnel protect group at the source end.

### 6.7.5.1 Configuration Example for Detection of MPLS OAM for Static LSP Connectivity

This topic describes how to configure the function of MPLS OAM to detect the static LSP connectivity.

#### Prerequisites

Before the configuration, make sure that:

- Set the IP addresses and the masks of the ports based on the example network. After that, LSRs can ping the peer LSRs.
- A static or dynamic route must be successfully configured on each device in the network (so that LSRs can reach each other through the IP route).

#### Networking

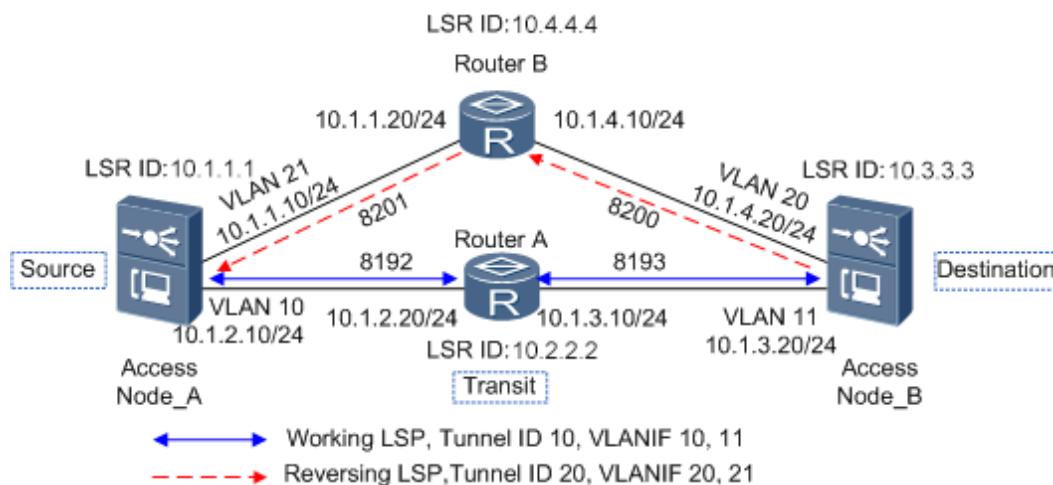
**Figure 6-13** shows an example network of configuring MPLS OAM to detect the static LSP connectivity.

1. Source end MA5800\_A sends CV/FFD detection packets to the destination end through the detected LSP (MA5800\_A->Router A->MA5800\_B).
2. After detecting a defect, the destination transmits the BDI packets that carry the defect information to the source through the backward LSP (MA5800\_B->Router B->MA5800\_A). This enables the source end to obtain the defect status in time.

#### NOTE

To facilitate description of the MPLS OAM application, the MA5800 is used at both the source end and destination end as an example. In the actual application, the MA5800 at one end may be replaced by a device that supports MPLS OAM such as a PTN device, but their implementation principles are the same.

**Figure 6-13** Example network of detection of MPLS OAM for static LSP connectivity



## Data Plan

**Table 6-5** provides the data plan for detection of MPLS OAM for static LSP connectivity.

**Table 6-5** Data plan for detection of MPLS OAM for static LSP connectivity

| Item     | Data                                                                                                                                                                                                               |
|----------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| MA5800_A | LSR ID: 10.1.1.1                                                                                                                                                                                                   |
|          | Port: 0/9/0<br>IP address of VLAN interface 10 connected to Router A: 10.1.2.10/24<br>Tunnel ID: 10; tunnel interface ID: 10<br>Out label value of the LSP ingress: 8192<br>In label value of the LSP egress: 8193 |
|          | Port: 0/9/1<br>IP address of VLAN interface 21 connected to Router B: 10.1.1.10/24                                                                                                                                 |
|          | Static LSP: Router A to MA5800_B                                                                                                                                                                                   |
| MA5800_B | LSR ID: 10.3.3.3                                                                                                                                                                                                   |
|          | Port: 0/9/0<br>IP address of VLAN interface 11 connected to Router A: 10.1.3.20/24                                                                                                                                 |
|          | Port: 0/9/1<br>IP address of VLAN interface 20 connected to Router B: 10.1.4.20/24<br>Tunnel ID: 20; tunnel interface ID: 20<br>Out label value of the LSP ingress: 8200<br>In label value of the LSP egress: 8201 |
|          | Static LSP: Router B to MA5800_A                                                                                                                                                                                   |
| Router A | LSR ID: 10.2.2.2                                                                                                                                                                                                   |
|          | IP address of the interface connected to the MA5800_A: 10.1.2.20/24                                                                                                                                                |
|          | IP address of the interface connected to the MA5800_B: 10.1.3.10/24                                                                                                                                                |
| Router B | LSR ID: 10.4.4.4                                                                                                                                                                                                   |
|          | IP address of the interface connected to the MA5800_A: 10.1.1.20/24                                                                                                                                                |
|          | IP address of the interface connected to the MA5800_B: 10.1.4.10/24                                                                                                                                                |

## Procedure

- **Configure source end MA5800\_A.**

- a. Configure the loopback interface.

```
huawei(config)#interface loopback 0
huawei(config-if-loopback0)#ip address 10.1.1.1 32
huawei(config-if-loopback0)#quit
```

- b. Enable the basic MPLS and MPLS TE.

- i. Enable the basic MPLS and MPLS TE globally.

```
huawei(config)#mpls lsr-id 10.1.1.1
huawei(config)#mpls
huawei(config-mpls)#mpls te
huawei(config-mpls)#quit
```

- ii. Enable the basic MPLS and MPLS TE on the interface.

```
huawei(config)#vlan 10 standard
huawei(config)#port vlan 10 0/9 0
huawei(config)#interface vlanif 10
huawei(config-if-vlanif10)#ip address 10.1.2.10 24
huawei(config-if-vlanif10)#mpls
huawei(config-if-vlanif10)#mpls te
huawei(config-if-vlanif10)#quit
huawei(config)#vlan 21 standard
huawei(config)#port vlan 21 0/9 1
huawei(config)#interface vlanif 21
huawei(config-if-vlanif21)#ip address 10.1.1.10 24
huawei(config-if-vlanif21)#mpls
huawei(config-if-vlanif21)#mpls te
huawei(config-if-vlanif21)#quit
```

- c. Configure the MPLS TE tunnel from the source end to the destination end.

Configure the MPLS TE tunnel bound to the detected LSP.

```
huawei(config)#interface tunnel 10
huawei(config-if-tunnel10)#tunnel-protocol mpls te
huawei(config-if-tunnel10)#destination 10.3.3.3
huawei(config-if-tunnel10)#mpls te tunnel-id 20
huawei(config-if-tunnel10)#mpls te signal-protocol static
huawei(config-if-tunnel10)#mpls te commit
huawei(config-if-tunnel10)#quit
```

- d. Configure the static LSP bound to the MPLS TE tunnel.

Source end MA5800 functions as the ingress of the detected static LSP.

```
huawei(config)#static-lsp ingress tunnel-interface tunnel 10
destination 10.3.3.3 nexthop 10.1.2.20 out-label 8192
```

Source end MA5800 functions as the egress of the detected static LSP.

```
huawei(config)#static-lsp egress LSP1 incoming-interface vlanif 10 in-label 8193
```

Source end MA5800 functions as the egress of the backward static LSP.

```
huawei(config)#static-lsp egress LSP2 incoming-interface vlanif 20 in-label 8201
```

- e. Enable MPLS OAM at source end MA5800\_A.

```
huawei(config)#mpls
huawei(config-mpls)#mpls oam
huawei(config-mpls)#quit
huawei(config)#mpls oam ingress tunnel 10 type ffd frequency 100
backward-lsp lsr-id 10.3.3.3 tunnel-id 20
...//Configure the MPLS OAM source end. Configure the tunnel ID of the detected LSP to 10,
detection packet type to FFD, Tx frequency to 100 ms, LSR-ID of the backward LSP to 10.3.3.3,
```

```
...//and backward LSP tunnel ID to 20.  
huawei(config)#mpls oam ingress enable all
```

- f. Save the data.

```
huawei(config)#save
```

- **Configure Router A or Router B.**

When functioning as the transit node, Router A or Router B mainly forwards MPLS labels. The ingress interface, in label, next hop IP address, and out label must be configured bi-directionally. For detailed configuration, see the configuration guide of the specific router.

- **Configure destination end MA5800\_B.**

- a. Configure the loopback interface.

```
huawei(config)#interface loopback 0  
huawei(config-if-loopback0)#ip address 10.3.3.3 32  
huawei(config-if-loopback0)#quit
```

- b. Enable the basic MPLS and MPLS TE.

- i. Enable the basic MPLS and MPLS TE globally.

```
huawei(config)#mpls lsr-id 10.3.3.3  
huawei(config)#mpls  
huawei(config-mpls)#mpls te  
huawei(config-mpls)#quit
```

- ii. Enable the basic MPLS and MPLS TE on the interface.

```
huawei(config)#vlan 11 standard  
huawei(config)#port vlan 11 0/9 0  
huawei(config)#interface vlanif 11  
huawei(config-if-vlanif11)#ip address 10.1.3.20 24  
huawei(config-if-vlanif11)#mpls  
huawei(config-if-vlanif11)#mpls te  
huawei(config-if-vlanif11)#quit  
huawei(config)#vlan 20 standard  
huawei(config)#port vlan 20 0/9 1  
huawei(config)#interface vlanif 20  
huawei(config-if-vlanif20)#ip address 10.1.4.20 24  
huawei(config-if-vlanif20)#mpls  
huawei(config-if-vlanif20)#mpls te  
huawei(config-if-vlanif20)#quit
```

- c. Configure the MPLS TE tunnel from the destination end to the source end.

Configure the MPLS TE tunnel bound to the detected LSP.

```
huawei(config)#interface tunnel 10  
huawei(config-if-tunnel10)#tunnel-protocol mpls te  
huawei(config-if-tunnel10)#destination 10.1.1.1  
huawei(config-if-tunnel10)#mpls te tunnel-id 10  
huawei(config-if-tunnel10)#mpls te signal-protocol static  
huawei(config-if-tunnel10)#mpls te commit  
huawei(config-if-tunnel10)#quit
```

Configure the MPLS TE tunnel bound to the backward LSP.

```
huawei(config)#interface tunnel 20  
huawei(config-if-tunnel20)#tunnel-protocol mpls te  
huawei(config-if-tunnel20)#destination 10.1.1.1  
huawei(config-if-tunnel20)#mpls te tunnel-id 20  
huawei(config-if-tunnel20)#mpls te signal-protocol static  
huawei(config-if-tunnel20)#mpls te commit  
huawei(config-if-tunnel20)#quit
```

- d. Configure the static LSP bound to the tunnel.

Destination end MA5800 functions as the egress of the detected static LSP.

```
huawei(config)#static-lsp egress LSP2 incoming-interface vlanif 10 in-label 8192
```

Destination end MA5800 functions as the ingress of the detected static LSP.

```
huawei(config)#static-lsp ingress tunnel-interface tunnel 10  
destination 10.1.1.1 nexthop 10.1.3.10 out-label 8193
```

Destination end MA5800 functions as the ingress of the backward static LSP.

```
huawei(config)#static-lsp ingress tunnel-interface tunnel 20  
destination 10.1.1.1 nexthop 10.1.4.10 out-label 8200
```

- e. Enable MPLS OAM at destination end MA5800.

```
huawei(config)#mpls  
huawei(config-mpls)#mpls oam  
huawei(config-mpls)#quit  
huawei(config)#mpls oam egress lsr-id 10.1.1.1 tunnel-id 10 type ffd frequency 100  
backward-lsp tunnel 20 private  
...//Configure the MPLS OAM destination end. Configure the ingress LSR-ID of the detected LSP  
to 10.1.1.1, tunnel ID to 10, detection packet type to FFD, Tx frequency to 100 ms,  
  
...//backward LSP tunnel ID to 20, and tunnel to exclusive mode.  
  
huawei(config)#mpls oam egress enable all
```

- f. Save the data.

```
huawei(config)#save
```

----End

## Result

After the configuration, shut down the interface of VLAN 10 by running the **shutdown** command on MA5800\_A to simulate the link fault:

- On MA5800\_B, run the **display mpls oam egress** command and you can see the following defect state: dLocv detected (dLocv).
- On MA5800\_A, run the **display mpls oam ingress** command and you can see the following defect state: in defect (In-defect).

Perform similar operations on MA5800\_B and you can obtain similar results.

### 6.7.5.2 Configuration Example of the MPLS OAM Protection Switching Function

This topic describes how to configure MPLS OAM to implement the protection switching function.

#### Service Requirements

- The OAM mechanism is used to detect in real time whether the MPLS link is normal and generates an alarm in time when a link fault is detected.
- The end-to-end tunnel protection technology is provided to recover the interrupted service.
- RSVP-TE is used to create an LSP tunnel for the specified path and reserve resources so that the existing bandwidth resources can be fully used and QoS can be improved for specific services.

Prerequisite

- The OSPF protocol must be successfully configured on each LSR in the network (the host route of each port must be successfully advertised).
- The interface IP address and mask, loopback interface, and LSR-ID must be configured on each LSR.
- The global and physical interface MPLS and MPLS TE functions must be enabled on each node of the LSR.

Networking

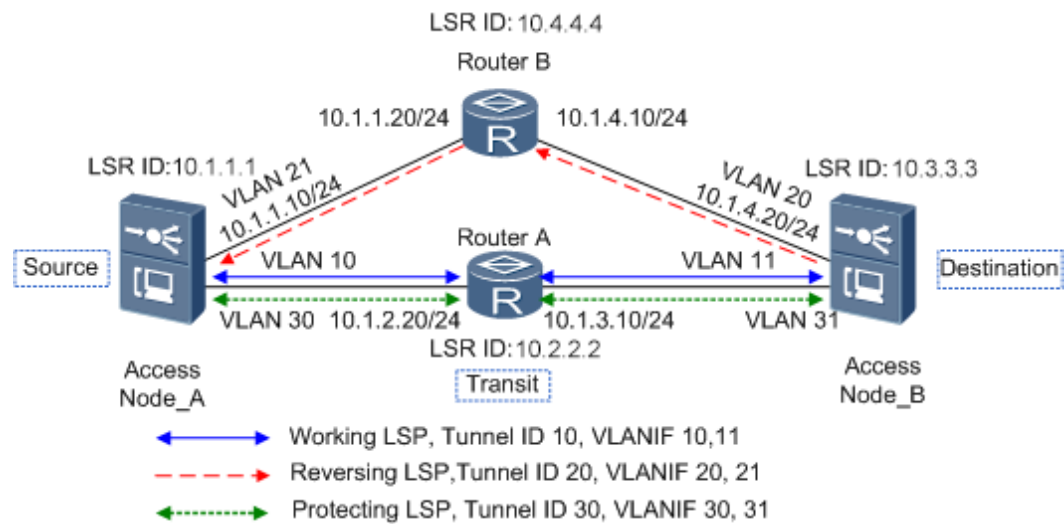
Figure 6-14 shows an example network for configuring the MPLS OAM protection switching function.

Configure two LSP tunnels on source end MA5800\_A and destination end MA5800\_B functioning primary and secondary LSPs. Enable the MPLS OAM protection switching function for the LSPs. When the primary LSP is faulty, the traffic is switched to the secondary LSP. Configure the backward LSP for reporting a fault to source end MA5800\_A.

NOTE

To prevent a fault from occurring on a transit node (for example, router A), it is recommended that you specify different transit nodes when creating a secondary LSP.

Figure 6-14 Configuring the MPLS OAM protection switching function



Data Plan

Table 6-6 provides the data plan for the MPLS OAM protection switching.

Table 6-6 Data plan for the MPLS OAM protection switching

| Item     | Data             |
|----------|------------------|
| MA5800_A | LSR ID: 10.1.1.1 |

| Item     | Data                                                                                                                                                            |
|----------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------|
|          | Port: 0/9/0<br>IP address of VLAN interface 10 connected to Router A:<br>10.1.2.10/24                                                                           |
|          | Port: 0/9/1<br>IP address of VLAN interface 30 connected to Router A:<br>10.1.5.10/24<br>IP address of VLAN interface 21 connected to Router B:<br>10.1.1.10/24 |
|          |                                                                                                                                                                 |
| MA5800_B | LSR ID: 10.3.3.3                                                                                                                                                |
|          | Port: 0/9/0<br>IP address of VLAN interface 11 connected to Router A:<br>10.1.3.20/24                                                                           |
|          | Port: 0/9/1<br>IP address of VLAN interface 20 connected to Router B:<br>10.1.4.20/24<br>IP address of VLAN interface 31 connected to Router A:<br>10.1.6.20/24 |
|          | Backward tunnel: Router B to MA5800_A                                                                                                                           |
| Router A | LSR ID: 10.2.2.2                                                                                                                                                |
| Router B | LSR ID: 10.4.4.4                                                                                                                                                |

## Procedure

- **Configure source end MA5800\_A.**
  - a. Configure the loopback interface.

```
huawei(config)#interface loopback 0
huawei(config-if-loopback0)#ip address 10.1.1.1 32
huawei(config-if-loopback0)#quit
```
  - b. Enable the basic MPLS, MPLS TE, and RSVP-TE functions.
    - i. Enable the global basic MPLS, MPLS TE, and RSVP-TE functions.

```
huawei(config)#mpls lsr-id 10.1.1.1
huawei(config)#mpls
huawei(config-mpls)#mpls te
huawei(config-mpls)#mpls rsvp-te
huawei(config-mpls)#mpls te cspf
huawei(config-mpls)#quit
```
    - ii. Enable the interface basic MPLS, MPLS TE, and RSVP-TE functions.

```
//Configure the attributes of VLAN interface 10 and configure the L3 IP address of VLAN
interface10 to 10.1.2.10/24.
huawei(config)#vlan 10 standard
huawei(config)#port vlan 10 0/9 0
huawei(config)#interface vlanif 10
huawei(config-if-vlanif10)#ip address 10.1.2.10 24
huawei(config-if-vlanif10)#mpls
huawei(config-if-vlanif10)#mpls te
```

```
huawei(config-if-vlanif10)#mpls rsvp-te
huawei(config-if-vlanif10)#mpls te bandwidth max-reservable-bandwidth 10240
// (Optional) Configure VLAN interface 10 to provide a reservable bandwidth of 10240
kbit/s for all tunnels.
huawei(config-if-vlanif10)#quit
// Configure the attributes of VLAN interface 30 and configure the L3 IP address of VLAN
interface 30 to 10.1.5.10/24.
huawei(config)#vlan 30 standard
huawei(config)#port vlan 30 0/9 1
huawei(config)#interface vlanif 30
huawei(config-if-vlanif30)#ip address 10.1.5.10 24
huawei(config-if-vlanif30)#mpls
huawei(config-if-vlanif30)#mpls te
huawei(config-if-vlanif30)#mpls rsvp-te
huawei(config-if-vlanif30)#mpls te bandwidth max-reservable-bandwidth 10240
// (Optional) Configure VLAN interface 30 to provide a reservable bandwidth of 10240
kbit/s for all tunnels.
huawei(config-if-vlanif30)#quit
// Configure the attributes of VLAN interface 21 and configure the L3 IP address of VLAN
interface 21 to 10.1.1.10/24.
huawei(config)#vlan 21 standard
huawei(config)#port vlan 21 0/9 1
huawei(config)#interface vlanif 21
huawei(config-if-vlanif21)#ip address 10.1.1.10 24
huawei(config-if-vlanif21)#mpls
huawei(config-if-vlanif21)#mpls te
huawei(config-if-vlanif21)#mpls rsvp-te
huawei(config-if-vlanif21)#mpls te bandwidth max-reservable-bandwidth 10240
// (Optional) Configure VLAN interface 21 to provide a reservable bandwidth of 10240
kbit/s for all tunnels.
huawei(config-if-vlanif21)#quit
```

c. Enable MPLS TE for the OSPF area.

```
huawei(config)#ospf 100
huawei(config-ospf-100)#opaque-capability enable
huawei(config-ospf-100)#area 0
huawei(config-ospf-100-area-0.0.0.0)#mpls-te enable standard-complying
huawei(config-ospf-100-area-0.0.0.0)#quit
huawei(config-ospf-100)#quit
```

d. Configure the MPLS TE tunnel from the source end to the destination end.

Configure the attributes of the working MPLS TE tunnel from the source end to the destination end.

```
huawei(config)#interface tunnel 10
huawei(config-if-tunnel10)#tunnel-protocol mpls te
huawei(config-if-tunnel10)#destination 10.3.3.3
huawei(config-if-tunnel10)#mpls te tunnel-id 10
huawei(config-if-tunnel10)#mpls te signal-protocol rsvp-te
huawei(config-if-tunnel10)#mpls te bandwidth ct0 5120 // (Optional) Configure the global
bandwidth of tunnel 10 to 5120 kbit/s.
huawei(config-if-tunnel10)#quit
```

Configure the attributes of the protection MPLS TE tunnel from the source end to the destination end.

```
huawei(config)#interface tunnel 30
huawei(config-if-tunnel30)#tunnel-protocol mpls te
huawei(config-if-tunnel30)#destination 10.3.3.3
huawei(config-if-tunnel30)#mpls te tunnel-id 30
huawei(config-if-tunnel30)#mpls te signal-protocol rsvp-te
huawei(config-if-tunnel30)#mpls te bandwidth ct0 5120 // (Optional) Configure the global
bandwidth of tunnel 30 to 5120 kbit/s.
huawei(config-if-tunnel30)#quit
```

e. Configure a tunnel protect group.

Configure tunnel 30 as the protect tunnel for tunnel 10, switching mode to revertive, and automatic WTR time to 900s (the corresponding WTR is 30 with step 30s).

```
huawei(config)#interface tunnel 10
huawei(config-if-tunnel10)#mpls te protection tunnel 30 mode revertive wtr 30
huawei(config-if-tunnel10)#quit
```

- f. Enable MPLS OAM at source end MA5800\_A.

```
huawei(config)#mpls
huawei(config-mpls)#mpls oam
huawei(config-mpls)#quit
huawei(config)#mpls oam ingress tunnel 10 type ffd frequency 100
backward-lsp lsr-id 10.3.3.3 tunnel-id 20
//Configure the MPLS OAM source end. Configure the tunnel ID of the detected LSP to 10,
detection packet type to FFD, Tx frequency to 100 ms, LSR-ID of the backward LSP to 10.3.3.3,
//and backward LSP tunnel ID to 20.
huawei(config)#mpls oam ingress enable all
```

- g. Save the data.

```
huawei(config)#save
```

- **Configure Router A or Router B.**

When functioning as the transit node, Router A or Router B mainly forwards MPLS labels. The ingress interface, in label, next hop IP address, and out label must be configured bi-directionally. For detailed configuration, see the configuration guide of the specific router.

- **Configure destination end MA5800\_B.**

- a. Configure the loopback interface.

```
huawei(config)#interface loopback 0
huawei(config-if-loopback0)#ip address 10.3.3.3 32
huawei(config-if-loopback0)#quit
```

- b. Enable the basic MPLS, MPLS TE, and RSVP-TE functions.

- i. Enable the global basic MPLS, MPLS TE, and RSVP-TE functions.

```
huawei(config)#mpls lsr-id 10.3.3.3
huawei(config)#mpls
huawei(config-mpls)#mpls te
huawei(config-mpls)#mpls rsvp-te
huawei(config-mpls)#mpls te cspf
huawei(config-mpls)#quit
```

- ii. Enable the interface basic MPLS, MPLS TE, and RSVP-TE functions.

```
//Configure the attributes of VLAN interface 11 and configure the L3 IP address of VLAN
interface 11 to 10.1.3.20/24.
huawei(config)#vlan 11 standard
huawei(config)#port vlan 11 0/9 0
huawei(config)#interface vlanif 11
huawei(config-if-vlanif11)#ip address 10.1.3.20 24
huawei(config-if-vlanif11)#mpls
huawei(config-if-vlanif11)#mpls te
huawei(config-if-vlanif11)#mpls rsvp-te
huawei(config-if-vlanif11)#quit
//Configure the attributes of VLAN interface 20 and configure the L3 IP address of VLAN
interface 20 to 10.1.4.20/24.
huawei(config)#vlan 20 standard
huawei(config)#port vlan 20 0/9 1
huawei(config)#interface vlanif 20
huawei(config-if-vlanif20)#ip address 10.1.4.20 24
huawei(config-if-vlanif20)#mpls
huawei(config-if-vlanif20)#mpls te
huawei(config-if-vlanif20)#mpls rsvp-te
huawei(config-if-vlanif20)#quit
//Configure the attributes of VLAN interface 31 and configure the L3 IP address of VLAN
interface 31 to 10.1.6.20/24.
huawei(config)#vlan 31 standard
```

```
huawei(config)#port vlan 31 0/9 1
huawei(config)#interface vlanif 31
huawei(config-if-vlanif31)#ip address 10.1.6.20 24
huawei(config-if-vlanif31)#mpls
huawei(config-if-vlanif31)#mpls te
huawei(config-if-vlanif31)#mpls rsvp-te
huawei(config-if-vlanif31)#quit
```

- c. Configure the MPLS TE tunnel bound to the backward LSP.

Configure the tunnel ID to 20, destination IP address to 10.1.1.1, and global bandwidth for the tunnel to 5120 kbit/s.

```
huawei(config)#interface tunnel 20
huawei(config-if-tunnel20)#tunnel-protocol mpls te
huawei(config-if-tunnel20)#destination 10.1.1.1
huawei(config-if-tunnel20)#mpls te tunnel-id 20
huawei(config-if-tunnel20)#mpls te signal-protocol rsvp-te
huawei(config-if-tunnel20)#mpls te bandwidth ct0 5120
huawei(config-if-tunnel20)#mpls te reserved-for-binding
huawei(config-if-tunnel20)#quit
```

- d. Enable MPLS OAM at destination end MA5800\_B.

```
huawei(config)#mpls
huawei(config-mpls)#mpls oam
huawei(config-mpls)#quit
huawei(config)#mpls oam egress lsr-id 10.1.1.1 tunnel-id 10 type ffd frequency 100
backward-lsp tunnel 20 private
//Configure the MPLS OAM destination end. Configure the ingress LSR-ID of the detected LSP
to 10.1.1.1, tunnel ID to 10, detection packet type to FFD, Tx frequency to 100 ms,
//backward LSP tunnel ID to 20, and tunnel to exclusive mode.
huawei(config)#mpls oam egress enable all
```

- e. Save the data.

```
huawei(config)#save
```

----End

## Result

After the configuration, you can shut down the interface of VLAN 10 by running the **shutdown** command on MA5800\_A to simulate the link fault. Then, you can query the information about the primary tunnel (with ID 10) that is configured on MA5800\_A by running the **display mpls te protection tunnel** command on MA5800\_A. The information is as follows:

- Status of the working tunnel (work-tunnel defect state): in defect.
- Status of the protection tunnel (protect-tunnel defect state): non-defect.
- Switch result: The traffic is switched to protection tunnel 30.